Springer Monographs in Mathematics

Inder Bir Singh Passi
Mahender Singh
Manoj Kumar Yadav

Automorphisms of Finite Groups

Springer

Springer Monographs in Mathematics

This series publishes advanced monographs giving well-written presentations of the "state-of-the-art" in fields of mathematical research that have acquired the maturity needed for such a treatment. They are sufficiently self-contained to be accessible to more than just the intimate specialists of the subject, and sufficiently comprehensive to remain valuable references for many years. Besides the current state of knowledge in its field, an SMM volume should ideally describe its relevance to and interaction with neighbouring fields of mathematics, and give pointers to future directions of research.

More information about this series at http://www.springer.com/series/3733

Inder Bir Singh Passi · Mahender Singh
Manoj Kumar Yadav

Automorphisms of Finite Groups

Springer

Inder Bir Singh Passi
Centre for Advanced Study
in Mathematics
Panjab University
Chandigarh, India

Mahender Singh
Department of Mathematical Sciences
Indian Institute of Science Education
and Research, Mohali
SAS Nagar, Punjab, India

Manoj Kumar Yadav
School of Mathematics
Harish-Chandra Research Institute HBNI
Jhunsi Allahabad, Uttar Pradesh, India

ISSN 1439-7382 ISSN 2196-9922 (electronic)
Springer Monographs in Mathematics
ISBN 978-981-13-2894-7 ISBN 978-981-13-2895-4 (eBook)
https://doi.org/10.1007/978-981-13-2895-4

Library of Congress Control Number: 2018957651

AMS Subject Classification (2010): 20D45, 20J05, 20D15, 20E18

This Springer imprint is published by the registered company Springer Nature Singapore Pte Ltd.
The registered company address is: 152 Beach Road, #21-01/04 Gateway East, Singapore 189721, Singapore

Preface

In mathematics, the theory of groups is a basic tool for the study of symmetries of objects. From this point of view, the symmetries of a group G itself are encoded in the automorphism group $\mathrm{Aut}(G)$ of G. Thus, the automorphism groups of finite groups are of fundamental interest in the study of the theory of groups. Since finite groups are in abundance, a complete exposition of all aspects of automorphism groups of finite groups is not feasible in a single volume. Thus, exposition of developments according to a specific theme is highly justifiable. The purpose of this monograph is to present developments on the relationship between orders of finite groups and those of their automorphism groups.

It is clear that the automorphism group of a finite group is finite. Therefore, it is natural to look for a relationship between the order $|G|$ of the group G and the order $|\mathrm{Aut}(G)|$ of its automorphism group $\mathrm{Aut}(G)$. Over the years, this has been studied extensively. The first-known result regarding this problem is due to Frobenius [36], an exposition of which is also available in [16, pp. 250–252], where it is shown that the order of G controls the orders of the elements in $\mathrm{Aut}(G)$. Birkhoff and Hall [12] proved that $|\mathrm{Aut}(G)|$ is always a divisor of $|\mathrm{Aut}(E)||G|^{r-1}$, where r is the number of distinct prime divisors of $|G|$ and E is the elementary abelian group of order $|G|$. In the direction of a lower bound on $|\mathrm{Aut}(G)|$, Hilton [58] proved that if G is a finite abelian group such that p^n divides $|G|$, p prime, then $p^{n-1}(p-1)$ divides $|\mathrm{Aut}(G)|$. Continuing this line of investigation, Herstein and Adney [55] proved that if G is any finite group such that p^2 divides $|G|$, then p divides $|\mathrm{Aut}(G)|$. In 1954, Scott [114] proved that if p^3 divides $|G|$, then p^2 divides $|\mathrm{Aut}(G)|$. With these results as motivation, Scott [114] conjectured that a finite group has at least a prescribed number of automorphisms if the order of the group is sufficiently large. The local version of the conjecture is as follows:

There exists a function $f : \mathbb{N} \to \mathbb{N}$ such that, for each $h \in \mathbb{N}$ and each prime p, if G is any finite group such that $p^{f(h)}$ divides $|G|$, then p^h divides $|\mathrm{Aut}(G)|$.

In 1956, Ledermann and Neumann [80, 81] confirmed the above conjecture by constructing a cubic polynomial function with the desired properties, using extension theory of groups and bounds on the order of Schur multiplier of finite groups. We, henceforth, refer to the above statement as Ledermann–Neumann theorem. Green [49] improved previously known bounds on the order of Schur multiplier of finite p-groups and, using it together with the standard factorization of 2-cocycle associated to a central extension of groups, refined the functional bound of Ledermann–Neumann theorem to a quadratic polynomial function. Howarth [63] and Hyde [68] further improved this quadratic polynomial function by deriving new bounds on the order of the group of central automorphisms. One of the aims of the monograph is to give an exposition of these works. We have chosen to present the various improvements rather than just the best-known results in view of the new group-theoretic results of independent interest obtained in the course of improving the bound.

It is natural to ask whether the function f can be bounded from below. Hyde [68] provided an answer to this question by showing that the least function f such that $|\mathrm{Aut}(G)|_p \geq p^h$ whenever $|G|_p \geq p^{f(h)}$ satisfies $f(h) \geq 2h - 1$. One might wonder whether this bound can be further lowered down if we restrict ourselves to the class of finite p-groups.

For every group G, the subset $\mathrm{Inn}(G)$ consisting of all inner automorphisms of G is a normal subgroup of $\mathrm{Aut}(G)$. Thus, we can construct the quotient $\mathrm{Aut}(G)/\mathrm{Inn}(G)$, denoted by $\mathrm{Out}(G)$, and called the group of outer automorphisms of G. It seems that Schenkman [108] was the first to ask the following question:

Does every non-abelian finite p-group admit a non-inner automorphism of prime power order?

In the same paper, he claimed a much stronger statement for groups of nilpotency class 2: Namely, if G is a finite p-group of nilpotency class 2, then $|G|$ divides $|\mathrm{Aut}(G)|$. Unfortunately, there remained a gap in his proof. A correct proof of the preceding statement was later given by Faudree [33]. The question was answered in full generality by Gaschütz [40] in 1966. Using cohomological methods, he proved that if G is a finite p-group of order at least p^2, then p divides $|\mathrm{Out}(G)|$. Thus, if a non-abelian group G is of order p^n and its center $\mathrm{Z}(G)$ is of order p, then by the preceding result of Gaschütz, $|G|$ divides $|\mathrm{Aut}(G)|$. In the same year, Otto [98], motivated by the functional bounds due to Herstein and Adney [55] and Scott [114], proved that if G is a non-cyclic finite abelian p-group of order greater than p^2, then $|G|$ divides $|\mathrm{Aut}(G)|$. By this time, the following problem, which was later also recorded in [89, Problem 12.77], became well known.

Divisibility Problem: *Does the order of a non-cyclic finite p-group G of order greater than p^2 divide the order of its automorphism group* $\mathrm{Aut}(G)$*?*

Notice that Divisibility Problem can also be thought of as a question whether for all non-cyclic finite p-groups G, the identity function f on $\mathbb{N}\backslash\{1,2\}$ satisfies the property that, for each $h \in \mathbb{N}\backslash\{1,2\}$, if $p^{f(h)}$ divides $|G|$, then p^h divides $|\mathrm{Aut}(G)|$.

One of the first reductions for Divisibility Problem was given by Otto [98], who showed that it is enough to consider purely non-abelian p-groups (recall that a group is said to be *purely non-abelian* if it does not admit a nontrivial abelian direct factor). Buckley [14] reduced the problem further by showing that we can restrict our attention to only those finite p-groups for which the center $\mathrm{Z}(G)$ is contained in the Frattini subgroup $\Phi(G)$ of G. It has since been proved that the problem has an affirmative solution for many special classes of non-cyclic finite p-groups, for example p-groups with metacyclic central quotient [18], modular p-groups [22], p-abelian p-groups [19], groups with small central quotient [20], groups with cyclic Frattini subgroup [30], groups of order p^7 [41], and groups of coclass 2 [35]. Using techniques from coclass theory, Eick [26] showed that, for all but finitely many 2-groups of a given coclass, the problem has an affirmative solution.

It is worth pointing out that the main ingredient in the solution of Divisibility Problem for groups G in various classes is the subgroup

$$\mathrm{IC}(G) := \mathrm{Inn}(G)\mathrm{Autcent}(G)$$

of the automorphism group $\mathrm{Aut}(G)$ of G, where

$$\mathrm{Autcent}(G) = \{\phi \in \mathrm{Aut}(G) \mid x^{-1}\phi(x) \in \mathrm{Z}(G) \text{ for all } x \in G\},$$

the group of central automorphisms of G.

In 2015, it was shown by González-Sánchez and Jaikin-Zapirain [46], making an extensive use of pro-p-techniques, that there exist non-cyclic finite p-groups of order greater than p^2 for which $|G|$ does not divide $|\mathrm{Aut}(G)|$. We present a detailed exposition of this important development in the theory of automorphism groups. However, it is still intriguing to know for what other classes of non-cyclic finite p-groups the problem has an affirmative solution and to construct explicit counterexamples.

In view of the existence of counterexamples to Divisibility Problem, it is reasonable to introduce the following property:

A non-cyclic finite p-group G of order greater than p^2 is said to have Divisibility Property if $|G|$ divides $|\mathrm{Aut}(G)|$.

Determining all finite p-groups admitting Divisibility Property continues to be a challenging problem.

Another fundamental problem in the study of automorphism groups of finite groups is the following extension and lifting problem for automorphisms of groups.

If $\mathcal{E} : 1 \to N \to G \to H \to 1$ is a short exact sequence of groups, then under what conditions does an automorphism of N extend to an automorphism of G and analogously when does an automorphism of H lift to an automorphism of G?

A crucial role in the investigation of this problem has been played by an exact sequence due to Wells [126] relating derivations, automorphisms, and second cohomology groups of groups under consideration. Let

$$\alpha : H \to \mathrm{Out}(N)$$

be the coupling associated to the extension $\mathcal{E}$ (see Sect. 2.2 of Chap. 2 for definition). The coupling α leads to an H-module structure on the center $\mathrm{Z}(N)$ of N. Let $\mathrm{Der}(H, \mathrm{Z}(N))$ be the group of derivations from H to $\mathrm{Z}(N)$, $\mathrm{Aut}_N(G)$ the group of automorphisms of G normalizing N (keeping N invariant as a set),

$$C_\alpha = \{(\phi, \theta) \in \mathrm{Aut}(H) \times \mathrm{Aut}(N) \mid \bar{\theta}\,\alpha(x)\,\bar{\theta}^{-1} = \alpha(\phi(x)) \,\text{for all}\, x \in H\},$$

and $\mathrm{H}^2(H,\ \mathrm{Z}(N))$ the second cohomology of H with coefficients in $\mathrm{Z}(N)$, where $\bar{\theta} = \mathrm{Inn}(N)\theta \in \mathrm{Out}(N)$. With the foregoing setting, Wells derived the following fundamental exact sequence, which we refer to as Wells exact sequence throughout the monograph:

$$1 \to \mathrm{Der}(H,\ \mathrm{Z}(N)) \to \mathrm{Aut}_N(G) \to C_\alpha \to \mathrm{H}^2(H,\ \mathrm{Z}(N)).$$

Wells exact sequence also turned out to be very useful, as we will see, in the study of the relationship between the order of a finite group and the order of its automorphism group. Notably, Wells exact sequence is used in Sect. 4.1 of Chap. 4 to obtain a reduction of Divisibility Problem for finite p-groups to the case when $\mathrm{Z}(G) \leq \Phi(G)$. Another instance of an extensive use of Wells exact sequence is in Sect. 5.3 of Chap. 5 for estimating $|\mathrm{Aut}_N(G)|$ for 2-groups G. Notice that the exactness of Wells sequence at C_α is equivalent to saying that a pair of automorphisms in C_α is induced by an automorphism in $\mathrm{Aut}_N(G)$ if and only if the cohomology class corresponding to the pair vanishes. This fact is used in many instances throughout the monograph to extend certain automorphism of N to an automorphism of G, for instance, Sects. 3.3 and 3.4 in Chap. 3 and Sect. 5.4 in Chap. 5.

Expositions of Wells exact sequence have appeared in the literature a couple of times, for example, by Robinson [104, 105] and recently by Dietz [23]. The extension and lifting problem for automorphisms has been investigated using Wells exact sequence by Jin [73], Passi, Singh and Yadav [99], and Robinson [106, 107]. In the monograph, we give a thorough exposition of Wells exact sequence following its construction due to Jin-Liu [74], along with some applications.

The monograph is broadly divided into three parts. The first part is an exposition of Wells exact sequence including some of its applications. The second part is an exposition of various developments on the functional bound. The final part presents the works on Divisibility Property of finite p-groups culminating in the existence of groups without this property.

In Chap. 1, we discuss the basic results on p-groups that are used in subsequent chapters of the monograph.

In Chap. 2, we begin with basic notions from group cohomology and extension theory of groups leading to the construction of the fundamental exact sequence of Wells. We also discuss some ramifications of Wells exact sequence, followed by a characterization of extensions with trivial coupling in terms of central products of groups. We conclude the chapter with applications of Wells exact sequence in the extension and lifting problem for automorphisms of finite groups.

In Chap. 3, starting with basic results on Schur multiplier of finite groups, we present the Ledermann–Neumann theorem giving a cubic polynomial function and its subsequent refinements to quadratic polynomial functions. In particular, an affirmative solution of Divisibility Problem for non-cyclic abelian p-groups is derived.

In Chap. 4, we take up the study of groups admitting Divisibility Property and first present some general reduction results allowing us to work in a smaller class of finite p-groups, namely the class of purely non-abelian finite p-groups. We then discuss Divisibility Property for (i) p-groups of nilpotency class 2, (ii) p-groups with metacyclic central quotient, (iii) modular p-groups, (iv) p-abelian p-groups, and (v) p-groups with small central quotient.

In Chap. 5, we continue our study of Divisibility Property and examine it for (i) p-groups of order p^7, (ii) p-groups of coclass 2, (iii) p-groups of a given coclass, and (iv) p^2-abelian p-central p-groups. Finally, we present results for some other classes of groups under some rather strong conditions, including p-groups with cyclic Frattini subgroup.

In Chap. 6, which is of slightly different flavor, we present the existence of groups without Divisibility Property using Lie theory and pro-p-techniques.

The monograph is aimed at researchers working in group theory; particularly, graduate students in algebra will hopefully find it useful. The primary prerequisite is an advanced course in the theory of finite groups. Section 5.3 of Chap. 5 requires familiarity with coclass theory and pro-p-groups. Additionally, Chap. 6 demands familiarity with basic analysis, topology and Lie algebras. An attempt has been made to unify various ideas developed over the years and to keep the monograph mostly self-contained. Either the results are proved or complete references are provided. Also, some problems are posed at appropriate places, more precisely Problems 2.57, 3.50, 3.88, 4.22, 4.35, 5.11, and 6.22.

We conclude with some notational setup. Throughout the monograph, we evaluate the composition of functions from right to left. For example, if $f : A \to B$ and $h : B \to C$ are two functions, then $hf(x) = h(f(x))$. The internal direct product of two subgroups H and K of a multiplicatively written group G (not necessarily abelian) is denoted by $H \oplus K$.

Acknowledgements

Inder Bir Singh Passi thanks Indian National Science Academy, New Delhi, for their support and Ashoka University, Sonipat, for making available their facilities. Mahender Singh acknowledges support from the DST INSPIRE Faculty grant and the SERB MATRICS grant. Manoj Kumar Yadav thanks the Indian Institute of Science Education and Research, Mohali for providing excellent hospitality during his visits to the Institute. Inder Bir Singh Passi and Mahender Singh thank Harish-Chandra Research Institute, Allahabad, for warm hospitality extended by the Institute during their visits. Mahender Singh and Manoj Kumar Yadav thank Dipendra Prasad for hosting them at the Tata Institute of Fundamental Research, Mumbai, for a visit while this work was in progress. The authors thank Charles Leedham-Green and Rahul D. Kitture for their useful comments. The authors are grateful to Shamim Ahmad and Krati Shrivastav from Springer for their untiring support at the production stage of the monograph.

Contents

About the Authors

Inder Bir Singh Passi is Professor Emeritus at Panjab University, Chandigarh; Honorary Professor at the Indian Institute of Science Education and Research, Mohali; Professor at Ashoka University, Sonipat; and INSA Emeritus Scientist. Earlier, he has held several academic positions including Professor at Kurukshetra University, Kurukshetra; Professor at Panjab University, Chandigarh; Visiting Professor at the University of California, Los Angeles; Universitaet Goettingen, Goettingen; and Harish-Chandra Research Institute, Allahabad. He is a recipient of the Shanti Swarup Bhatnagar Prize for Mathematical Sciences (1983), the Meghnad Saha Award for Research in Theoretical Sciences (1988), the Distinguished Service Award (2003) by Mathematical Association of India; Khosla National Award (2011) by the Indian Institute of Technology Roorkee; and Prasanta Chandra Mahalanobis Medal (2011) by the Indian National Science Academy. His research interests are in algebra, particularly in group theory and group rings. He has published/co-authored/edited more than ten books including *Group Rings and Their Augmentation Ideals* and *Lower Central and Dimension Series of Groups* (both with Springer), as well as several research papers in respected international journals, conference proceedings, and contributed volumes.

Mahender Singh is Assistant Professor at the Indian Institute of Science Education and Research, Mohali. He earned his Ph.D. in mathematics from Harish-Chandra Research Institute, Allahabad (2010). His research interests lie broadly in topology and algebra, with a focus on compact group actions on manifolds, equivariant maps, automorphisms and cohomology of groups, and quandles. He is a recipient of the INSPIRE Faculty award of the Department of Science and Technology, Government of India (2011). He has published several research papers in respected international journals, conference proceedings, and contributed volumes.

Manoj Kumar Yadav is Professor at the Harish-Chandra Research Institute, Allahabad. He received his Ph.D. in mathematics from Kurukshetra University, Haryana (2002). He is a recipient of the Indian National Science Academy Medal for Young Scientists (2009) and the Department of Science and Technology, Science and Engineering Research Council (SERC), fellowship Fast Track Scheme for Young Scientists (2005). He is a member of the National Academy of Sciences, India (NASI). His research interests lie in group theory, particularly the automorphisms, conjugacy classes, and Schur multipliers of groups. He has published several research papers in respected international journals, conference proceedings, and contributed volumes.

Notation

$\mathbb{N}$	Set of natural numbers
$\mathbb{Z}$	Ring of integers
$\mathbb{Q}$	Field of rational numbers
$\mathbb{C}$	Field of complex numbers
$\mathbb{C}^{\times}$	Multiplicative group of nonzero complex numbers
$\mathbb{F}_q$	Finite field with q-elements
$\mathbb{Z}_p$	Ring of p-adic integers
$\mathbb{Q}_p$	Field of p-adic numbers
$\lfloor x \rfloor$	Greatest integer less than or equal to the number x
$\lceil x \rceil$	Smallest integer greater than or equal to the number x
n_p	Highest power of p that divides n
(a, b)	Greatest common divisor of integers a and b
φ	Euler's totient function
$f\vert_A$	Restriction of the map f on a subset A of its domain
C_n	Cyclic group of order n
$\mathbb{Z}/n\mathbb{Z}$	Cyclic group of integers modulo n
Σ_n	Symmetric group on n symbols
$\exp(G)$	Exponent of G
$d(G)$	Minimum number of generators of G
$\langle X \rangle$	Subgroup of a group G generated by a subset X
HK	$\{hk \mid h \in H,\ k \in k\}$, where H and K are subgroups of a group G
$\mathrm{cc}(G)$	Coclass of G
$\lvert G \rvert$	Order of G
$\lvert g \rvert$	Order of $g \in G$ or equivalently $\lvert \langle g \rangle \rvert$
$\mathrm{Ker}(\phi)$	Kernel of the group homomorphism $\phi : G \to H$
$\mathrm{Im}(\phi)$	Image of the group homomorphism $\phi : G \to H$
$^{\phi}x$	Image of $x \in X$ under the map $\phi : X \to Y$
^{G}x	Conjugacy class of x in G
$H \leq G$	H is a subgroup of G
$H < G$	H is a proper subgroup of G

$\lvert G:H \rvert$	Index of the subgroup H in G
$N \trianglelefteq G$	N is a normal subgroup of G
$N \triangleleft G$	N is a proper normal subgroup of G
$X \backslash Y$	Set of elements of X which are not in Y
$[x_1, x_2]$	Commutator $x_1x_2x_1^{-1}x_2^{-1}$
$[x_1, \ldots, x_n]$	$[\ldots[[x_1, x_2], x_3], \ldots, x_n]$ the left-normed commutator of $x_1, \ldots, x_n$
$[H, K]$	Subgroup of G generated by $\{[h,k] \mid h \in H \, and \, k \in K\}$, where H and K are subgroups of G
$[G, G]$	Commutator subgroup of G
$\mathrm{Z}(G)$	Center of G
$\mathrm{C}_G(H)$	Centralizer of H in G
$\mathrm{C}_G(x)$	Centralizer of $\langle x \rangle$ in G
$\mathrm{N}_G(H)$	Normalizer of H in G
$\gamma_n(G)$	nth term of the lower central series of G; in particular, $\gamma_2(G) = [G, G]$
$\mathrm{Z}_n(G)$	nth term of the upper central series of G; in particular, $\mathrm{Z}_1(G) = \mathrm{Z}(G)$
$\Omega_n(G)$	$\left\langle x \in G \mid x^{p^n} = 1 \right\rangle$
$\mho_n(G)$	$\left\langle x^{p^n} \mid x \in G \right\rangle$
A_p	Unique Sylow p-subgroup of the abelian group A
$\Phi(G)$	Frattini subgroup of G
$\mathrm{Aut}(G)$	Group of automorphisms of G
$\mathrm{Inn}(G)$	Group of inner automorphisms of G
$\mathrm{Out}(G)$	$\mathrm{Aut}(G)/\mathrm{Inn}(G)$
$\mathrm{Aut}^H(G)$	Group of automorphisms of G which centralize the subgroup H (i.e., act as identity automorphism on H) or in case H is a quotient group of G, induce identity on H
$\mathrm{Aut}_H(G)$	Group of automorphisms of G which normalize the subgroup H (i.e., keep H invariant as a set)
$\mathrm{Aut}_K^H(G)$	$\mathrm{Aut}_K(G) \cap \mathrm{Aut}^H(G)$
$\mathrm{Aut}^{K,H}(G)$	$\mathrm{Aut}^K(G) \cap \mathrm{Aut}^H(G)$
$\mathrm{Autcent}(G)$	$\{\phi \in \mathrm{Aut}(G) \mid x^{-1}\phi(x) \in \mathrm{Z}(G) \, \mathrm{for\,all} \, x \in G\}$ or equivalently $\mathrm{Aut}^{G/\mathrm{Z}(G)}(G)$
$\mathrm{C}_{\mathrm{Out}(G)}(\mathrm{Z}(G))$	$\mathrm{Aut}^{\mathrm{Z}(G)}(G)/\mathrm{Inn}(G)$
$\mathrm{IC}(G)$	$\mathrm{Inn}(G)\mathrm{Autcent}(G)$
ι_x	Inner automorphism of G induced by $x \in G$
X^G	$\{x \in X \mid {}^g x = x \, \mathrm{for\,all} \, g \in G\}$, the fixed-point set of G-action on X
G_x	$\{g \in G \mid {}^g x = x\}$, the stabilizer subgroup of G at $x \in X$
$G \oplus H$	Direct product of G and H
$\oplus_i G_i$	Direct product of the family $\{G_i\}$
$X \times Y$	Cartesian product of X and Y
$\prod_i X_i$	Cartesian product of the family $\{X_i\}$
$\det(A)$	Determinant of a square matrix A

$\mathrm{M}(r, R)$	Ring of $r \times r$ matrices with entries in the ring R
$\mathrm{GL}(r, R)$	Group of $r \times r$ invertible matrices with entries in the ring R
$\mathrm{O}(r, R)$	Group of $r \times r$ orthogonal matrices with entries in the ring R
$\mathrm{UT}(r, R)$	Group of $r \times r$ upper unitriangular matrices with entries in the ring R
$\mathcal{M}(G)$	Schur multiplier of G
$R[[X]]$	Ring of formal power series in X with coefficients in the ring R
$R[G]$	Group algebra of G over the ring R
$\mathbb{Z}_p[[G]]$	Completed group algebra of a pro-p-group G over the ring $\mathbb{Z}_p$
$I_R(G)$	Augmentation ideal of the group algebra $R[G]$
$\mathrm{Der}(G, A)$	Group of derivations from G to A, where A is a G-module
$\mathrm{Der}(L)$	Derivation algebra of the Lie algebra L
$\mathrm{InnDer}(L)$	Inner derivation algebra of the Lie algebra L
$\mathrm{H}^n(G, A)$	nth cohomology of G with coefficients in the G-module A
$\mathrm{H}^n_{cts}(G, A)$	nth continuous cohomology of the topological group G with coefficients in the topological G-module A
$\mathrm{H}^n_{Lie}(L, A)$	nth Lie algebra cohomology of L with coefficients in the L-module A
$\mathrm{Ext}(H, N)$	Set of equivalence classes of extensions of H by N
$\mathrm{Ext}_\alpha(H, N)$	Set of equivalence classes of extensions of H by N inducing the coupling $\alpha : H \to \mathrm{Out}(N)$
$\Lambda^k L$	kth exterior power of the Lie algebra L
$\mathrm{Hom}(G, A)$	Group of homomorphisms from G to the abelian group A
$\mathrm{Hom}_R(M, N)$	Module of R-module homomorphisms from M to N
$\mathrm{End}_R(M)$	Algebra of R-module endomorphisms of M
$\widehat{G}$	Character group $\mathrm{Hom}(G, \mathbb{C}^\times)$ of G
$M \otimes_R N$	Tensor product of R-modules M and N

Chapter 1
Preliminaries on p-Groups

This chapter is a collection of some basic results in the theory of p-groups. Beginning with central series of groups, we discuss regular p-groups and present some numerical results on p-groups with large centers. We then present a generalization of a theorem of Gaschütz, and conlude the chapter with a quick review of pro-p-groups and coclass graphs.

1.1 Central Series

Given a group G, and its subgroup H, the *centralizer* of H in G is the subgroup of G defined by setting

$$\mathrm{C}_G(H) = \left\{g \in G \mid ghg^{-1} = h \text{ for all } h \in H\right\}.$$

If H is a normal subgroup of G, then so is $\mathrm{C}_G(H)$. The centralizer of G in G itself is called the *center* of G, and we denote it by $\mathrm{Z}(G)$.

A *central series* of G is an ascending series

$$1 = G_0 \leq G_1 \leq \cdots \leq G_i \leq \cdots$$

of normal subgroups G_i of G such that

$$G_{i+1}/G_i \leq \mathrm{Z}(G/G_i).$$

There are two extreme central series, namely, the lower and the upper central series, which are fundamental in group theory.

Let G be a group and $x, y \in G$. Then

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

is called the *commutator* of x and y. In general, given elements $x_1, \ldots, x_n \in G$,

I. B. S. Passi et al., *Automorphisms of Finite Groups*, Springer Monographs
in Mathematics, https://doi.org/10.1007/978-981-13-2895-4_1

$$[x_1, \ldots, x_n] := [\ldots[[x_1, x_2], x_3], \ldots, x_n],$$

is called the *left-normed commutator* of $x_1, \ldots, x_n$. For two subgroups H and K of G, we define

$$[H, K] = \big\langle [h, k] \mid h \in H,\ k \in K \big\rangle,$$

the commutator of H and K. If both H and K are normal subgroups of G, then so is $[H, K]$. Further, if $H = K$, then $[H, H]$ is called the *commutator subgroup* of H.

Set $\gamma_1(G) = G$. We define a descending series

$$G = \gamma_1(G) \geq \gamma_2(G) \geq \cdots \geq \gamma_i(G) \geq \cdots$$

of normal subgroups of G, recursively for $i \geq 1$, by setting

$$\gamma_{i+1}(G) = [\gamma_i(G), G];$$

this series is called the *lower central series* of G. If $\gamma_i(G) = 1$ for some integer i, then G is called a *nilpotent group*. A nilpotent group G is said to be of *nilpotency class c* if $\gamma_{c+1}(G) = 1$ but $\gamma_c(G) \neq 1$.

The ascending series

$$1 = \mathrm{Z}_0(G) \leq \mathrm{Z}_1(G) \leq \cdots \leq \mathrm{Z}_i(G) \leq \cdots$$

of normal subgroups of G, where $\mathrm{Z}_{i+1}(G)$ is such that

$$\mathrm{Z}_{i+1}(G)/\mathrm{Z}_i(G) = \mathrm{Z}\big(G/\mathrm{Z}_i(G)\big),$$

is called the *upper central series* of G.

Exercise 1.1 Let $1 = G_0 \leq G_1 \leq \cdots \leq G_i \leq \cdots$ be a central series of a group G. Then the following statements hold:

(1) $G_i \leq \mathrm{Z}_i(G)$ for all i.

(2) If G is a nilpotent group with nilpotency class c, then $\gamma_i(G) \leq G_{c-i+1}$. Moreover, $[\gamma_i(G), \mathrm{Z}_i(G)] = 1$ for $i \geq 1$.

(3) For $i \geq 2$, $\gamma_i(G) = 1$ if and only if $\mathrm{Z}_{i-1}(G) = G$.

Exercise 1.2 Let G be a finite nilpotent group with nilpotency class c and N a normal subgroup of G such that $N < \mathrm{Z}(G)$. If $\mathrm{Z}(G/N) = \mathrm{Z}(G)/N$, then $\mathrm{Z}_i(G/N) = \mathrm{Z}_i(G)/N$ for all $1 \leq i \leq c$.

Let G be a group and H a subgroup of G of finite index, say n. Let $\{x_1, \ldots, x_n\}$ be a set of representatives of the right cosets of H in G. Then, for $g \in G$, we have

$$Hx_i g = Hx_{g(i)},$$

where the map $i \mapsto g(i)$ is a permutation of the set $\{1, \ldots, n\}$. Consequently, the element $x_i g x_{g(i)}^{-1} \in H$ for all $g \in G$. Let A be an abelian group, and $\theta : H \to A$ be a group homomorphism. Then the *transfer* of θ is the map

$$\theta^* : G \to A$$

given by

$$\theta^*(g) = \prod_{i=1}^{n} \theta\big(x_i g x_{g(i)}^{-1}\big) \tag{1.3}$$

for $g \in G$. It is not difficult to see that the map θ^* does not depend on the choice of the coset representatives and is a group homomorphism. We need the following basic result [103, 10.1.3].

Proposition 1.4 *Let G be a finite group and $H \leq \mathrm{Z}(G)$ with $|G/H| = n$. Then the transfer of the identity homomorphism $\mathrm{id}_H : H \to H$ is the map $x \mapsto x^n$.*

Now we concentrate on finite p-groups. The following result is due to Exarchakos [30].

Proposition 1.5 *Let G be a finite p-group. Then*

$$\exp\big(\gamma_{i+1}(G)/\gamma_{i+2}(G)\big) \leq |\gamma_i(G)/\big(\mathrm{Z}(G) \cap \gamma_i(G)\big)|$$

for all $i \geq 1$.

Proof Let $|\gamma_i(G)/\big(\mathrm{Z}(G) \cap \gamma_i(G)\big)| = p^r$. Since $\mathrm{Z}(G) \cap \gamma_i(G)$ is a central subgroup of $\gamma_i(G)$, by Proposition 1.4, the transfer homomorphism

$$\tau : \gamma_i(G) \to \mathrm{Z}(G) \cap \gamma_i(G)$$

is given by $x \mapsto x^{p^r}$. Let $x \in \gamma_i(G)$ and $y \in G$. Then $[x^{p^r}, y] = 1$, and therefore

$$[x, y]^{p^r} = \tau\big([x, y]\big) = \tau(xyx^{-1}y^{-1}) = \tau(x)\tau(yx^{-1}y^{-1}) = x^{p^r} y x^{-p^r} y^{-1} = 1.$$

Hence, $\exp\big(\gamma_{i+1}(G)/\gamma_{i+2}(G)\big) \leq p^r$. □

The next result is due to Gallian [37, Theorem 2.1].

Proposition 1.6 *Let G be a p-group of nilpotency class c with $\gamma_i(G)/\gamma_{i+1}(G)$ cyclic of order p^r for all $2 \leq i \leq c$. Then*

$$\mathrm{Z}_i(G) \cap \gamma_{c-i}(G) = \gamma_{c-i+1}(G)$$

for all $0 \leq i \leq c - 2$.

Proof Since, by Exercise 1.1, $\gamma_{c-i+1}(G) \leq Z_i(G)$, it follows that

$$\gamma_{c-i+1}(G) \leq Z_i(G) \cap \gamma_{c-i}(G)$$

for all $0 \leq i \leq c-2$. We only need to prove the reverse inclusion. The result is obvious for $i = 0$. Now we proceed by induction on $i \geq 1$. For $i = 1$, $\gamma_c(G) \leq Z(G) \cap \gamma_{c-1}(G) \leq \gamma_{c-1}(G)$. By Proposition 1.5, we have

$$p^r = |\gamma_c(G)| = \exp\big(\gamma_c(G)\big) \leq \frac{|\gamma_{c-1}(G)|}{|\,Z(G) \cap \gamma_{c-1}(G)|} \leq \frac{|\gamma_{c-1}(G)|}{|\gamma_c(G)|} = p^r.$$

Consequently, $Z(G) \cap \gamma_{c-1}(G) = \gamma_c(G)$, and hence the result holds for $i = 1$.

Suppose that $Z_i(G) \cap \gamma_{c-i}(G) \leq \gamma_{c-i+1}(G)$ for some $i \geq 1$. For a subgroup H of G, let H^* denote the image of H under the natural homomorphism

$$G \to G/\gamma_{c-i+1}(G).$$

Since

$$[G, Z_{i+1}(G) \cap \gamma_{c-i-1}(G)] \leq Z_i(G) \cap \gamma_{c-i}(G) = \gamma_{c-i+1}(G),$$

it follows that

$$\big(Z_{i+1}(G) \cap \gamma_{c-i-1}(G)\big)^* \leq Z_{i+1}(G^*) \cap \gamma_{c-i-1}(G^*).$$

Since G^* has nilpotency class $c-i$ and factors of successive terms of its lower central series are cyclic of order p^r, we have

$$Z_{i+1}(G^*) \cap \gamma_{c-i-1}(G^*) = \gamma_{c-i}(G^*) = \big(\gamma_{c-i}(G)\big)^*.$$

Hence, $Z_{i+1}(G) \cap \gamma_{c-i-1}(G) \leq \gamma_{c-i}(G)$, and the proof is complete. □

For a finite group G, the *Frattini subgroup* of G, denoted by $\Phi(G)$, is defined as the intersection of all maximal subgroups of G. The product of two subgroups H, K of a group G is defined as

$$HK = \{hk \mid h \in H, k \in K\}.$$

Notice that HK is not a subgroup of G in general; however, if $HK = KH$, then it is a subgroup. In [70], Itô proved the following result (see [56, 61, 94] for some generalizations).

Proposition 1.7 *Let G be a finite p-group and H a proper subgroup of G. If $\gamma_2(H) < \gamma_2(G)$, then $\gamma_2\big(H\Phi(G)\big) < \gamma_2(G)$.*

Proof The proof is by induction on $|G : H|$ and $|G|$. Notice that the result holds for all non-abelian p-groups of order p^3. Suppose that the result is true for all groups with order smaller than $|G|$.

First assume that $\gamma_2(G) \leq H$, which implies that H is normal in G. If $\gamma_2(H) \neq 1$, then $\gamma_2\big(H\Phi(G)\big) < \gamma_2(G)$ by the induction hypothesis, since $\Phi\big(G/\gamma_2(H)\big) = \Phi(G)/\gamma_2(H)$ and $|G/\gamma_2(H)| < |G|$. Thus, we can assume that $\gamma_2(H) = 1$, that is, H is abelian. If $|\gamma_2(G)| \geq p^2$, then there exists a central subgroup C of order p contained in $\gamma_2(G)$ and G/C is non-abelian. Since $\Phi(G/C) = \Phi(G)/C$ and $|G/C| < |G|$, it follows that $\gamma_2\big(H\Phi(G)\big) < \gamma_2(G)$ by the induction hypothesis. If $|\gamma_2(G)| = p$, then G has nilpotency class 2, and therefore $\langle g^p \mid g \in G\rangle \leq \mathrm{Z}(G)$. Hence, $\Phi(G) \leq \mathrm{Z}(G)$, and consequently $H\Phi(G)$ is abelian.

If L is a subgroup of G of maximal order such that $\gamma_2(L) < \gamma_2(G)$, then $\gamma_2(G) < L$. For, otherwise $L < L\gamma_2(G)$, and therefore $L\gamma_2(G)$ contains a subgroup M containing L such that $|M/L| = p$. As L is normal in M, it follows that $\gamma_2(M) \leq L$. Notice that $\gamma_2(M) < \gamma_2(G)$, which is a contradiction to the maximality of the order of L. Consequently, by the preceding paragraph, we get $\gamma_2\big(L\Phi(G)\big) < \gamma_2(G)$. Thus, we can assume that the result is true for all subgroups L of G such that $|G : L| < |G : H|$.

Now consider the case when H does not contain $\gamma_2(G)$. Then, as in the preceding paragraph, $H\gamma_2(G)$ contains a subgroup K containing H such that $|G : K| < |G : H|$ and $\gamma_2(K) < \gamma_2(G)$. Hence, by the induction hypothesis, it follows that $\gamma_2\big(K\Phi(G)\big) < \gamma_2(G)$. Since $\gamma_2\big(H\Phi(G)\big) \leq \gamma_2\big(K\Phi(G)\big)$, we obtain $\gamma_2\big(H\Phi(G)\big) < \gamma_2(G)$, which completes the proof. □

A group G is said to be *metabelian* if it admits an abelian normal subgroup N such that the quotient group G/N is abelian. The results in the following proposition are well-known, and proofs can be found, for example, in [66, Chapter III].

Proposition 1.8 *Let G be a finite p-group of nilpotency class $c > 1$. Then the following statements hold:*

(1) $\exp\big(\mathrm{Z}_{i+1}(G)/\mathrm{Z}_i(G)\big)$ *is a non-increasing function of i.*

(2) $\exp\big(\gamma_i(G)/\gamma_{i+1}(G)\big)$ *is a non-increasing function of i.*

(3) $|G/\big(\mathrm{Z}_{c-1}(G)\Phi(G)\big)| \geq p^2$.

(4) *$G/\mathrm{Z}_{c-1}(G)$ has two independent generators of the same order.*

(5) *If G is generated by 2 elements and of nilpotency class at most 4, then G is metabelian.*

(6) *If $p > 2$ and $\mathrm{Z}_2(G)$ is cyclic, then G is cyclic.*

The following interesting result is due to Wiegold [127].

Theorem 1.9 *Let p be a prime and G a group such that $|G/\mathrm{Z}(G)| = p^r$. Then $\gamma_2(G)$ is a p-group with $|\gamma_2(G)| \leq p^{\frac{r(r-1)}{2}}$.*

Proof The proof is by induction on r. The result is obvious for $r \leq 1$. So we assume that $|G/\mathrm{Z}(G)| = p^r \geq p^2$. Let $x \in \mathrm{Z}_2(G) \setminus \mathrm{Z}(G)$, and set $H = G/N$, where

$$N = \langle [x, g] \mid g \in G\rangle = \{[x, g] \mid g \in G\}.$$

Notice that $\mathrm{Z}(G)/N \leq \mathrm{Z}(H)$ and $Nx \in \mathrm{Z}(H)$; for, $[Nx,\ Ng] = N[x, g] = N$ for all $g \in G$. Since x is not central, $Nx \notin \mathrm{Z}(G)/N$, and hence $|H/\mathrm{Z}(H)| = p^s$ for some $s < r$. Thus, by induction,

$$|\gamma_2(H)| \leq p^{\frac{(r-1)(r-2)}{2}}.$$

Since $\mathrm{Z}(G) < \mathrm{C}_G(x)$, we have

$$|N| = |G|/|\,\mathrm{C}_G(x)| < |G/\mathrm{Z}(G)| = p^r.$$

Using the fact that $\gamma_2(G)/N = \gamma_2(H)$, we obtain

$$|\gamma_2(G)| = |N|\,|\gamma_2(H)| \leq p^{\frac{r(r-1)}{2}},$$

which completes the proof. □

For a finite p-group G, define

$$\Omega_i(G) = \left\langle g \in G \mid g^{p^i} = 1 \right\rangle$$

and

$$\mho_i(G) = \left\langle g^{p^i} \mid g \in G \right\rangle$$

for each integer $i \geq 1$. Observe that both $\Omega_i(G)$ and $\mho_i(G)$ are characteristic subgroups of G.

A group G is said to be *metacyclic* if it admits a cyclic normal subgroup N such that G/N is cyclic. For example, groups of order p^3 and exponent p^2 are metacyclic.

The following result is useful [66, III.11.4 Satz].

Proposition 1.10 *Let G be a finite p-group, where p is an odd prime. If $|G/\mho_1(G)| \leq p^2$, then G is metacyclic.*

Let H be a normal subgroup of a group G. Then the pair (G, H) is called a *Camina pair* if

$$Hx \subseteq {}^G x$$

for all $x \in G \setminus H$, where

$${}^G x := \{gxg^{-1} \mid g \in G\}$$

denotes the *conjugacy class* of x in G. For example, the pair $\big(G, \gamma_2(G)\big)$, where G is an extraspecial p-group, is a Camina pair. Recall that, a finite p-group is said to be *extraspecial* if $\gamma_2(G) = \mathrm{Z}(G) = \Phi(G)$ is of order p.

With the preceding definition, we present the following result of Macdonald [84, Lemma 2.1, Theorem 2.2].

Proposition 1.11 *Let G be a finite p-group of nilpotency class c and H a normal subgroup of G such that (G, H) is a Camina pair. Then the following statements hold:*

(1) $H = \mathrm{Z}_{c-r+1}(G) = \gamma_r(G)$ *for some* $2 \le r \le c$.

(2) If $H = \mathrm{Z}(G)$, *then* $\exp\big(\mathrm{Z}_r(G)/\mathrm{Z}_{r-1}(G)\big) = p$ *for all* $1 \le r \le c$.

Proof By the definition of a Camina pair, $\mathrm{Z}(G) \le H$. If $H \ne \mathrm{Z}(G)$, then $\big(G/\mathrm{Z}(G), H/\mathrm{Z}(G)\big)$ is also a Camina pair. A repetition of the argument yields

$$H = \mathrm{Z}_{c-r+1}(G)$$

for some $2 \le r \le c$. Notice that $\mathrm{Z}_{c-r+1}(G) \ge \gamma_r(G)$. Suppose that $H = \mathrm{Z}_{c-r+1}(G) > \gamma_r(G)$. Then $\big(G/\gamma_r(G), H/\gamma_r(G)\big)$ is a Camina pair, and hence

$$\gamma_{r-1}(G)/\gamma_r(G) \le \mathrm{Z}\left(G/\gamma_r(G)\right) \le H/\gamma_r(G).$$

Consequently, $\gamma_{r-1}(G) \le H = \mathrm{Z}_{c-r+1}(G)$, which by an easy induction yields $\gamma_c(G) \le \mathrm{Z}_0(G) = 1$, a contradiction. Hence, $H = \mathrm{Z}_{c-r+1}(G) = \gamma_r(G)$ proving (1).

Suppose that $H = \mathrm{Z}(G)$. Then $(G/N, H/N)$ is a Camina pair for each proper normal subgroup N of H, and consequently $\mathrm{Z}(G/N) \le H/N$. Obviously, $H/N \le \mathrm{Z}(G/N)$, and hence $\mathrm{Z}(G/N) = \mathrm{Z}(G)/N$. Now, by taking $N = \mho_1\big(\mathrm{Z}(G)\big)$, we obtain $\mathrm{Z}\left(G/N\right) = \mathrm{Z}(G)/N$. Since $[\mathrm{Z}_2(G), G] \le \mathrm{Z}(G)$, it follows that $[\mho_1\big(\mathrm{Z}_2(G)\big), G] \le N$. Consequently, we have

$$\mho_1\big(\mathrm{Z}_2(G)\big)/N \le \mathrm{Z}(G)/N,$$

and hence $\exp\left(\mathrm{Z}_2(G)/\mathrm{Z}(G)\right) = p$. By Proposition 1.8(1), we get

$$\exp\left(\mathrm{Z}_{r+1}(G)/\mathrm{Z}_r(G)\right) = p$$

for all $r \ge 1$. In particular, $\exp\left(G/\mathrm{Z}_{c-1}(G)\right) = p$. Since, by Exercise 1.1, $[\gamma_{c-1}(G), \mathrm{Z}_{c-1}(G)] = 1$, we get $\exp\big([\gamma_{c-1}(G), G]\big) = p$. By assertion (1), we have $\mathrm{Z}(G) = \gamma_c(G)$, and the proof of assertion (2) is complete. □

We conclude this section with the following result of Yadav [128, Theorem 3.1] on Camina pairs.

Theorem 1.12 *Let G be a finite p-group such that $\big(G, \mathrm{Z}(G)\big)$ is a Camina pair. Then one of the following statements holds:*

(1) There exists a maximal subgroup M of G such that $\mathrm{Z}(M) = \mathrm{Z}(G)$.

(2) The elementary abelian groups $\mathrm{Z}_2(G)/\mathrm{Z}(G)$ *and* $G/\Phi(G)$ *have the same order.*

Proof We first prove the theorem for groups G with $|\mathrm{Z}(G)| = p$. If G has a maximal subgroup M such that $\mathrm{Z}(M) = \mathrm{Z}(G)$, then we are done. Therefore, we assume that there does not exist any maximal subgroup M of G such that $\mathrm{Z}(M) = \mathrm{Z}(G)$. By Proposition 1.11(2), $\mathrm{Z}_2(G)/\mathrm{Z}(G)$ is elementary abelian. Let M be a maximal subgroup of G and $x \in G$ such that $G = \langle M, x\rangle$. Since

$$\mathrm{Z}(G) \le \gamma_2(G) \le \Phi(G) \le M,$$

it follows that $\mathrm{Z}(G) \le \mathrm{Z}(M)$, and therefore $\mathrm{C}_G(M) = \mathrm{Z}(M)$.

We claim that $\mathrm{Z}(M) \le \mathrm{Z}_2(G)$. Let $y \in \mathrm{Z}(M)$. If $y \in \mathrm{Z}(G)$, then we are done. So let $y \notin \mathrm{Z}(G)$. Since $x^p \in \Phi(G) \le M$ and $y \in \mathrm{Z}(M)$, we get

$$[y, G] = [y, \langle M, x\rangle] = [y, \langle x\rangle]$$

and

$$|[y, \langle x\rangle]| = p.$$

By the given hypothesis $\mathrm{Z}(G) \subseteq [y, G]$. Thus, it follows that $[y, G] = \mathrm{Z}(G)$, and therefore $y \in \mathrm{Z}_2(G)$ proving our claim.

Let $y, z \in \mathrm{Z}(M) \setminus \mathrm{Z}(G)$. Then $y, z \in \mathrm{Z}_2(G) \setminus \mathrm{Z}(G)$, and therefore $[z, G] = \mathrm{Z}(G) = [y, G]$. Notice that $\mathrm{Z}(G) = [y, G] = \langle [y, x]\rangle$. Since $[z, x], [y, x] \in [z, G] = \mathrm{Z}(G)$ and $|\mathrm{Z}(G)| = p$, it follows that

$$[z, x] = [y, x]^i = [y^i, x]$$

for some i with $1 \le i < p$. Thus, $y^i z^{-1} \in \mathrm{C}_G(x)$, which implies that $y^i z^{-1} \in \mathrm{Z}(G)$, since $y^i z^{-1} \in \mathrm{Z}(M)$. Consequently,

$$\langle \mathrm{Z}(G), y\rangle = \langle \mathrm{Z}(G), z\rangle$$

and

$$|\mathrm{Z}(M)| = p\,|\mathrm{Z}(G)| = p^2.$$

We have proved that for any maximal subgroup $M/\Phi(G)$ of $G/\Phi(G)$, there exists a subgroup $Y/\mathrm{Z}(G) = \mathrm{Z}(M)/\mathrm{Z}(G)$ of $\mathrm{Z}_2(G)/\mathrm{Z}(G)$ such that $|Y/\mathrm{Z}(G)| = p$.

On the other hand, suppose that $Y'/\mathrm{Z}(G)$ is a subgroup of $\mathrm{Z}_2(G)/\mathrm{Z}(G)$ such that $|Y'/\mathrm{Z}(G)| = p$. Then $Y'/\mathrm{Z}(G)$ is cyclic, say, generated by $\mathrm{Z}(G)y'$ for some $y' \in \mathrm{Z}_2(G)$. Therefore, $\mathrm{C}_G(y')$ is a maximal subgroup M' of G, since

$$|\mathrm{C}_G(y')| = |G|/|[y', G]| = |G|/p.$$

Thus, $M'/\Phi(G)$ is a maximal subgroup of $G/\Phi(G)$ corresponding to $Y'/\mathrm{Z}(G)$, and it follows that $Y' = \mathrm{Z}(M')$. This establishes a bijection between the set of all subgroups $Y/\mathrm{Z}(G)$ of order p in $\mathrm{Z}_2(G)/\mathrm{Z}(G)$ and the set of all subgroups $M/\Phi(G)$ of index p in $G/\Phi(G)$. Since the two groups $\mathrm{Z}_2(G)/\mathrm{Z}(G)$ and $G/\Phi(G)$ are elementary abelian, the existence of such a correspondence implies that

$$\mathrm{Z}_2(G)/\mathrm{Z}(G) \cong G/\Phi(G),$$

which completes the proof when $|\mathrm{Z}(G)| = p$.

Now assume that G is a p-group with $|\mathrm{Z}(G)| \geq p^2$. Let N be a maximal subgroup of $\mathrm{Z}(G)$. Since $N < \mathrm{Z}(G)$, it follows that $\big(G/N, \mathrm{Z}(G)/N\big)$ is a Camina pair. By Proposition 1.11(1), we get $\mathrm{Z}(G/N) \leq \mathrm{Z}(G)/N$. That $\mathrm{Z}(G)/N \leq \mathrm{Z}(G/N)$ is obvious, and therefore $\big(G/N, \mathrm{Z}(G/N)\big)$ is a Camina pair. Since

$$|\mathrm{Z}(G/N)| = |\mathrm{Z}(G)/N| = p,$$

it follows from our assumption that the theorem holds for G/N. Thus, G/N satisfies one of the assertions in the statement of the theorem.

If G/N satisfies assertion (1), then it has a maximal subgroup $\overline{M}$ such that $\mathrm{Z}(\overline{M}) = \mathrm{Z}(G/N)$. Let

$$\pi : G \to G/N$$

be the natural projection. Then $\pi^{-1}(\overline{M})$ is a maximal subgroup M of G containing N such that $\pi(M) = \overline{M} = M/N$. Since $\overline{M}$ contains $\mathrm{Z}(G/N) = \mathrm{Z}(G)/N$, it follows that M contains $\mathrm{Z}(G)$. Hence, $\mathrm{Z}(G) \leq \mathrm{Z}(M)$, and we have

$$\mathrm{Z}(G)/N \leq \mathrm{Z}(M)/N \leq \mathrm{Z}(M/N) = \mathrm{Z}(G/N) = \mathrm{Z}(G)/N.$$

Thus, it follows that $\mathrm{Z}(G) = \mathrm{Z}(M)$, and hence G satisfies assertion (1).

If G/N satisfies assertion (2), then

$$|\mathrm{Z}_2(G/N)/\mathrm{Z}(G/N)| = |(G/N)/\Phi(G/N)|.$$

Since $\mathrm{Z}(G/N) = \mathrm{Z}(G)/N$, it follows by Exercise 1.2 that $\mathrm{Z}_2(G/N) = \mathrm{Z}_2(G)/N$. Hence,

$$\mathrm{Z}_2(G)/\mathrm{Z}(G) \cong \mathrm{Z}_2(G/N)/\mathrm{Z}(G/N).$$

By Proposition 1.11(1), $N \leq \mathrm{Z}(G) \leq \gamma_2(G) \leq \Phi(G)$, and we obtain $\Phi(G/N) = \Phi(G)/N$. Consequently,

$$G/\Phi(G) \cong (G/N)/\big(\Phi(G)/N\big) = (G/N)/\Phi(G/N).$$

Since

$$|\mathrm{Z}_2(G)/\mathrm{Z}(G)| = |\mathrm{Z}_2(G/N)/\mathrm{Z}(G/N)| = |(G/N)/\Phi(G/N)| = |G/\Phi(G)|,$$

it follows that G satisfies assertion (2), and the proof is complete. □

1.2 Regular Groups

A finite p-group G is said to be *regular* if for each pair of elements a, b in G, there exists an element c in $\gamma_2(H)$ such that

$$(ab)^p = a^p b^p c^p,$$

where $H = \langle a, b\rangle$. For $p \geq 3$, any finite p-group of nilpotency class 2 is regular. More generally, every finite p-group of nilpotency class less than p is regular. The reader is referred to Huppert [66, III.10] for more details on regular p-groups. We begin with the following result [66, III.10.2(c) Satz].

Lemma 1.13 *Let G be a finite p-group, p an odd prime, such that $\gamma_2(G)$ is cyclic. Then G is regular.*

Exercise 1.14 Let G be a finite regular p-group. Then the following statements hold:

(1) $\Omega_i(G) = \{g \in G \mid g^{p^i} = 1\}$ for all $i \geq 1$.
(2) $\mho_i(G) = \{g^{p^i} \mid g \in G\}$ for all $i \geq 1$.
(3) $|G/\Omega_i(G)| = |\mho_i(G)|$ for all $i \geq 1$.
(4) If $x, y \in G$, then, for all $k, l \geq 0$, $[x^{p^k}, y^{p^l}] = 1$ if and only if $[x, y]^{p^{k+l}} = 1$.

Before proceeding further with regular p-groups, we introduce some definitions. Let $\mathcal{L}$ be a lattice with join $\vee$ and meet $\wedge$. Then $\mathcal{L}$ is said to be *modular* if

$$a \vee (b \wedge c) = (a \vee b) \wedge c$$

for all $a, b, c \in \mathcal{L}$ with $a \leq c$. We refer the reader to [47] for more details on lattice theory. Notice that the set of all subgroups of a group forms a lattice with inclusion as the partial order. Given two subgroups A and B of a group G, the join $A \vee B$ is the subgroup $\langle AB\rangle$, and the meet $A \wedge B$ is their intersection $A \cap B$. A group is called *modular* if its lattice of subgroups is modular.

Metacyclic p-groups are examples of modular groups. More concrete examples are the groups which occur as a direct product of the quaternion group of order 8 and finite elementary abelian 2-groups. We refer the curious reader to [109, Chapter 2] for a detailed study of modular groups. Further, the reader can refer to [9, Section 73] for classification of modular p-groups.

For a positive integer n, a group G is said to be *n-abelian* if

$$(xy)^n = x^n y^n$$

for all elements $x, y \in G$. Our interest here lies in the case when $n = p$, a prime. Any finite p-group of exponent p is obviously p-abelian. For odd primes p, if the commutator subgroup $\gamma_2(G)$ of a finite p-group G is of exponent p, then G is p-abelian. It is shown a little later that the exponent of the commutator subgroup of a p-abelian p-group is always p. Examples of finite p-groups with elementary abelian commutator subgroups can be easily constructed by taking a finite p-group G and factoring out by $\Phi\big(\gamma_2(G)\big)$, the Frattini subgroup of $\gamma_2(G)$.

For odd primes p, we investigate three specific classes, introduced above, of regular p-groups, namely, (1) p-groups G with central quotient $G/\operatorname{Z}(G)$ metacyclic, (2) modular p-groups and (3) p-abelian p-groups. These investigations are applied later in the monograph. That p-abelian p-groups are regular is clear, and the regularity of the other two classes is established below.

Let G be a finite p-group with metacyclic central quotient $G/\operatorname{Z}(G)$ and of nilpotency class greater than 2. Set

$$\overline{G} = G/\operatorname{Z}(G).$$

Then there exists a cyclic normal subgroup B of $\overline{G}$ such that $\overline{G}/B$ is also cyclic. Therefore, we can choose elements a and b in G such that

$$B = \langle \operatorname{Z}(G)b \rangle\,,$$

where the order of $\operatorname{Z}(G)b$ is p^m for some $m \geq 1$, and

$$\overline{G}/B = \langle B\bar{a} \rangle\,,$$

where $\bar{a} = \operatorname{Z}(G)a$.

For the group G in the preceding paragraph, we have

Lemma 1.15 *For odd primes p, $\gamma_2(G)$ is cyclic of order p^m generated by $[a, b]$. Furthermore, G is regular.*

Proof Consider the subgroup $M = \langle b, \operatorname{Z}(G)\rangle$ of G. Notice that $\gamma_2(G) \leq M$ and $b \in \operatorname{C}_G\big(\gamma_2(G)\big)$. Therefore, M is a normal abelian subgroup of G, and G/M is the cyclic subgroup $\langle Ma \rangle$, and $[a, b]^k = [a, b^k]$ for any positive integer k. Since the order of $\operatorname{Z}(G)b$ is p^m, we have

$$[a, b]^{p^m} = [a, b^{p^m}] = 1.$$

Furthermore, since $G = \langle a, b, \operatorname{Z}(G)\rangle$, it follows that $[a, b]^{p^n} \neq 1$ for any positive integer $n < m$. Thus, the order of $[a, b]$ is p^m. It also follows that

$$\gamma_2(G) = [a, G] = \langle [a, b] \rangle\,,$$

and hence $\gamma_2(G)$ is cyclic of order p^m. Since p is odd, G is regular by Lemma 1.13. □

The following two results are due to Davitt and Otto [21].

Theorem 1.16 *Let G be a finite p-group with metacyclic central quotient $\overline{G} = G/\mathrm{Z}(G)$ and of nilpotency class greater than 2, where p is an odd prime. Let $a, b \in G$ be such that $B = \langle \overline{b} \rangle$ is of order p^m for some $m \geq 1$ and $\overline{G}/B = \langle B\overline{a} \rangle$, where $\overline{b} = \mathrm{Z}(G)b$ and $\overline{a} = \mathrm{Z}(G)a$. Then the following statements hold:*

(1) The element a can be chosen such that

$$[a, b] = b^{p^{\alpha}} z \tag{1.17}$$

for some $0 \leq \alpha < m$ and $z \in \mathrm{Z}(G)$.

(2) If $M = \langle b, \mathrm{Z}(G) \rangle$, then the order of Ma is p^m.

(3) $|G/\mathrm{Z}(G)| = p^{2m}$ and $|G/\gamma_2(G)| = p^m\,|\mathrm{Z}(G)|$.

Proof By Lemma 1.15, G is regular. Further, by Exercise 1.14(4), we have

$$[a^{p^m}, b] = [a, b]^{p^m} = 1.$$

It therefore follows that $a^{p^m} \in \mathrm{Z}(G)$. Hence, the order of $\mathrm{Z}(G)a$ is p^m, since $[a, b]^{p^k} \neq 1$ for any $k < m$.

Since $[a, b] \in \gamma_2(G) \leq M$, we have $[a, b] = b^{rp^{\alpha}} z$, where r is coprime to p and $z \in \mathrm{Z}(G)$. Also, since the nilpotency class of G is at least 3, we can choose α such that $0 \leq \alpha < m$. Notice that

$$\gamma_2(G) = \left\{[a^i, b] \mid 0 \leq i < p^m\right\}.$$

Since r and p are coprime, there exists an integer s such that s is coprime to p and $rs \equiv 1$ modulo the order of b. Thus, $(b^{rp^{\alpha}} z)^s = b^{p^{\alpha}} z^s$ also generates $\gamma_2(G)$, and therefore $b^{p^{\alpha}} z^s = [a^i, b]$ for some i, $0 \leq i < p^m$, coprime to p. Consequently, we have $\langle B\bar{a} \rangle = \left\langle B\bar{a}^i \right\rangle$. Now replacing a by a^i settles assertion (1).

Observe that the order of $[a, b]$ modulo $\mathrm{Z}(G)$ is $p^{m-\alpha}$, and therefore

$$|\gamma_2(G)\,\mathrm{Z}(G)| = p^{m-\alpha}\,|\mathrm{Z}(G)|.$$

Since $|\gamma_2(G)| = p^m$, we have $|\gamma_2(G) \cap \mathrm{Z}(G)| = p^{\alpha}$. If $a^{p^s} \in M$, then, M being abelian,

$$1 = [a^{p^s}, b] = [a, b]^{p^s}.$$

Thus, the order of Ma is at least p^m. On the other hand, since $\mathrm{Z}(G) \leq M$, the order of Ma cannot exceed the order of $\mathrm{Z}(G)a$, which is p^m. Hence, the order of Ma is p^m, which is assertion (2).

As a consequence of assertion (2), G/M is cyclic of order p^m. Thus,

$$|G/\mathrm{Z}(G)| = |G/M|\,|M/\mathrm{Z}(G)| = p^{2m},$$

which obviously gives $|G/\gamma_2(G)| = p^m\,|\mathrm{Z}(G)|$, and the proof is complete. □

We continue assuming that G is a finite p-group with $G/\mathrm{Z}(G)$ metacyclic. Let $\exp\big(G/\gamma_2(G)\big) = p^k$ and $\exp\big(\mathrm{Z}(G)\big) = p^l$. Then there exists $z_1 \in \mathrm{Z}(G)$ of order p^l such that

$$\mathrm{Z}(G) = \langle z_1 \rangle \oplus W_1$$

for some subgroup W_1 of $\mathrm{Z}(G)$ with exponent p^β, where $\beta \le l$. Let $M = \langle b, \mathrm{Z}(G)\rangle$. Since $\gamma_2(G) \le M$ and the order of Ma is p^m (by Theorem 1.16(1)), it follows that the order of $\gamma_2(G)a$ is at least p^m, and therefore $k \ge m$. With this set-up, we now prove the following result.

Theorem 1.18 *Let G be a finite p-group with metacyclic central quotient and of nilpotency class greater than 2, where p is an odd prime. Then the following statements hold:*

(1) $|\mathrm{Z}_2(G)/\mathrm{Z}(G)| = p^{2\alpha}$, *where α is as in* (1.17).

(2) The elements b and z_1 can be chosen such that

$$a^{p^m} \equiv z_1^{p^{t_a}} \mod W_1$$

and

$$b^{p^m} \equiv z_1^{p^{t_b}} \mod W_1$$

for some $0 \le t_a, t_b \le l$.

Proof Using the facts that $|G/\mathrm{Z}(G)| = p^{2m}$, $|\gamma_2\big(G/\mathrm{Z}(G)\big)| = p^{m-\alpha}$ and $[a, b] \equiv b^{p^\alpha} \mod \mathrm{Z}(G)$, the proof of assertion (1) is an easy exercise.

Since $a^{p^m} \in \mathrm{Z}(G)$, it follows that $a^{p^m} = z_1^{rp^{t_a}} w_1$ for some $w_1 \in W_1$ and some integer r which is coprime to p. Since $\langle z_1 \rangle = \big\langle z_1^r \big\rangle$, replacing z_1 by z_1^r settles first part of the assertion (2). Similarly, $b^{p^m} = z_1^{sp^{t_b}} w_1'$ for some $w_1' \in W_1$ and some integer s which is coprime to p. Then there exists an integer q such that $qs \equiv 1$ modulo the order of z_1 and q is coprime to p. Then

$$(b^q)^{p^m} = z_1^{qsp^{t_b}} (w_1')^q \equiv z_1^{p^{t_b}} \mod W_1,$$

and $\langle \mathrm{Z}(G)b^q \rangle = \langle \mathrm{Z}(G)b \rangle$. Hence, we can replace b by b^q, and the proof of assertion (2) is complete. □

Next, we investigate finite non-abelian modular p-groups. Recall that, a group is called *Hamiltonian* if all its subgroups are normal. The following result is a folklore [66, III.7.12 Satz].

Theorem 1.19 *Every non-abelian p-group of odd order is non-Hamiltonian.*

The following result is due to Iwasawa [69]. Also see [117, p. 13, Theorem 14] for a proof.

Theorem 1.20 *Let G be a modular non-Hamiltonian p-group. Then the following statements hold:*

(1) There exists an abelian normal subgroup A of G such that G/A is cyclic.

(2) For each generator Ab of G/A, there exists an integer $\alpha > 0$ such that $[a, b] = a^{p^\alpha}$ for all $a \in A$.

A variant of the preceding theorem is the following result of Davitt and Otto [22].

Theorem 1.21 *Let G be a modular p-group, p an odd prime. Then there exists an abelian normal subgroup A of G and an integer $\alpha > 0$ such that G/A is cyclic, $\mho_\alpha(A) = \gamma_2(G)$ and $\mho_{2\alpha}(A) = \gamma_3(G)$.*

Proof Since p is an odd prime, by Theorem 1.19, G is non-Hamiltonian. Now, by Theorem 1.20, G contains an abelian normal subgroup A and an element b such that

$$G/A = \langle Ab \rangle$$

is cyclic. Further, there exists $\alpha > 0$ such that

$$[a, b] = a^{p^\alpha}$$

for all $a \in A$. Since G/A is abelian, we have $\gamma_2(G) \leq A$, and it follows that

$$\mho_\alpha(A) \leq \gamma_2(G).$$

Notice that $[a, b^i] = a^{(1+p^\alpha)^i - 1}$ lies in $\mho_\alpha(A)$ for each $a \in A$ and $i \geq 0$. Using commutator identities, it is not difficult to show that each commutator is of the form a^{p^α} for some $a \in A$. Consequently, we have $\mho_\alpha(A) = \gamma_2(G)$. The proof of the assertion $\mho_{2\alpha}(A) = \gamma_3(G)$ is similar and left as an exercise. □

The next two results are also due to Davitt and Otto [22].

Theorem 1.22 *For an odd prime p, a non-abelian modular p-group G is regular.*

Proof Let $x, y \in G$ and $H = \langle x, y \rangle$. Assume that H is non-abelian. Since $\gamma_2(G)$ is abelian, we have

$$(xy)^p = x^p y^p c^p d,$$

where $c \in \gamma_2(H)$ and $d \in \gamma_p(H)$. Since G is modular, then so is H. Thus, by Theorem 1.21, there exists an integer α_1 such that $\gamma_3(H) = \mho_{\alpha_1}\big(\gamma_2(H)\big)$, and we have

$$\gamma_p(H) \leq \gamma_3(H) = \mho_{\alpha_1}\big(\gamma_2(H)\big) \leq \mho_1\big(\gamma_2(H)\big).$$

Consequently, $d = d_1^p$ for some $d_1 \in \gamma_2(H)$. Since $\gamma_2(H) \leq \gamma_2(G)$ which is abelian, we have $c^p d = (cd_1)^p$ with $cd_1 \in \gamma_2(H)$. Therefore,

$$(xy)^p = x^p y^p c_1^p,$$

where $c_1 = cd_1$, and hence G is regular. □

Next, we determine the structures and the orders of $\mathrm{Z}(G)$ and $\mathrm{Z}_2(G)$ of a modular p-group G.

Theorem 1.23 *Let G be a modular p-group of nilpotency class greater than 2 and A an abelian normal subgroup of G as in Theorem 1.21 such that $|G/A| = |\langle Ab\rangle| = p^k$ and $\exp\big(\gamma_2(G)\big) = p^m$ for some positive integers k and m. Then the following statements hold:*

(1) $k \geq m > \alpha$;

(2) $\mathrm{Z}(G) = \langle b^{p^m}\rangle\big(A \cap \mathrm{Z}(G)\big) = \langle b^{p^m}\rangle\Omega_\alpha(A)$ *with* $|\mathrm{Z}(G)| = p^{k-m}\,|\Omega_\alpha(A)|$;

(3) $\mathrm{Z}_2(G) = \langle b^{p^{m-\alpha}}\rangle\Omega_{2\alpha}(A)$ *with* $|\mathrm{Z}_2(G)| = p^{k-m+\alpha}\,|\Omega_{2\alpha}(A)|$.

Proof By Theorem 1.21, we have $\mho_\alpha(A) = \gamma_2(G)$, and consequently $\exp(A) = p^{m+\alpha}$. Since $\gamma_2(G)$ is abelian, it follows that for each $a \in A$,

$$1 = [a,b]^{p^m} = [a, b^{p^m}] = [a^{p^m}, b].$$

Consequently, $a^{p^m},\ b^{p^m} \in \mathrm{Z}(G)$, and hence $\mho_m(G) \leq \mathrm{Z}(G)$. If $m \leq \alpha$, then

$$\gamma_2(G) = \mho_\alpha(A) \leq \mho_\alpha(G) \leq \mho_m(G) \leq \mathrm{Z}(G)$$

and G has nilpotency class 2, which is contrary to our assumption. Hence, we have

$$m > \alpha.$$

Notice that $a^{p^\alpha} = 1$ if and only if $a \in \mathrm{Z}(G)$. It follows that

$$\Omega_\alpha(A) = A \cap \mathrm{Z}(G). \tag{1.24}$$

Since b^{p^m} lies in $\mathrm{Z}(G)$, we have $\langle b^{p^m}\rangle\big(A \cap \mathrm{Z}(G)\big) \leq \mathrm{Z}(G)$. Conversely, let $x = b^i a \in \mathrm{Z}(G)$, where $a \in A$. Then

$$1 = [x,b] = [b^i a, b] = [a,b] = a^{p^\alpha},$$

and hence $a \in \Omega_\alpha(A)$. Now, for $a_1 \in A$, we have

$$1 = [x, a_1] = [b^i, a_1] = [b, a_1]^i,$$

and hence p^m divides i. Thus,

$$\mathrm{Z}(G) = \langle b^{p^m} \rangle \big(A \cap \mathrm{Z}(G) \big) = \langle b^{p^m} \rangle \Omega_\alpha(A).$$

Next, we claim that $|\,\langle \mathrm{Z}(G)b \rangle\,| = p^m$. Suppose that $|\,\langle \mathrm{Z}(G)b \rangle\,| \le p^{m-1}$. Then, by the regularity of G, each commutator in G has order $\le p^{m-1}$, and hence $\exp\big(\gamma_2(G)\big) \le p^{m-1}$, a contradiction. Therefore,

$$k \ge m,$$

and hence

$$|\,\mathrm{Z}(G)| = p^{k-m}\,|\Omega_\alpha(A)|$$

proving assertions (1) and (2).

Notice that

$$\mathrm{Z}_2(G) = \big\{ x \in G \mid [x, b], [x, a] \in \mathrm{Z}(G) \text{ for all } a \in A \big\}.$$

If $a \in \Omega_{2\alpha}(A)$, then $[a, b] = a^{p^\alpha} \in \Omega_\alpha(A) \le \mathrm{Z}(G)$, and consequently

$$\Omega_{2\alpha}(A) \le \mathrm{Z}_2(G).$$

Conversely, let $x = b^i a \in \mathrm{Z}_2(G)$ with $a \in A$. Then

$$[x, b] = [b^i a, b] = [a, b] = a^{p^\alpha} \in \mathrm{Z}(G) \cap A = \Omega_\alpha(A),$$

and hence $a \in \Omega_{2\alpha}(A)$. Since $b^i \in \mathrm{Z}_2(G)$, we have

$$[b^i, a_1] \in \mathrm{Z}(G) \cap A = \Omega_\alpha(A)$$

for each $a_1 \in A$. Thus, we obtain

$$1 = [b^i, a_1]^{p^\alpha} = [b^{ip^\alpha}, a_1].$$

Therefore, $b^{ip^\alpha} \in \mathrm{Z}(G)$ and p^m divides ip^α. Hence, $p^{m-\alpha}$ divides i, which yields

$$\mathrm{Z}_2(G) = \langle b^{p^{m-\alpha}} \rangle \Omega_{2\alpha}(A).$$

By (1.24), we get

$$|\,\langle Ab \rangle\,| = |\,\langle \Omega_\alpha(A)b \rangle\,| = p^k. \tag{1.25}$$

Thus, we obtain $|\langle \Omega_{2\alpha}(A)b\rangle| = p^k$ and

$$|\mathrm{Z}_2(G)| = p^{k-m+\alpha}\,|\Omega_{2\alpha}(A)|,$$

which is assertion (3). □

Notice that a finite p-abelian p-group is always regular. Consequently,

$$\mho_k(G) = \{x^{p^k} \mid x \in G\}$$

and

$$\Omega_k(G) = \{x \in G \mid x^{p^k} = 1\}.$$

We conclude this section with the following observation originally due to Hobby [60, Theorem 1].

Theorem 1.26 *Let G be a finite p-abelian p-group. Then $\mho_1(G) \le \mathrm{Z}(G)$ and $\gamma_2(G) \le \Omega_1(G)$.*

Proof Let $g, h \in G$ be such that the order of g is p^k. Set

$$u = g^{1+p+\cdots+p^{k-1}}.$$

Then we have

$$u^{-1}h^p u = (u^{-1}hu)^p = u^{-p}h^p u^p,$$

equivalently $u^{p-1}h^p u^{1-p} = h^p$. Notice that $u^{1-p} = g^{1-p^k} = g$, which implies $g^{-1}h^p g = h^p$, and hence $\mho_1(G) \le \mathrm{Z}(G)$. The second assertion is obvious from the first. □

1.3 Groups with Large Center

Throughout this section, we assume that $\mathrm{Z}(G) \le \Phi(G)$. The results are due to Davitt [20]. We begin with a general result about the relationship between the exponents of abelianization and center of finite p-groups.

Theorem 1.27 *Let G be a finite p-group such that $\Phi(G)$ is regular. Then the following statements hold:*

(1) If $\exp\big(\gamma_2(G)\big) = p$*, then* $\exp\big(G/\gamma_2(G)\big) \ge \exp\big(\mathrm{Z}(G)\big)$.

(2) If $\exp\big(\gamma_2(G)\big) = p^2$*, then* $\exp\big(G/\gamma_2(G)\big) \ge \exp\big(\mathrm{Z}(G)\big)/p$.

Proof Let $\exp(G) = p^m$. Since $\exp\bigl(\gamma_2(G)\bigr) = p$, we have

$$\exp\bigl(G/\gamma_2(G)\bigr) \geq p^{m-1}.$$

Notice that $\Phi(G) = \mho_1(G)\gamma_2(G)$. Since $\mathrm{Z}(G) \leq \Phi(G)$ and $\Phi(G)$ is regular, we have

$$\exp\bigl(\mathrm{Z}(G)\bigr) \leq \max\bigl\{\exp\bigl(\mho_1(G)\bigr), \exp\bigl(\gamma_2(G)\bigr)\bigr\} = p^{m-1}.$$

Consequently, it follows that $\exp\bigl(G/\gamma_2(G)\bigr) \geq \exp\bigl(\mathrm{Z}(G)\bigr)$, proving assertion (1). The proof of assertion (2) goes on similar lines. □

Exercise 1.28 If A is an abelian normal subgroup of a group G with cyclic factor group $G/A = \langle Ax\rangle$, then the map $a \mapsto [a, x]$ is an epimorphism from A to $\gamma_2(G)$ and $|A| = |\gamma_2(G)|\,|A \cap \mathrm{Z}(G)|$.

Next we show that p-groups with sufficiently large centers are metabelian.

Theorem 1.29 *Let G be a non-abelian p-group such that $|G/\mathrm{Z}(G)| \leq p^4$. Then G is metabelian.*

Proof The group G possesses the series of normal subgroups

$$\mathrm{Z}(G) \leq K \leq \Phi(G) < G,$$

where $K = \gamma_2(G)\,\mathrm{Z}(G)$. Observe that it is sufficient to prove that K is abelian. Under the given hypothesis, $|K/\mathrm{Z}(G)|$ is 1, p or p^2. If $|K/\mathrm{Z}(G)|$ is 1 or p, then K is obviously abelian. So we assume that $|K| = p^2$. Notice that in this case $K = \Phi(G)$. If $K/\mathrm{Z}(G)$ is cyclic, then obviously K is abelian. The only case which remains is when $K/\mathrm{Z}(G)$ is non-cyclic. Then there exist elements $a, b \in K$ such that

$$K/\mathrm{Z}(G) = \langle \mathrm{Z}(G)a\rangle \oplus \langle \mathrm{Z}(G)b\rangle\,.$$

If the nilpotency class of G is 3, then $[a, b] \in \gamma_4(G) = 1$, and therefore K is abelian. If the nilpotency class of G is 4, then $\gamma_3(G) \not\leq \mathrm{Z}(G)$. Therefore, we can choose $a \in \gamma_2(G)$ and $b \in \gamma_3(G)$. Thus, $[a, b] \in \gamma_5(G) = 1$, which implies that K is abelian. □

Theorem 1.30 *Let G be a p-group such that $|G/\mathrm{Z}(G)| \leq p^4$. Then the following statements hold:*

(1) If $\exp\bigl(\gamma_2\bigl(G/\mathrm{Z}(G)\bigr)\bigr) = p$, then $\mho_1\bigl(\gamma_2(G)\bigr) \leq \mathrm{Z}(G)$ and $\exp\bigl(\gamma_3(G)\bigr) = p$.

(2) If $\exp\bigl(\gamma_2\bigl(G/\mathrm{Z}(G)\bigr)\bigr) \leq p^2$, then $\exp\bigl(\gamma_2(G)\bigr) \leq p^2$.

Proof Set $H = G/\mathrm{Z}(G)$. Notice that $\gamma_2(H) = \gamma_2(G)\,\mathrm{Z}(G)/\mathrm{Z}(G)$. Since the exponent of $\gamma_2(H)$ is p, it follows that $\mho_1\bigl(\gamma_2(G)\bigr) \leq \mathrm{Z}(G)$. Again notice that the nilpotency class of G is at most 4. Thus, for any $x \in G$ and $u \in \gamma_2(G)$, we have

$$1 = [x, u^p] = [x, u]^p,$$

and therefore $\exp\big(\gamma_3(G)\big) = p$.

Since the exponent of H is at most p^2 and the nilpotency class of G is at most 4, for any $x, y \in G$, we have

$$1 = [x^{p^2}, y] = [x, y]^{p^2}[x, y, x]^{\binom{p^2}{2}}[x, y, x, x]^{\binom{p^2}{3}}.$$

If $p \geq 3$, then $\exp\big(\gamma_3(H)\big) \leq p$ as $|H| \leq p^4$. Thus, it follows that $[x, y]^{p^2} = 1$. If $p = 2$, then an easy GAP [38] check or an exercise shows that $\exp\big(\gamma_2(H)\big) \leq 2$; hence $[x, y]^{p^2} = 1$. Since $\gamma_2(G)$ is abelian, by Theorem 1.29, and is generated by elements of order at most p^2, it follows that $\exp\big(\gamma_2(G)\big) \leq p^2$. □

We conclude this section with the following result on 3-groups.

Theorem 1.31 *Let G be a 3-group such that $G/\mathrm{Z}(G)$ is not metacyclic and $|G/\mathrm{Z}(G)| \leq 3^4$. Then the following statements hold:*

(1) $\exp\big(\gamma_2\big(G/\mathrm{Z}(G)\big)\big) = 3$*;*

(2) $\exp\big(\gamma_3(G)\big) = 3$*;*

(3) $\Phi(G)$ *is regular.*

Proof Set $H = G/\mathrm{Z}(G)$. Since H is not metacyclic, we have $\exp(H) \leq 3^2$. Therefore, by Theorem 1.30(1), $\exp\big(\gamma_2(G)\big) \leq 3^2$. Obviously, we have $|\gamma_2(H)| \leq 3^2$. Suppose that $\exp\big(\gamma_2(H)\big) = 3^2$. Then H is regular and $d(H) = 2$. If $H = \langle x, y\rangle$, then $\gamma_2(H) = \langle [x, y]\rangle$, and $\mho_1(H) = \big\langle x^3, y^3\big\rangle$ is of order 3^2. Thus, $|G/\mho_1(G)| = 3^2$, which implies that H is metacyclic, a contradiction. Hence, assertion (1) holds.

By (1), we get $\exp\big(\gamma_2(H)\big) = 3$. Therefore, by Theorem 1.30(1), we have $\mho_1\big(\gamma_2(G)\big) \leq \mathrm{Z}(G)$ and $\exp\big(\gamma_3(G)\big) = 3$, proving assertion (2). Assertion (3) is immediate from the inequality $|\Phi(G)/\mathrm{Z}(G)| \leq 3^2$. □

1.4 Gaschütz's Theorem and Its Generalization

We begin the section with some basic definitions. Let G be a group and X a set. By a *left action* of G on X, we mean a map $G \times X \to X$, written as

$$(g, x) \mapsto {}^{g}x,$$

satisfying the following conditions:

(1) ${}^{1}x = x$ for all $x \in X$, where 1 is the identity element of G;

(2) ${}^{g_1g_2}x = {}^{g_1}({}^{g_2}x)$ for all $g_1, g_2 \in G$ and $x \in X$.

An action of a group G on a set X is said to be *free* if, for each $x \in X$, the *stabilizer* subgroup

$$G_x := \{g \in G \mid {}^g x = x\}$$

of G at x is the trivial subgroup. Further, for each $x \in X$, the set $\{{}^g x \mid g \in G\}$ is called the *orbit* of x, and the action is called *transitive* if it has just one orbit.

For each $x \in X$, the map $g \mapsto {}^g x$ induces a bijection between the set G/G_x of right cosets of G_x in G and the orbit of the element x. This observation is referred to as the *orbit-stabilizer theorem* in the literature.

Throughout the monograph, all our group-actions are left actions, unless stated otherwise. For a group G and $g \in G$, let ι_g denote the inner automorphism of G induced by g.

In 1966, as an ingenious application of cohomological methods, Gaschütz [40] (see also [122, Theorem 12.2.3]) proved the following result.

Theorem 1.32 *Let G be a non-abelian finite p-group. Then G has a non-inner automorphism of order a power of p.*

The following generalization of the preceding theorem for non-abelian p-groups was obtained by Schmid [111], again using cohomological methods, which was reproved by Webb [123] without using cohomology theory.

Theorem 1.33 *Let G be a non-abelian finite p-group. Then G has a non-inner automorphism centralizing $\mathrm{Z}(G)$ and of order a power of p.*

We here present Webb's proof.

Let G be a finite p-group and M a maximal subgroup of G. Let $g \in G$ be such that $G/M = \langle Mg \rangle$. Define endomorphisms τ and γ of $\mathrm{Z}(M)$ as follows

$$\tau(m) = m\, {}^g m \cdots {}^{g^{p-1}} m$$

and

$$\gamma(m) = [m, g],$$

for all $m \in \mathrm{Z}(M)$.

Exercise 1.34 $\mathrm{Im}(\gamma) \le \mathrm{Ker}(\tau)$ and $\mathrm{Im}(\tau) \le \mathrm{Ker}(\gamma) = \mathrm{Z}(G) \cap M$. Moreover, $|\,\mathrm{Ker}(\tau)/\,\mathrm{Im}(\gamma)| = |\,\mathrm{Ker}(\gamma)/\,\mathrm{Im}(\tau)|$.

For a given $\alpha \in \mathrm{Aut}(M)$, we define

$$A_\alpha = \left\{\phi \in \mathrm{Aut}^{G/M}(G) \mid \phi|_M = \alpha\right\}$$

and

$$M_\alpha = \left\{m \in M \mid [\alpha, \iota_g] = \iota_m \text{ and } \alpha(g^p) = (mg)^p\right\}.$$

Notice that, in the definition of M_α, ι_g is viewed as an automorphism of M. With this set-up, we prove the following result.

Lemma 1.35 *Let $\alpha \in \mathrm{Aut}(M)$. Then the map $A_\alpha \to M_\alpha$ given by $\phi \mapsto \phi(g)g^{-1}$ is a bijection. Further, if the order of α is some power of p, then so is the case for each element of A_α.*

Proof If $\phi \in A_\alpha$, then a routine calculation gives $\phi(g)g^{-1} \in M_\alpha$. Let $u \in M_\alpha$. Define $\phi : M \to M$ by $\phi(m) = \alpha(m)$ for all $m \in M$ and $\phi(g) = ug$. Since $\alpha(g^p) = (ug)^p$, it follows that ϕ is well-defined.

Next, we show that ϕ is a homomorphism, and hence an automorphism. For $m_1, m_2 \in M$, we have

$$\begin{aligned}\phi(m_1 g^i)\phi(m_2 g^j) &= \alpha(m_1)(ug)^i \alpha(m_2)(ug)^j \\ &= \alpha(m_1)\ {}^{(ug)^i}\alpha(m_2)(ug)^{j-i} \\ &= \alpha(m_1)(\iota_u \iota_g)^i \big(\alpha(m_2)\big)(ug)^{j-i} \\ &= \alpha(m_1)(\alpha \iota_{g^i} \alpha^{-1})\big(\alpha(m_2)\big)(ug)^{j-i} \\ &= \alpha(m_1)(\alpha \iota_{g^i})(m_2)(ug)^{j-i} \\ &= \phi(m_1 g^i m_2 g^j).\end{aligned}$$

Thus, we establish a bijection between A_α and M_α. Further, if the order of α is p^r and the order of the element $\alpha^{p^r-1}(u)\alpha^{p^r-2}(u)\cdots\alpha(u)u$ of M is p^k, then a direct computation shows that the order of ϕ is p^{r+k}. □

Let id_M be the identity automorphism of M. Notice that, by Lemma 1.35, $A_{\mathrm{id}_M} = \mathrm{Aut}^{M,G/M}(G)$ is a p-group.

Lemma 1.36 *Let G be a finite p-group and M a maximal subgroup containing $\mathrm{Z}(G)$ such that $G/M = \langle Mg \rangle$. Then $\mathrm{Aut}^{M,G/M}(G) \nleq \mathrm{Inn}(G)$ if and only if $\mathrm{Im}(\tau) \neq \mathrm{Ker}(\gamma)$.*

Proof Replacing α by the identity automorphism id_M of M, we obtain

$$A_{\mathrm{id}_M} = \mathrm{Aut}^{M,G/M}(G)$$

and

$$M_{\mathrm{id}_M} = \{m \in \mathrm{Z}(M) \mid g^p = (mg)^p\}.$$

Now, by Lemma 1.35, it follows that $\mathrm{Aut}^{M,G/M}(G) \le \mathrm{Inn}(G)$ if and only if M_{id_M} consists of elements of the form $\iota_u(g)g^{-1}$, where $u \in \mathrm{C}_G(M)$. Since $\mathrm{Z}(G) \le M$, it follows that $\mathrm{C}_G(M) = \mathrm{Z}(M)$. But, $\mathrm{C}_G(M) = \mathrm{Z}(M)$ if and only if $M_{\mathrm{id}_M} \subseteq [\mathrm{Z}(M), g] = \mathrm{Im}(\gamma)$. A direct calculation shows that

$$\mathrm{Ker}(\tau) = M_{\mathrm{id}_M}.$$

Since $\mathrm{Im}(\gamma) \le \mathrm{Ker}(\tau)$, we have $\mathrm{Aut}^{M,G/M}(G) \le \mathrm{Inn}(G)$ if and only if $\mathrm{Ker}(\tau) = \mathrm{Im}(\gamma)$. In view of Exercise 1.34, the last equality holds if and only if $\mathrm{Im}(\tau) = \mathrm{Ker}(\gamma)$. □

The proof of Lemma 1.36 indeed gives

Corollary 1.37 *If* $\mathrm{Im}(\tau) \le \mathrm{Ker}(\gamma)$*, then*

$$|\operatorname{Aut}^{M,G/M}(G)\operatorname{Inn}(G)/\operatorname{Inn}(G)| = |\operatorname{Ker}(\gamma)/\operatorname{Im}(\tau)|.$$

For a group G, set

$$\mathrm{C}_{\mathrm{Out}(G)}\big(\mathrm{Z}(G)\big) = \operatorname{Aut}^{\mathrm{Z}(G)}(G)/\operatorname{Inn}(G).$$

Exercise 1.38 Let G be a non-abelian group of order 8. Then 2 divides the order of $\mathrm{C}_{\mathrm{Out}(G)}\big(\mathrm{Z}(G)\big)$.

Next, we prove

Lemma 1.39 *Let G be a non-abelian finite p-group such that $|G| > 8$ and each maximal subgroup of G containing $\mathrm{Z}(G)$ is abelian. Then p divides the order of $\mathrm{C}_{\mathrm{Out}(G)}\big(\mathrm{Z}(G)\big)$.*

Proof Contrarily, assume that the result is false. Then notice that

$$\operatorname{Aut}^{M,G/M}(G) = A_{\mathrm{id}_M} \le \operatorname{Inn}(G).$$

By Exercise 1.34 and Lemma 1.36, we have

$$\mathrm{Im}(\tau) = \mathrm{Ker}(\gamma) = \mathrm{Z}(G).$$

We claim that any element $x \in G \setminus \mathrm{Z}(G)$ generates a maximal subgroup of G. Let $x \in G \setminus \mathrm{Z}(G)$. Since, G being non-abelian, $G/\mathrm{Z}(G)$ is not cyclic, we can choose a maximal subgroup N of G containing x and $\mathrm{Z}(G)$. Let $y \in G$ be such that $G = \langle y, N\rangle$, and M be a maximal subgroup of G containing y and $\mathrm{Z}(G)$. Notice that $G = NM$. By the given hypothesis, both N and M are abelian. Thus,

$$\mathrm{Z}(G) \le N \cap M \le \mathrm{C}_G(N) \cap \mathrm{C}_G(M) = \mathrm{Z}(G),$$

which gives $\mathrm{Z}(G) = N \cap M$. By the maximality of N and M, it now follows that $N = \langle x, \mathrm{Z}(G)\rangle$ and both x^p and y^p lie in $\mathrm{Z}(G)$. Thus,

$$G = \langle x, y, \mathrm{Z}(G)\rangle$$

and $|G/\mathrm{Z}(G)| = p^2$, which implies that $\gamma_2(G) = \langle [x, y]\rangle$ is of order p; nilpotency class of G is 2. By the given hypothesis on the order of G, we can assume that either p is odd or $p = 2$ and $|\mathrm{Z}(G)| \ge 4$. For, if $|\mathrm{Z}(G)| = 2$, then $|G| = 8$.

Since N is abelian, we get

$$\mathrm{Z}(N) = N = \langle x, \mathrm{Z}(G)\rangle .$$

Thus, by the definition of τ and G being of nilpotency class 2, we have

$$\begin{aligned}\mathrm{Z}(G) &= \mathrm{Im}(\tau)\\ &= \langle \tau(x),\ \tau(z) \mid z \in \mathrm{Z}(G)\rangle\\ &= \big\langle x^p[x,y]^{p(p-1)/2},\ z^p \mid z \in \mathrm{Z}(G)\big\rangle\\ &= \big\langle x^p[x,y]^{p(p-1)/2}\big\rangle,\ \text{since } z^p \in \Phi\big(\mathrm{Z}(G)\big).\end{aligned}$$

If p is odd, then obviously $\mathrm{Z}(G) = \langle x^p\rangle$. If $p = 2$, since $[x, y]$ is of order 2 and $\mathrm{Z}(G)$ is cyclic of order at least 4, it follows that $[x, y] \in \Phi\big(\mathrm{Z}(G)\big)$. Hence, $N = \langle x, \mathrm{Z}(G)\rangle = \langle x\rangle$ is cyclic, and the claim follows.

Since $y \in G \setminus \mathrm{Z}(G)$, we have $M = \langle y\rangle$ is cyclic of order at least p^2, and therefore $y^p \neq 1$. Notice, by the choice of y, that $y^p = x^{rp}$, for some integer r. Consequenty, we get $y^{-1}x^r \in G \setminus \mathrm{Z}(G)$. Thus, $\big\langle y^{-1}x^r\big\rangle$ is a maximal subgroup of G having order p, if p is odd, or 4, if $p = 2$, none of which is possible. □

We are now ready to prove Theorem 1.33.

Proof of Theorem 1.33. We proceed by induction on the order of finite p-groups. Let G be a non-abelian finite p-group. Suppose that the theorem holds for all non-abelian finite p-groups of order less than $|G|$. In view of Lemma 1.39 and Lemma 1.36, we can, respectively, assume that G admits a non-abelian maximal subgroup M containing $\mathrm{Z}(G)$ and

$$\mathrm{Im}(\tau) = \mathrm{Ker}(\gamma).$$

Then by induction hypothesis p divides the order of $\mathrm{C}_{\mathrm{Out}(M)}\big(\mathrm{Z}(M)\big)$.

Let $g \in G$ be such that $G = \langle g, M\rangle$ and $\psi := \iota_g|_M$, the restriction of ι_g to M, where ι_g denotes the inner automorphism of G induced by g. Then the order of ψ is some power of p. We claim that ψ normalizes $\mathrm{C}_{\mathrm{Out}(M)}\big(\mathrm{Z}(M)\big)$, that is, $(\bar{\psi})\bar{\alpha}\bar{\psi}^{-1} \in \mathrm{C}_{\mathrm{Out}(M)}\big(\mathrm{Z}(M)\big)$ for all $\alpha \in \mathrm{Aut}^{\mathrm{Z}(M)}(M)$, where $\bar{\psi} = \mathrm{Inn}(M)\psi$ and $\bar{\alpha} = \mathrm{Inn}(M)\alpha$. Let $\alpha \in \mathrm{Aut}^{\mathrm{Z}(M)}(M)$. Since $\mathrm{Z}(M)$ is a normal subgroup of G, for all $u \in \mathrm{Z}(M)$, we have

$$\psi\alpha\psi^{-1}(u) = \psi\big(\alpha(\psi^{-1}(u)\big) = \psi\big(\psi^{-1}(u)\big) = u,$$

and the claim follows. The group $\langle\psi\rangle$ acts on the set of all Sylow p-subgroups of $\mathrm{C}_{\mathrm{Out}(M)}\big(\mathrm{Z}(M)\big)$. Using the Sylow theorem and the orbit-stabilizer theorem, it follows that some Sylow p-subgroup of $\mathrm{C}_{\mathrm{Out}(M)}\big(\mathrm{Z}(M)\big)$ is kept invariant by $\langle\psi\rangle$. Now, restricting the action of $\langle\psi\rangle$ on this Sylow p-subgroup and again using the orbit-stabilizer theorem, we get a non-inner automorphism $\alpha \in \mathrm{Aut}^{\mathrm{Z}(M)}(M)$ of p-power order such that

$$[\alpha, \psi] = \iota_m \in \mathrm{Inn}(M),$$

where $m \in M$.

Notice, ψ being the restriction of ι_g, that

$$\alpha\psi^p\alpha^{-1} = (\iota_m\psi)^p = \iota_{(mg)^p} \tag{1.40}$$

and

$$\psi^p = \iota_{g^p} \in \mathrm{Inn}(M).$$

Putting the value of ψ^p in (1.40) and equating both the sides give

$$(mg)^{-p}\alpha(g^p) \in \mathrm{Z}(M).$$

Since α centralizes $\mathrm{Z}(M)$, we have

$$(mg)^{-p}\alpha(g^p) = \alpha^{-1}\big((mg)^{-p}\big)g^p.$$

Noticing that $[\alpha^{-1}\big((mg)^{-p}\big)g^p, g] = 1$, we obtain $(mg)^{-p}\alpha(g^p) \in \mathrm{Ker}(\gamma)$. Since $\mathrm{Im}(\tau) = \mathrm{Ker}(\gamma)$, there exists an element $y \in \mathrm{Z}(M)$ such that

$$(mg)^{-p}\alpha(g^p) = \tau(y). \tag{1.41}$$

A straightforward calculation shows that

$$(myg)^p = (ymg)^p = {}^{g}y \cdots {}^{g^{p-1}}y\, {}^{g^p}y\, (mg)^p = (mg)^p\, y\, {}^{g}y \cdots {}^{g^{p-1}}y = (mg)^p\tau(y),$$

since $y \in \mathrm{Z}(M)$ and $\mathrm{Z}(M)$ is normal in G. Hence, by (1.41), we obtain

$$\alpha(g^p) = (myg)^p.$$

Noticing that $\iota_m = \iota_{my}$, it follows that $my \in \mathrm{M}_\alpha$.

By Lemma 1.35, α extends to an automorphism ϕ of G of p-power order. By the choice of α and the fact that $\mathrm{Z}(G) \le \mathrm{Z}(M)$, ϕ centralizes $\mathrm{Z}(G)$. It only remains to show that ϕ is non-inner. Contrarily, assume that ϕ is inner, say, induced by $x \in G$. Then, by the choice of α, x centralizes $\mathrm{Z}(M)$. Suppose that $x \in G \setminus M$. Then $G = \langle x, M\rangle$, and therefore $\mathrm{Z}(M) = \mathrm{Z}(G)$. Thus,

$$\mathrm{Ker}(\gamma) = \mathrm{Im}(\tau) = \mathrm{Z}(M),$$

which forces $\mathrm{Ker}(\tau) = 1$. But, on the other hand,

$$1 \ne \Omega_1\big(\mathrm{Z}(G)\big) \le \mathrm{Ker}(\tau),$$

a contradiction, and hence $x \in M$. Then $\alpha = \phi|_M \in \mathrm{Inn}(M)$, which contradicts the fact that α is non-inner. Thus, ϕ is non-inner, and the proof is complete. □

1.5 Pro-p-Groups

In this section, we record some preliminaries on pro-p-groups. We refer the reader to [24] for detailed account of pro-p-groups.

We begin with the definition of a directed set. A *directed set* is a non-empty partially ordered set $(\Lambda, \leq)$ with the property that for every $\lambda, \mu \in \Lambda$ there exists $\nu \in \Lambda$ with $\lambda, \mu \leq \nu$. For example, the set of natural numbers $\mathbb{N}$ with the usual order $\leq$ is a directed set.

A *topological group* G is a topological space which is also a group such that the map $G \times G \to G$ given by

$$(g, h) \mapsto gh^{-1},$$

$g, h \in G$, is continuous. Here $G \times G$ is equipped with the product topology. An *inverse system* of topological groups over a directed set $(\Lambda, \leq)$ is a family of topological groups $\{G_\lambda\}_{\lambda \in \Lambda}$ with continuous group homomorphisms

$$\pi_{\lambda,\mu} : G_\lambda \to G_\mu$$

whenever $\mu \leq \lambda$ satisfying the compatibility conditions

$$\pi_{\lambda,\lambda} = \mathrm{id}_{G_\lambda}$$

and

$$\pi_{\mu,\nu}\, \pi_{\lambda,\mu} = \pi_{\lambda,\nu},$$

for $\nu \leq \mu \leq \lambda$.

The *inverse limit* of the inverse system $\{G_\lambda\}_{\lambda \in \Lambda}$ of topological groups, denoted by $\varprojlim G_\lambda$, is the subgroup of the topological group $\prod_{\lambda \in \Lambda} G_\lambda$ consisting of elements $(g_\lambda)_{\lambda \in \Lambda}$ such that $\pi_{\lambda,\mu}(g_\lambda) = g_\mu$ whenever $\mu \leq \lambda$.

Notice that each finite group can be viewed as a topological group when equipped with the discrete topology. If we start with an inverse system $\{G_\lambda\}_{\lambda \in \Lambda}$ of finite groups each of them equipped with the discrete topology, then $\prod_{\lambda \in \Lambda} G_\lambda$ has the product topology, and hence $\varprojlim G_\lambda$ with the induced topology becomes a compact Hausdorff topological group.

For a prime p, a *pro-p-group*, by definition, is the inverse limit of an inverse system of finite p-groups. For example, finite p-groups are pro-p-groups if given the discrete topology. A prototype example is the additive group $\mathbb{Z}_p$ of p-adic integers defined as the inverse limit of the inverse system of finite cyclic groups $\{\mathbb{Z}/p^n\mathbb{Z}\}_{n \in \mathbb{N}}$ with natural maps

$$\mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}/p^m\mathbb{Z}$$

whenever $n \geq m$. In fact, $\mathbb{Z}_p$ is a pro-p-group containing $\mathbb{Z}$ as a dense subgroup. Further, $\mathbb{Z}_p$ is a ring without zero divisors and its field of fractions is the field $\mathbb{Q}_p$ of

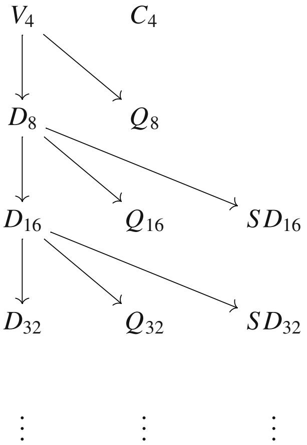
p-adic numbers. We refer the reader to [43] for an elementary introduction to theory of p-adic numbers.

Define the *coclass* of a finite p-group G of order p^n, denoted by $\mathrm{cc}(G)$, as

$$\mathrm{cc}(G) := n - \mathrm{cl}(G),$$

where $\mathrm{cl}(G)$ denotes the nilpotency class of G. An infinite pro-p-group L is said to be of *coclass* r if there exists some positive integer k such that $\mathrm{cc}\left(L/\gamma_i(L)\right) = r$ for all $i \geq k$.

Given a prime p and a positive integer r, let $\mathcal{G}(p, r)$ denote the directed graph whose vertex set consists of all isomorphism types of finite p-groups of coclass r, and there is a directed edge from H to G if there exists a normal subgroup N of G such that $|N| = p$ and $G/N \cong H$. The graph $\mathcal{G}(p, r)$ is referred to as the *coclass graph* of finite p-groups of coclass r. For example, the coclass graph $\mathcal{G}(2, 1)$ is as follows:



Here, V_4 is the Klein 4-group. For $n \geq 3$, D_{2^n}, Q_{2^n} are the dihedral and the quaternion groups of orders 2^n, respectively. And for $n \geq 4$, SD_{2^n} is the semi-dihedral group of order 2^n.

If G and H are two groups representing two different vertices of $\mathcal{G}(p, r)$, then we say that G is a *descendant* of H if there is a directed edge from H to G. Observe that, if G is a descendant of H, then

$$\mathrm{cc}(G) = \mathrm{cc}(H) = r.$$

Since $|G| = p\,|H|$, it follows that $\mathrm{cl}(H) = \mathrm{cl}(G) - 1$, and therefore N must necessarily be the last term of the lower central series of G.

Let L be an infinite pro-p-group of coclass r, t be the minimal positive integer such that $\mathrm{cc}\left(L/\gamma_t(L)\right) = r$ and $L/\gamma_t(L)$ do not arise as a quotient of an infinite pro-p-group of coclass r not isomorphic to L. Then the full subtree $\mathcal{T}(L)$ of $\mathcal{G}(p, r)$

consisting of all descendants of $L/\gamma_t(L)$ is called a *maximal coclass tree* in $\mathcal{G}(p, r)$. It follows, by construction, that the sequence of groups $\{G_i\}_{i\geq 0}$ with

$$G_i := L/\gamma_{t+i}(L),$$

called the *main line* of $\mathcal{T}(L)$, contains every infinite path of $\mathcal{T}(L)$.

Now onwards we assume that $p = 2$. Let $\mathcal{T}(L)$ be a maximal coclass tree in $\mathcal{G}(2, r)$ and $\{G_i\}_{i\geq 0}$ its main line. For each non-negative integer i, let $\mathcal{T}(L)_i$ be the subgraph of $\mathcal{T}(L)$ consisting of all descendants of G_i which are not descendants of G_{i+1}. The following theorem gives a description of L [24, Theorem 10.1].

Theorem 1.42 *Let L be an infinite pro-2-group of coclass r. Then L has an open normal subgroup $T \cong (\mathbb{Z}_2)^d$ for $d = 2^s$ for some $s \leq r + 1$. Furthermore, $P = L/T$ is a 2-group of order $2^{r+(r+1)2^{r+1}}$ and has coclass r.*

The following result is [24, Theorem 10.2] for $p = 2$.

Theorem 1.43 *For a given integer r, there are only finitely many isomorphism types of infinite pro-2-groups of coclass r.*

The preceding theorem can be interpreted as the graph $\mathcal{G}(2, r)$ containing only a finite number of maximal coclass trees. An immediate consequence of the construction of the maximal coclass tree and the preceding theorem is the following result.

Corollary 1.44 *For a given integer r, all but finitely many 2-groups of coclass r are contained in a maximal coclass tree of $\mathcal{G}(2, r)$.*

In Theorem 1.42, the integer d is referred to as the *rank* of the maximal coclass tree $\mathcal{T}(L)$, the open normal subgroup T is the *translation subgroup* of L and P is its *point subgroup*. It follows from [82, Lemma 7.4.3] that there exists a sufficiently large positive integer k such that $T \cong \gamma_k(L)$.

We conclude this chapter with two theorems of Eick and Leedham-Green [27], which play a crucial role in Sect. 5.3 of Chap. 5. The first one being the following result [27, Theorems 27, 28].

Theorem 1.45 *Let L be an infinite pro-2-group of coclass r and $\mathcal{T}(L)$ a maximal coclass tree in $\mathcal{G}(2, r)$ of rank d. Then there exists a positive integer m such that for each $j \geq m$, there is a graph isomorphism*

$$\tau_j : \mathcal{T}(L)_j \to \mathcal{T}(L)_{j+d}.$$

Furthermore, $|\tau_j(G)| = 2^d\,|G|$ for all $G \in \mathcal{T}(L)_j$.

Let m be the smallest positive integer as in the preceding theorem. Then a group G_m representing the root of the subgraph $\mathcal{T}(L)_m$ is called the *periodicity root* of $\mathcal{T}(L)$. The full subtree of $\mathcal{T}$ with root as the periodicity root is called the *periodic part* of $\mathcal{T}$. Setting $T_0 = T$ and

$$T_{i+1} = [T_i, L],$$

the final result of this chapter is as follows [27, Theorem 7].

Theorem 1.46 *Let L be an infinite pro-2-group of coclass r, $T = \gamma_k(L)$ for some integer k and $P = L/T$. If k is chosen sufficiently large, then every group G in the periodic part of $\mathcal{T}(L)$ can be written as an extension of P by T/T_j, where j is such that $|G| = 2^j\ |P|$. Furthermore, $\tau_j(G)$ is an extension of P by T/T_{j+d}.*

Chapter 2
Fundamental Exact Sequence of Wells

Given a normal subgroup N of a group G, a basic problem in the theory of automorphisms of groups is that of extending an automorphism of N to an automorphism of G, and the analogous one of lifting an automorphism of the quotient group G/N to an automorphism of G. A crucial role in the investigation of these problems is played by an exact sequence due to Wells [126]. In this chapter, a detailed exposition of this sequence and its role in determining conditions for extension and lifting of automorphisms is presented.

2.1 Cohomology of Groups

Let G be a group and R a commutative ring with unity. The *group algebra* of G over R, denoted by $R[G]$, is defined as the free R-module with basis G and the product which extends simultaneously the group operation in G and the ring multiplication in R. More precisely, elements of $R[G]$ are finite formal sums of the form $\sum a_g g$, where $a_g \in R$ and $g \in G$. Further, for elements $\sum a_g g, \ \sum b_g g \in R[G]$, the product is defined as

$$\left(\sum a_g g\right)\left(\sum b_g g\right) = \sum c_g g,$$

where $c_g = \sum_{xy=g} a_x b_y$. It can be easily verified that $R[G]$ is an R-algebra. Further, since R is a ring with unity, $R[G]$ is also a ring with unity. There is a natural homomorphism

$$\varepsilon : R[G] \to R$$

given by

$$\varepsilon\left(\sum a_g g\right) = \sum a_g$$

called the *augmentation map*. The kernel of ε is a 2-sided ideal of $R[G]$, called the *augmentation ideal* of $R[G]$, and denoted by $I_R(G)$ or simply by $I(G)$ in case the ring of coefficients is clear from the context. Group algebras over the ring $\mathbb{Z}$ of

I. B. S. Passi et al., *Automorphisms of Finite Groups*, Springer Monographs
in Mathematics, https://doi.org/10.1007/978-981-13-2895-4_2

integers are of particular interest in group theory. For a given group G, modules over the group algebra $\mathbb{Z}[G]$ are also referred to as *G-modules*. Notice that if a group G acts on an abelian group N by automorphisms, then N can be viewed as a G-module.

Let R be a commutative ring. A *cochain complex* of R-modules is a family

$$\mathcal{C} = \{C^n,\ \partial^n\}_{n \geq 0}$$

of R-modules C^n and R-module homomorphisms

$$\partial^n : C^n \to C^{n+1},$$

defined for each integer $n \geq 0$, such that $\partial^n \partial^{n-1}$ is the trivial homomorphism. Set $C^{-1} = 1$ and $\partial^{-1} : C^{-1} \to C^0$ as the trivial map. For each integer $n \geq 0$, ∂^n is called the nth *coboundary operator*, and C^n the R-module of *n-cochains*. Further, $\mathrm{Ker}(\partial^n)$ is referred to as the R-module of *n-cocycles*, and $\mathrm{Im}(\partial^{n-1})$ the R-module of *n-coboundaries*. The *n-dimensional cohomology* of the cochain complex $\mathcal{C}$ is the R-module

$$\mathrm{H}^n(\mathcal{C}) := \mathrm{Ker}(\partial^n)/\,\mathrm{Im}(\partial^{n-1}).$$

For an n-cocycle $c \in \mathrm{Ker}(\partial^n)$, we denote by $[c] \in \mathrm{H}^n(\mathcal{C})$ the corresponding *cohomology class*.

If $\mathcal{C} = \{C^n,\ \partial^n\}_{n \geq 0}$ and $\mathcal{C}' = \{C'^n,\ \partial'^n\}_{n \geq 0}$ are two cochain complexes, then a cochain transformation $f : \mathcal{C} \to \mathcal{C}'$ is a family of R-module homomorphisms $f^n : C^n \to C'^n$ such that

$$f^{n+1}\partial^n = \partial'^n f^n$$

for each $n \geq 0$. It follows that each f^n maps n-cocycles of $\mathcal{C}$ to n-cocycles of $\mathcal{C}'$ and n-coboundaries of $\mathcal{C}$ to n-coboundaries of $\mathcal{C}'$. Consequently, the cochain transformation f induces a family of homomorphisms

$$\mathrm{H}^n(f) : \mathrm{H}^n(\mathcal{C}) \to \mathrm{H}^n(\mathcal{C}')$$

defined by

$$\mathrm{H}^n(f)\big([c]\big) = \big[f^n(c)\big]$$

for $c \in \mathrm{Ker}(\partial^n)$.

Let us recall the construction of the cochain complex defining the cohomology of groups. We refer the reader to the excellent books [1, 11] for details on cohomology of groups.

Let G be a group and N a left G-module, that is, there is a left action of G on the abelian group N by automorphisms. Set $C^{-1}(G,\ N) = 1$, and $C^0(G,\ N) = N$ viewed as maps from the trivial group to the group N. For each integer $n \geq 1$, let $C^n(G,\ N)$ be the set of all maps

$$\sigma : G^n := \underbrace{G \times \cdots \times G}_{n \text{ copies}} \to N.$$

Each $C^n(G, N)$ is endowed with the structure of an abelian group with respect to the point-wise multiplication of functions, and referred to as the group of *n-cochains*. The *coboundary operator*

$$\partial^n : C^n(G, N) \to C^{n+1}(G, N)$$

is given by

$$\begin{aligned} &\partial^n(\sigma)(g_1, \ldots, g_{n+1}) \\ &= {}^{g_1}\sigma(g_2, \ldots, g_{n+1}) \prod_{k=1}^{n} \sigma(g_1, \ldots, g_k g_{k+1}, \ldots, g_{n+1})^{(-1)^k} \sigma(g_1, \ldots, g_n)^{(-1)^{n+1}} \end{aligned} \tag{2.1}$$

for all $\sigma \in C^n(G, N)$ and $(g_1, \ldots, g_{n+1}) \in G^{n+1}$. It is straightforward to verify that $\partial^n \partial^{n-1}$ is the trivial homomorphism, and thus we obtain a cochain complex

$$\cdots \to C^{n-1}(G, N) \overset{\partial^{n-1}}{\to} C^n(G, N) \overset{\partial^n}{\to} C^{n+1}(G, N) \to \cdots$$

of abelian groups.

Set $\mathrm{Z}^n(G, N) = \mathrm{Ker}(\partial^n)$ the group of *n-cocycles*, and $\mathrm{B}^n(G, N) = \mathrm{Im}(\partial^{n-1})$ the group of *n-coboundaries*. Then the n-dimensional *cohomology group* of G with coefficients in N is the cohomology of the cochain complex $\{C^n(G, N), \partial^n\}_{n \geq 0}$, and denoted by

$$\mathrm{H}^n(G, N) = \mathrm{Z}^n(G, N)/\,\mathrm{B}^n(G, N).$$

Except in Chap. 6, the cohomology groups are written multiplicatively throughout the monograph.

The low dimensional cohomology groups have very interesting interpretations. To be precise,

$$\mathrm{H}^0(G, N) = N^G = \big\{n \in N \mid {}^g n = n \text{ for all } g \in G\big\},$$

the fixed-point set of the action of G on N. The first cohomology group

$$\mathrm{H}^1(G, N) = \mathrm{Z}^1(G, N)/\,\mathrm{B}^1(G, N),$$

where

$$\mathrm{Z}^1(G, N) = \big\{\sigma : G \to N \mid \sigma(g_1 g_2) = \sigma(g_1)\, {}^{g_1}\sigma(g_2)\, \textit{for}\ g_1, g_2 \in G\big\}$$

also called the group of *derivations* or *crossed homomorphisms*, and

$$\mathrm{B}^1(G,\ N) = \big\{\sigma : G \to N \mid \text{there exists } n \in N \text{ such that } \sigma(g) = ({}^{g}n)n^{-1}\ for\ g \in G\big\}$$

also called the group of *inner derivations*. Due to this, the group $\mathrm{Z}^1(G,\ N)$ is also denoted by $\mathrm{Der}(G,\ N)$ in the literature.

The second cohomology group $\mathrm{H}^2(G,\ N)$ classifies equivalence classes of extensions

$$1 \to N \to \Pi \to G \to 1$$

of G by N inducing the given G-module structure on N. For these interpretations and more on cohomological methods in group theory, see [50].

Let G and G' be two groups. Let A be a G-module and A' a G'-module. We say that a pair (α, β) of group homomorphisms $\alpha : G' \to G$ and $\beta : A \to A'$ is *action-compatible* if the following diagram commutes

$$\begin{tikzcd}
G \times A \arrow[r] \arrow[d, shift left=2, "\beta"] & A \arrow[d, "\beta"] \\
G' \times A' \arrow[u, shift left=2, "\alpha"] \arrow[r] & A'.
\end{tikzcd}$$

In other words,

$${}^{g'}\beta(a) = \beta\big({}^{\alpha(g')}a\big)$$

for all $a \in A$ and $g' \in G'$. With this set-up, we have the following result.

Proposition 2.2 *Let (α, β) be an action-compatible pair. Then, for each $n \geq 0$, there is a homomorphism of cohomology groups*

$$(\alpha, \beta)^n : \mathrm{H}^n(G, A) \to \mathrm{H}^n(G', A').$$

Proof Fix $n \geq 0$. For each $\sigma \in C^n(G,\ A)$, define $\sigma' : G'^n \to A'$ by

$$\sigma'(g'_1, g'_2, \ldots, g'_n) = \beta\big(\sigma\big(\alpha(g'_1), \alpha(g'_2), \ldots, \alpha(g'_n)\big)\big)$$

for $(g'_1, g'_2, \ldots, g'_n) \in G'^n$. Then σ' is an element of $C^n(G',\ A')$.

Define $(\alpha, \beta)^n : C^n(G,\ A) \to C^n(G',\ A')$ by setting

$$(\alpha, \beta)^n(\sigma) = \sigma'.$$

It is routine to check that $(\alpha, \beta)^n$ is a homomorphism commuting with the coboundary operators, that is, the following diagram commutes

$$\begin{tikzcd}
C^n(G,\ A) \arrow[r, "(\alpha,\beta)^n"] \arrow[d, "\partial^n"] & C^n(G',\ A') \arrow[d, "\partial^n"] \\
C^{n+1}(G,\ A) \arrow[r, "(\alpha,\beta)^{n+1}"] & C^{n+1}(G',\ A').
\end{tikzcd}$$

Consequently, it follows that $(\alpha,\beta)^n$ preserves both cocycles and coboundaries, and hence induces a map

$$(\alpha,\beta)^n : \mathrm{H}^n(G,\ A) \to \mathrm{H}^n(G',\ A')$$

given by

$$(\alpha,\beta)^n\big([\sigma]\big) = [\sigma'].$$

It is again routine to check that $(\alpha,\beta)^n$ is a group homomorphism. □

In particular, if $G = G'$ and $\alpha = \mathrm{id}_G$, then we write $(\alpha,\beta) = \beta$ and obtain the following

Corollary 2.3 *Let G be a group, A and A' two G-modules, and $\beta : A \to A'$ a G-module homomorphism. Then, for each $n \geq 0$, there is a homomorphism*

$$\beta^n : \mathrm{H}^n(G,\ A) \to \mathrm{H}^n(G,\ A')$$

of cohomology groups.

Similarly, if $A = A'$ and $\beta = \mathrm{id}_A$, then we write $(\alpha,\beta) = \alpha$ and obtain the following

Corollary 2.4 *Let G and G' be two groups and A a module over both G and G'. Let $\alpha : G' \to G$ be an action-compatible homomorphism. Then, for each $n \geq 0$, there is a homomorphism*

$$\alpha^n : \mathrm{H}^n(G,\ A) \to \mathrm{H}^n(G',\ A)$$

of cohomology groups.

Let H be a subgroup of a group G and $\alpha : H \hookrightarrow G$ the inclusion. Let A be an H-module. Define

$$\beta : \mathrm{Hom}_{\mathbb{Z}[H]}\big(\mathbb{Z}[G],\ A\big) \to A$$

by $f \mapsto f(1)$, where 1 is the unity of the group algebra $\mathbb{Z}[G]$. Then the pair (α,β) is action-compatible, and hence induces a homomorphism

$$\mathrm{H}^*\big(G,\ \mathrm{Hom}_{\mathbb{Z}[H]}(\mathbb{Z}[G],\ A)\big) \to \mathrm{H}^*(H,\ A).$$

It is a well-known result, called the Eckmann-Shapiro Lemma, that the above homomorphism is, in fact, an isomorphism (see [11, p.73, Proposition 6.2], [11, p.80, Exercise 2] and [25, Theorem 4]).

Theorem 2.5 *Let H be a subgroup of a group G and A an H-module. Then, for each $n \geq 0$, there is an isomorphism of cohomology groups*

$$\Psi^n : \mathrm{H}^n\big(G,\ \mathrm{Hom}_{\mathbb{Z}[H]}(\mathbb{Z}[G],\ A)\big) \to \mathrm{H}^n(H,\ A).$$

Let A be a G-module and H a subgroup of G. Then A is also an H-module. Further, the group $\mathrm{Hom}_{\mathbb{Z}[H]}(\mathbb{Z}[G],\ A)$ can be turned into a G-module by setting

$$({}^{g}f)(g') = f(g'g)$$

for $g, g' \in G$ and $f \in \mathrm{Hom}_{\mathbb{Z}[H]}(\mathbb{Z}[G],\ A)$. Define a map

$$q : A \to \mathrm{Hom}_{\mathbb{Z}[H]}\big(\mathbb{Z}[G],\ A\big)$$

by setting, for each $a \in A$,

$$q(a)(g) = {}^{g}a$$

for $g \in G$. Then q is a G-module homomorphism since

$$q({}^{g}a)(g') \ = \ {}^{(g'g)}a = q(a)(g'g) = ({}^{g}q(a))(g')$$

for $g, g' \in G$ and $a \in A$. By Corollary 2.3, for each $n \geq 0$, there is a homomorphism of cohomology groups

$$q^n : \mathrm{H}^n(G,\ A) \to \mathrm{H}^n\big(G,\ \mathrm{Hom}_{\mathbb{Z}[H]}(\mathbb{Z}[G],\ A)\big).$$

For each $n \geq 0$, setting $res^G_H = \Psi^n q^n$, we obtain a homomorphism of cohomology groups

$$res^G_H : \mathrm{H}^n(G,\ A) \to \mathrm{H}^n(H,\ A)$$

called the *restriction map*.

Remark 2.6 Let A be a G-module and H a subgroup of G. Then A is also an H-module and the inclusion $H \hookrightarrow G$ is an action-compatible homomorphism. By Corollary 2.4, there is a homomorphism

$$\mathrm{H}^n(G,\ A) \to \mathrm{H}^n(H,\ A)$$

for each $n \geq 0$. A direct check shows that this homomorphism is the same as the restriction homomorphism defined above.

Next, we proceed in the opposite direction. Assume that A is a G-module and H a finite index subgroup of G. Let the index of H in G be n, and $\{g_1, \ldots, g_n\}$ a set of representatives of the right cosets of H in G. Define a map

$$t : \mathrm{Hom}_{\mathbb{Z}[H]}\big(\mathbb{Z}[G],\ A\big) \to A$$

by setting

$$t(f) = \prod\nolimits_{j=1}^{n} {}^{g_j^{-1}}(f(g_j))$$

for $f \in \mathrm{Hom}_{\mathbb{Z}[H]}\big(\mathbb{Z}[G],\ A\big)$. Since, for any $h \in H$,

$${}^{(hg_j)^{-1}}(f(hg_j)) \ = \ {}^{(hg_j)^{-1}h}(f(g_j)) \ = \ {}^{g_j^{-1}}(f(g_j))$$

for each $1 \leq j \leq n$, it follows that the function t is independent of the choice of the coset representatives. Since $\{g_1 g, \ldots, g_n g\}$ is also a set of coset representatives, we obtain

$$\begin{aligned} t({}^{g}f) &= \prod_{j=1}^{n} {}^{g_j^{-1}}(({}^{g}f)(g_j)) \\ &= \prod_{j=1}^{n} {}^{g_j^{-1}}(f(g_j g)) \\ &= {}^{g}(\prod_{j=1}^{n} {}^{(g_j g)^{-1}} f(g_j g)) \\ &= {}^{g}(t(f)), \end{aligned}$$

and hence t is a G-module homomorphism. Now by Corollary 2.3, for each $n \geq 0$, there is a homomorphism

$$t^n : \mathrm{H}^n\big(G,\ \mathrm{Hom}_{\mathbb{Z}[H]}(\mathbb{Z}[G],\ A)\big) \to \mathrm{H}^n(G,\ A).$$

For each $n \geq 0$, set $cores_H^G = t^n(\Psi^n)^{-1}$. Then

$$cores_H^G : \mathrm{H}^n(H,\ A) \to \mathrm{H}^n(G,\ A)$$

is a homomorphism of cohomology groups called the *corestriction map* or the *transfer map*.

Remark 2.7 Let H be a finite index subgroup of a group G. If A is a trivial G-module, then $\mathrm{H}^1(H,\ A) = \mathrm{Hom}(H, A)$ and $\mathrm{H}^1(G,\ A) = \mathrm{Hom}(G, A)$. If $f \in \mathrm{Hom}(H, A)$, then $cores_H^G(f) \in \mathrm{Hom}(G, A)$ is also referred to as the *transfer* of f, since it coincides with the transfer homomorphism given by (1.3).

The following fundamental result relates the restriction and the corestriction maps (see [11, Chapter III, Proposition 9.5(ii)] and [25, Theorem 5]).

Theorem 2.8 *Let A be a G-module and H a subgroup of G of index k. Then, for each $n \geq 0$, the homomorphism*

$$cores_H^G\ res_H^G : \mathrm{H}^n(G,\ A) \to \mathrm{H}^n(G,\ A)$$

is given by $cores_H^G\ res_H^G([\mu]) = [\mu]^k$.

Proof Let the index of H in G be k. Notice that $cores_H^G\ res_H^G = t^n q^n$ for each $n \geq 0$. Further, $tq : A \to A$ is given by

$$t\big(q(a)\big) = \prod\nolimits_{j=1}^{k} {}^{g_j^{-1}}\big(q(a)(g_j)\big) = \prod\nolimits_{j=1}^{k} {}^{g_j^{-1}}({}^{g_j}a) = a^k$$

for $a \in A$. Hence, $cores_H^G\ res_H^G = (tq)^n = t^n q^n$ is the desired map. □

A sequence

$$\cdots \longrightarrow G_{n-1} \xrightarrow{f_{n-1}} G_n \xrightarrow{f_n} G_{n+1} \longrightarrow \cdots$$

of groups G_n and group homomorphisms $f_n : G_n \to G_{n+1}$ is said to be *exact at* G_n if

$$\mathrm{Im}(f_{n-1}) = \mathrm{Ker}(f_n).$$

Further, the sequence is said to be *exact* if it is exact at G_n for each n.

The following result exhibits a long exact sequence of cohomology groups associated to a short exact sequence of G-modules [11, p.71, Proposition 6.1(ii)].

Theorem 2.9 *Let G be a group and*

$$1 \to A' \xrightarrow{i} A \xrightarrow{j} A'' \to 1$$

a short exact sequence of G-modules. Then, for each $n \geq 0$, there is a natural map

$$\delta^n : \mathrm{H}^n(G,\ A'') \to \mathrm{H}^{n+1}(G,\ A'),$$

known as the connecting homomorphism, such that the sequence

$$\cdots \to \mathrm{H}^n(G,\ A') \xrightarrow{i^n} \mathrm{H}^n(G,\ A) \xrightarrow{j^n} \mathrm{H}^n(G,\ A'') \xrightarrow{\delta^n} \mathrm{H}^{n+1}(G,\ A') \to \cdots$$

is exact.

The next result on vanishing of higher dimensional cohomology groups of p-groups is due to Gaschütz [39] (see also [122, Theorem 12.2.1]).

Theorem 2.10 *Let G be a finite p-group and A a G-module which is also a finite p-group. If* $\mathrm{H}^1(G,\ A) = 1$, *then* $\mathrm{H}^k(H,\ A) = 1$ *for all $k \geq 1$ and all subgroups H of G.*

If G is a finite group, then we consider the element

$$N = \sum_{g \in G} g$$

of the integral group algebra $\mathbb{Z}[G]$ of G, called the *norm element* of $\mathbb{Z}[G]$. If A is a G-module, then the fixed-point set of the action of G

$$A^G := \{a \in A \mid {}^g a = a \text{ for all } g \in G\}$$

is a submodule of A. Since A is written multiplicatively, for $a \in A$ and $\sum_{g \in G} n_g g \in \mathbb{Z}[G]$, we use the convention

$$\big(\sum_{g \in G} n_g g\big) a := \prod_{g \in G} ({}^g a)^{n_g}.$$

With the preceding set-up, we state the following well-known result on the cohomology of finite cyclic groups [11, p. 58].

Proposition 2.11 *Let $G = \langle x \rangle$ be a finite cyclic group and A a G-module. Let $\tau : A \to A$ be the trace map given by $\tau(a) = Na$. Then, for all $n \geq 1$, we have*

$$\mathrm{H}^{2n+1}(G,\ A) \cong \mathrm{H}^1(G,\ A) \cong \mathrm{Ker}(\tau)/\big(I(G)A\big)$$

and

$$\mathrm{H}^{2n}(G,\ A) \cong \mathrm{H}^2(G,\ A) \cong A^G/\operatorname{Im}(\tau).$$

We conclude this section with some constructions of derivations. The concept of derivations comes very handy at many instances for constructing automorphisms of finite groups, one such being presented at the end of this section.

Proposition 2.12 *Let $G = \langle x \rangle$ be a finite cyclic group and A a G-module. Let $\tau : A \to A$ be the trace map given by $\tau(a) = Na$. Then for each $a \in \mathrm{Ker}(\tau)$, there exists a unique derivation $\delta : G \to A$ such that $\delta(x) = a$.*

Proof Define $\delta : G \to A$ by setting

$$\delta(x^k) = \left(\sum_{i=0}^{k-1} x^i\right) a.$$

Since $a \in \mathrm{Ker}(\tau)$, it follows that the map δ is well-defined. Clearly, δ is a derivation. The uniqueness follows from the fact that the unique derivation δ for which $\delta(x) = 1$ is the trivial derivation. □

Proposition 2.13 *Let $G = \langle x \rangle \oplus \langle y \rangle$ be a 2-generated abelian group. Let A be a G-module such that $I(G)A \leq A^G$, where $I(G)$ is the augmentation ideal of the integral group algebra of G and A^G is the submodule of invariant elements. Let $\tau_x = \sum_{i \geq 0} x^i$ and $\tau_y = \sum_{i \geq 0} y^i$. Then for each $a, b \in A$ with $\tau_x a = 1$, $\tau_y b = 1$*

and $(-1+y)a = (-1+x)b$, there exists a unique derivation $\delta : G \to A$ such that $\delta(x) = a$ and $\delta(y) = b$.

Proof Define $\delta : G \to A$ by

$$\delta(x^s y^t) = \left(\left(\sum_{i=0}^{s-1} x^i\right) a\right) \left(\left(\sum_{j=0}^{t-1} y^j\right) b\right) \left(\left(s(-1+y^t)\right) a\right).$$

Since $(-1+y)a \in I(G)A$ and $I(G)A \leq A^G$, we have

$$\left(s(-1+y^t)\right)a = \left(s(1+y+y^2+\cdots+y^{t-1})(-1+y)\right)a = \left(st(-1+y)\right)a = \left(t(-1+x^s)\right)b.$$

A direct computation using the hypothesis and preceding equation shows that δ is a derivation satisfying the required properties. The uniqueness is obvious. □

The following basic result is due to Gavioli [42, Section 2].

Proposition 2.14 *Let G be a finite group and N an abelian normal subgroup of G viewed as a G-module via the conjugation action. Then for any derivation $\delta : G \to N$, there exists an endomorphism ϕ of G given by $\phi(g) = \delta(g)g$ for all $g \in G$. Further, if $\delta(N) = 1$, then ϕ is an automorphism of G.*

Proof For $g, h \in G$, we have

$$\phi(gh) = \delta(gh)gh = \delta(g)\, {}^g\delta(h)\, gh = \delta(g)g\delta(h)h = \phi(g)\phi(h),$$

which implies that ϕ is a homomorphism. Further, if $\delta(N) = 1$, then $\phi(g) = 1$ implies that $g = 1$. Hence, ϕ is an automorphism of G. □

2.2 Group Extensions

Let H and N be two groups. Then an *extension* $\mathcal{E}$ of H by N is an exact sequence of the form

$$\mathcal{E} : 1 \to N \xrightarrow{i} G \xrightarrow{\pi} H \to 1.$$

For simplicity, we consider N as a subgroup of G, and hence do not name the inclusion $N \hookrightarrow G$ explicitly, unless needed. We say that $\mathcal{E}$ is an *abelian extension* if N is abelian, and a *central extension* if $N \leq \mathrm{Z}(G)$.

Two group extensions

$$\mathcal{E}_1 : 1 \to N \to G_1 \xrightarrow{\pi_1} H \to 1$$

and

$$\mathcal{E}_2 : 1 \to N \to G_2 \xrightarrow{\pi_2} H \to 1$$

are said to be *equivalent* if there exists a homomorphism $\gamma : G_1 \to G_2$ such that the following diagram commutes

$$\begin{tikzcd}
1 \arrow[r] & N \arrow[r] \arrow[d, "\mathrm{id}_N"] & G_1 \arrow[r, "\pi_1"] \arrow[d, "\gamma"] & H \arrow[r] \arrow[d, "\mathrm{id}_H"] & 1 \\
1 \arrow[r] & N \arrow[r] & G_2 \arrow[r, "\pi_2"] & H \arrow[r] & 1.
\end{tikzcd}$$

Any homomorphism $\gamma : G_1 \to G_2$, as in the preceding commutative diagram, is called an *equivalence* of $\mathcal{E}_1$ and $\mathcal{E}_2$. It is easy to see that the preceding relation, between extensions of the group N by the group H, is an equivalence relation (see [85]). Let $\mathrm{Ext}(H, N)$ denote the set of equivalence classes of extensions of H by N and $[\mathcal{E}]$ the equivalence class of an extension $\mathcal{E}$.

Let $1 \to N \to G \overset{\pi}{\to} H \to 1$ be an extension of H by N. Then a *right transversal* is a map $t : H \to G$ satisfying

$$\pi\big(t(x)\big) = x$$

for all $x \in H$. A transversal which is a group homomorphism is called a *section*. An extension of groups admitting a section is called a *split extension*.

Let $1 \to N \to G \overset{\pi}{\to} H \to 1$ be an extension of H by N and $t : H \to G$ a fixed *right transversal* such that $t(1) = 1$. Then each $g \in G$ can be written uniquely as $g = nt(x)$ for some $x \in H$ and $n \in N$ satisfying $\pi(g) = x$. Let

$$\chi : H \to \mathrm{Aut}(N) \tag{2.15}$$

be the map defined by

$$\chi(x)\big(n\big) = t(x)nt(x)^{-1}$$

for $x \in H$ and $n \in N$. For $x, y \in H$, we then have

$$\pi(t(xy)) = xy = \pi(t(x))\pi(t(y)) = \pi(t(x)t(y)).$$

Thus, there exists a unique element, say $\mu(x, y) \in N$, such that

$$t(x)t(y) = \mu(x, y)t(xy).$$

For each $n \in N$, let $\iota_n : N \to N$ be the inner automorphism of N induced by n:

$$\iota_n(z) = nzn^{-1}$$

for all $z \in N$. Thus,

$$\chi(x)\chi(y) = \iota_{\mu(x,y)}\chi(xy) \tag{2.16}$$

for all $x, y \in H$. We notice that the map $\chi : H \to \mathrm{Aut}(N)$ is, in general, not a homomorphism. However, clearly χ composed with the natural projection

$$\mathrm{Aut}(N) \to \mathrm{Out}(N) := \mathrm{Aut}(N)/\,\mathrm{Inn}(N)$$

is a homomorphism, denoted by

$$\overline{\chi} : H \to \mathrm{Out}(N).$$

Proposition 2.17 *The homomorphism* $\overline{\chi} : H \to \mathrm{Out}(N)$ *is independent of the choice of the transversal* $t : H \to G$. *Furthermore, if* $\overline{\chi}_1$, $\overline{\chi}_2$ *are the homomorphisms associated to two equivalent extensions of* H *by* N, *then* $\overline{\chi}_1 = \overline{\chi}_2$.

Proof Let $\mathcal{E} : 1 \to N \to G \to H \to 1$ be an extension of H by N. For $i = 1,\ 2$, let $t_i : H \to G$ be transversals from H to G and $\chi_i : H \to \mathrm{Aut}(N)$ the associated maps. Since both t_1 and t_2 are transversals of H in G, there exists a map $\lambda : H \to N$ such that

$$t_2(x) = \lambda(x)t_1(x)$$

for all $x \in H$. Consequently, we get

$$\chi_2(x) = \iota_{\lambda(x)}\chi_1(x)$$

for all $x \in H$. Hence, the associated homomorphisms $\overline{\chi}_i : H \to \mathrm{Out}(N)$ for $i = 1,\ 2$ are equal.

Let $\mathcal{E}_i : 1 \to N \to G_i \overset{\pi_i}{\to} H \to 1$ for $i = 1,\ 2$ be two equivalent extensions and $\gamma : G_1 \to G_2$ an equivalence. Then we have the commutative diagram

$$\begin{tikzcd}
1 \arrow[r] & N \arrow[r] \arrow[d, "\mathrm{id}_N"] & G_1 \arrow[r, "\pi_1"] \arrow[d, "\gamma"] & H \arrow[r] \arrow[d, "\mathrm{id}_H"] & 1 \\
1 \arrow[r] & N \arrow[r] & G_2 \arrow[r, "\pi_2"] & H \arrow[r] & 1.
\end{tikzcd}$$

For $i = 1,\ 2$, let $t_i : H \to G_i$ be transversals and $\chi_i : H \to \mathrm{Aut}(N)$ the respective associated maps. Commutativity of the preceding diagram implies that $\gamma(n) = n$ for all $n \in N$, and

$$\pi_2\big(\gamma(t_1(x))\big) = \pi_1\big(t_1(x)\big) = x = \pi_2\big(t_2(x)\big)$$

for all $x \in H$. Thus, for each $x \in H$, there exists an element, say $\lambda(x) \in N$, such that

$$\lambda(x)\gamma\big(t_1(x)\big) = t_2(x).$$

For $n \in N$, we then have

$$\begin{aligned}\chi_2(x)\big(n\big) &= t_2(x)nt_2(x)^{-1}\\ &= \lambda(x)\gamma\big(t_1(x)\big)n\gamma\big(t_1(x)\big)^{-1}\lambda(x)^{-1}\\ &= \lambda(x)\gamma\big(\chi_1(x)(n)\big)\lambda(x)^{-1}\\ &= \iota_{\lambda(x)}\chi_1(x)(n).\end{aligned}$$

Hence, $\chi_2(x) = \iota_{\lambda(x)}\chi_1(x)$ for all $x \in H$, and consequently, the associated homomorphisms $\overline{\chi}_1, \overline{\chi}_2 : H \to \mathrm{Out}(N)$ are equal. □

In view of the preceding proposition, to every equivalence class of extensions $[\mathcal{E}] \in \mathrm{Ext}(H,\ N)$ there is associated a unique homomorphism $\overline{\chi} : H \to \mathrm{Out}(N)$, called the *coupling* associated to $[\mathcal{E}]$.

Let H and N be two groups and $\alpha : H \to \mathrm{Out}(N)$ a coupling. Set

$$\mathrm{Ext}_\alpha(H,\ N) = \big\{[\mathcal{E}] \in \mathrm{Ext}(H,\ N) \mid \alpha \text{ is the coupling associated to } [\mathcal{E}]\big\}.$$

Thus, we can write

$$\mathrm{Ext}(H,\ N) = \bigsqcup_\alpha \mathrm{Ext}_\alpha(H,\ N),$$

where α runs over all couplings $H \to \mathrm{Out}(N)$.

We conclude this section with the following

Remark 2.18 Given two groups H and N, a homomorphism from H to $\mathrm{Out}(N)$ is called an *abstract kernel*. It must be noted that not every abstract kernel is a coupling; however, if $\mathrm{Z}(N) = 1$, then every abstract kernel is a coupling (see [85, Chapter 4, pp. 129–131], [6] or [77]).

2.3 Action of Cohomology Group on Extensions

Given groups $H,\ N$ and a coupling $\alpha : H \to \mathrm{Out}(N)$, we construct a free and transitive action of the cohomology group $\mathrm{H}^2\big(H,\ \mathrm{Z}(N)\big)$ on the set $\mathrm{Ext}_\alpha(H,\ N)$. The idea can be found, for example, in [85].

Let $\mathcal{E} : 1 \to N \to G \to H \to 1$ be an extension and $t : H \to G$ a transversal with $t(1) = 1$. Then, as shown in Sect. 2.2, for all $x, y \in H$, there exists a unique element, say $\mu(x,\ y) \in N$, such that

$$t(x)t(y) = \mu(x,\ y)t(xy).$$

We notice that μ is a map from $H \times H$ to N such that

$$\mu(x,\ 1) = 1 = \mu(1,\ x)$$

for all $x \in H$. It is easy to check that the choice of a transversal $t : H \to G$, and the resulting maps $\mu : H \times H \to N$ and $\chi : H \to \mathrm{Aut}(N)$, as explained in Sect. 2.2, have the following properties.

Proposition 2.19 *Let H and N be two groups, and $\mathcal{E}, \mathcal{E}_1, \mathcal{E}_2$ be extensions of H by N. Then the following statements hold:*

(1) Let t be a transversal of $\mathcal{E}$ and μ be the associated map. Then

$$\mu(x, y)\mu(xy, z) = {}^{\chi(x)}\mu(y, z)\mu(x, yz) \tag{2.20}$$

for all $x, y, z \in H$.

(2) Let t_1 and t_2 be two transversals of $\mathcal{E}$ and μ_1 and μ_2 be the associated maps. Then there exists a map $\lambda : H \to N$ such that

$$t_2(x) = \lambda(x)t_1(x)$$

for all $x \in H$, and

$$\mu_2(x, y) = \lambda(x)\,{}^{\chi_1(x)}\lambda(y)\mu_1(x, y)\lambda(xy)^{-1} \tag{2.21}$$

for all $x, y \in H$.

(3) Let μ_1 and μ_2 be the maps associated to the transversals t_1 and t_2 of $\mathcal{E}_1$ and $\mathcal{E}_2$ respectively. If $\mathcal{E}_1$ and $\mathcal{E}_2$ are equivalent extensions, then there exists a map $\lambda : H \to N$ such that (2.21) holds.

The condition given by (2.20) is referred to as the *cocycle condition*. In fact, if N is abelian, then $\mu : H \times H \to N$ is a 2-cocycle (see (2.1) for $n = 2$).

Let $\alpha : H \to \mathrm{Out}(N)$ be a coupling and

$$\mathcal{Z}^2_\alpha(H, N) := \big\{(\chi, \mu) \mid \chi, \mu \text{ satisfy (2.16), (2.20) and } \alpha = \overline{\chi}\big\}.$$

Elements of $\mathcal{Z}^2_\alpha(H, N)$ are called *associated pairs*. Two associated pairs (χ_1, μ_1), (χ_2, μ_2) are called *equivalent*, written $(\chi_1, \mu_1) \sim (\chi_2, \mu_2)$, if there exists a map $\lambda : H \to N$ such that

$$\chi_2(x) = \iota_{\lambda(x)}\chi_1(x) \text{ and } \mu_2(x, y) = \lambda(x)\,{}^{\chi_1(x)}\lambda(y)\mu_1(x, y)\lambda(xy)^{-1} \tag{2.22}$$

for all $x, y \in H$. A routine check shows that the above relation is an equivalence relation on the set $\mathcal{Z}^2_\alpha(H, N)$. Define

$$\mathcal{H}^2_\alpha(H, N) = \mathcal{Z}^2_\alpha(H, N)/_\sim,$$

and denote by $[(\chi, \mu)] \in \mathcal{H}^2_\alpha(H, N)$ the equivalence class of the associated pair (χ, μ).

Notice that *if N is abelian, then $\mathcal{H}^2_\alpha(H, N)$ is precisely the second cohomology group $\mathrm{H}^2_\alpha(H, N)$ with N viewed as an H-module via α.*

We have the following result [85, Chapter 4].

Theorem 2.23 *Let H, N be two groups and $\alpha : H \to \mathrm{Out}(N)$ a coupling. Then there is a bijection*

$$\mathrm{Ext}_\alpha(H, N) \longleftrightarrow \mathcal{H}^2_\alpha(H, N).$$

Proof Define $\Phi : \mathrm{Ext}_\alpha(H, N) \to \mathcal{H}^2_\alpha(H, N)$ as follows. Let

$$\mathcal{E} : 1 \to N \to G \to H \to 1$$

be an extension with coupling α. Fix a transversal $t : H \to G$ such that $t(1) = 1$. Then there exist maps $\chi : H \to \mathrm{Aut}(N)$ and $\mu : H \times H \to N$ satisfying (2.16), (2.20), and inducing α. Consequently, we get $[(\chi, \mu)] \in \mathcal{H}^2_\alpha(H, N)$. Set

$$\Phi\big([\mathcal{E}]\big) = [(\chi, \mu)].$$

By Propositions 2.17 and 2.19, it follows that the map Φ is well-defined.

Next we define a map $\Psi : \mathcal{H}^2_\alpha(H, N) \to \mathrm{Ext}_\alpha(H, N)$ as follows. Given an associated pair (χ, μ), we define a binary operation on the set $H \times N$ by setting

$$(x, n)(y, m) = \big(xy, n^{\chi(x)} m \mu(x, y)\big)$$

for all $n, m \in N$ and $x, y \in H$. It is routine to check that the preceding binary operation induces a group structure on $H \times N$, and we denote the resulting group by $G(\chi, \mu)$. Consider the extension

$$\mathcal{E}(\chi, \mu) : 1 \to N \xrightarrow{i'} G(\chi, \mu) \xrightarrow{\pi'} H \to 1,$$

where $i'(n) = (1, n)$ and $\pi'(x, n) = x$ for $n \in N$ and $x \in H$. Define Ψ by setting

$$\Psi\big([(\chi, \mu)]\big) = [\mathcal{E}(\chi, \mu)].$$

One can then check that Ψ is well-defined and the two maps Φ and Ψ are inverses of each other. □

By Theorem 2.23, we have $[\mathcal{E}] = [\mathcal{E}(\chi, \mu)]$ for each $[\mathcal{E}] \in \mathrm{Ext}_\alpha(H, N)$. Further, as a consequence of Theorem 2.23, we obtain the following well-known correspondence [11, p. 93, Theorem 3.12].

Theorem 2.24 *Let $\alpha : H \to \mathrm{Aut}(N)$ be a group homomorphism inducing an H-module structure on an abelian group N. Then there is a bijection*

$$\mathrm{Ext}_\alpha(H, N) \longleftrightarrow \mathrm{H}^2(H, N).$$

The following result is of independent interest.

Proposition 2.25 *Let $\alpha : H \to \mathrm{Out}(N)$ be a coupling and (χ_1, μ_1) an associated pair. If $\chi_2 : H \to \mathrm{Aut}(N)$ is any map with $\overline{\chi}_2 = \alpha$, then there exists a map $\mu_2 : H \times H \to N$ such that (χ_2, μ_2) is an associated pair satisfying $[(\chi_1, \mu_1)] = [(\chi_2, \mu_2)]$.*

Proof In view of the Theorem 2.23, there exists an extension

$$\mathcal{E} : 1 \to N \to G \to H \to 1$$

corresponding to the associated pair (χ_1, μ_1). Let $t_1 : H \to G$ be a transversal inducing the associated pair (χ_1, μ_1). Since $\overline{\chi}_1 = \alpha = \overline{\chi}_2$, there exists a map $\lambda : H \to N$ such that

$$\chi_2(x) = \iota_{\lambda(x)}\chi_1(x)$$

for all $x \in H$. Define a transversal $t_1' : H \to G$ by

$$t_1'(x) = \lambda(x)t_1(x)$$

for $x \in H$. Consequently, we have an associated pair (χ_1', μ_1') which is equivalent to (χ_1, μ_1). But,

$$\chi_1'(x) = \iota_{\lambda(x)}\chi_1(x) = \chi_2(x)$$

for all $x \in H$, and hence $[(\chi_1, \mu_1)] = [(\chi_2, \mu_2)]$, where $\mu_2 = \mu_1'$. □

Let $\alpha : H \to \mathrm{Out}(N)$ be a homomorphism, and

$$\tilde{\alpha} : H \to \mathrm{Aut}\big(\mathrm{Z}(N)\big)$$

the homomorphism obtained by composing α with the homomorphism

$$\mathrm{Out}(N) \to \mathrm{Aut}\big(\mathrm{Z}(N)\big)$$

induced by the restriction homomorphism $\mathrm{Aut}(N) \to \mathrm{Aut}(\mathrm{Z}(N))$. Clearly, if N is abelian, then $\alpha = \tilde{\alpha}$.

Let $\mathrm{H}^2\big(H, \mathrm{Z}(N)\big)$ be the second cohomology group of H with coefficients in $\mathrm{Z}(N)$ regarded as an H-module via $\tilde{\alpha}$. Recall that, the multiplication of cocycles is element-wise, that is,

$$\nu\mu(x, y) = \nu(x, y)\mu(x, y)$$

for all $x, y \in H$. There exists a free and transitive action of the group $\mathrm{H}^2\big(H, \mathrm{Z}(N)\big)$ on the set $\mathrm{Ext}_\alpha(H, N)$ (see [11, p. 105, Theorem 6.6] or [85, Theorem 8.8]). To be precise, we have

Theorem 2.26 *Let $[\mathcal{E}] \in \mathrm{Ext}_\alpha(H, N)$ and (χ, μ) an associated pair for $\mathcal{E}$. Then, for $[\nu] \in \mathrm{H}^2\big(H, \mathrm{Z}(N)\big)$, the operation*

$$^{[\nu]}[\mathcal{E}] = {}^{[\nu]}[\mathcal{E}(\chi,\ \mu)] = [\mathcal{E}(\chi,\ \nu\mu)] \tag{2.27}$$

defines a free and transitive action of the group $\mathrm{H}^2(H,\ \mathrm{Z}(N))$ *on the set* $\mathrm{Ext}_\alpha(H,\ N)$.

Proof It is routine to check that the action (2.27) is well-defined. Let $[\mathcal{E}] \in \mathrm{Ext}_\alpha(H,\ N)$ and $[\nu] \in \mathrm{H}^2\big(H,\ \mathrm{Z}(N)\big)$ be such that $^{[\nu]}[\mathcal{E}] = [\mathcal{E}]$. Then

$$[(\chi,\ \nu\mu)] = [(\chi,\ \mu)],$$

and hence there exists a map $\lambda : H \to N$ such that

$$\chi(x) = \iota_{\lambda(x)}\chi(x) \tag{2.28}$$

and

$$\nu(x, y)\mu(x,\ y) = \lambda(x)\,{}^{\chi(x)}\lambda(y)\mu(x,\ y)\lambda(xy)^{-1} \tag{2.29}$$

for all $x,\ y \in H$. The equation (2.28) implies that $\lambda(x) \in \mathrm{Z}(N)$ for all $x \in H$. Consequently, (2.29) implies that

$$\nu(x,\ y) = {}^{\chi(x)}\lambda(y)\lambda(xy)^{-1}\lambda(x)$$

for all $x,\ y \in H$. Thus, $[\nu] = 1$, and hence the action is free.

Let $[\mathcal{E}_1]$ and $[\mathcal{E}_2]$ be two elements in $\mathrm{Ext}_\alpha(H,\ N)$. Then for $i = 1,\ 2$, $[\mathcal{E}_i] = [\mathcal{E}_i(\chi_i,\ \mu_i)]$ for some associated pair $(\chi_i,\ \mu_i)$. By Proposition 2.25, we construct μ_1' such that $(\chi_2,\ \mu_1')$ is an associated pair with

$$[\mathcal{E}_1(\chi_1,\ \mu_1)] = [\mathcal{E}_1(\chi_2,\ \mu_1')].$$

We set

$$\nu(x,\ y) := \mu_1'(x, y)\mu_2(x, y)^{-1}$$

for $x,\ y \in H$. Then it follows that $\nu(x, y) \in \mathrm{Z}(N)$ and

$$\nu : H \times H \to Z(N)$$

is a 2-cocycle. Thus, we have

$$[\mathcal{E}_1] = [\mathcal{E}_1(\chi_1,\ \mu_1)] = [\mathcal{E}_1(\chi_2,\ \mu_1')] = [\mathcal{E}_1(\chi_2,\ \nu\mu_2)] = {}^{[\nu]}[\mathcal{E}_2(\chi_2,\ \mu_2)] = {}^{[\nu]}[\mathcal{E}_2].$$

Hence, the action (2.27) is transitive, and the proof is complete. □

Since the action (2.27) is free and transitive, as a consequence of the preceding theorem, we have

Corollary 2.30 *There is a bijection*

$$\mathrm{Ext}_\alpha(H,\ N) \longleftrightarrow \mathrm{H}^2\big(H,\ \mathrm{Z}(N)\big). \tag{2.31}$$

Remark 2.32 Combining Theorem 2.24 and (2.31), we see that there is a bijection

$$\mathrm{Ext}_\alpha(H,\ N) \longleftrightarrow \mathrm{Ext}_{\tilde{\alpha}}\big(H,\ \mathrm{Z}(N)\big). \tag{2.33}$$

2.4 Action of Automorphism Group on Extensions

Let H and N be two groups. We construct a natural action, first considered by Buckley [14], of the group $\mathrm{Aut}(H) \times \mathrm{Aut}(N)$ on the set $\mathrm{Ext}(H,\ N)$ of all equivalence classes of extensions of H by N.

Let $\alpha : H \to \mathrm{Out}(N)$ be a coupling. To each extension

$$\mathcal{E} : 1 \longrightarrow N \xrightarrow{i} G \xrightarrow{\pi} H \longrightarrow 1$$

representing an element of $\mathrm{Ext}_\alpha(H,\ N)$, and to each $(\phi,\ \theta) \in \mathrm{Aut}(H) \times \mathrm{Aut}(N)$, we associate the following extension

$$^{(\phi,\,\theta)}\mathcal{E} : 1 \longrightarrow N \xrightarrow{i\theta^{-1}} G \xrightarrow{\phi\pi} H \longrightarrow 1.$$

Notice that this association maps equivalent extensions to equivalent extensions. Thus, for $(\phi,\ \theta) \in \mathrm{Aut}(H) \times \mathrm{Aut}(N)$ and $[\mathcal{E}] \in \mathrm{Ext}_\alpha(H, N)$, we can define an operation by setting

$$^{(\phi,\,\theta)}[\mathcal{E}] := [^{(\phi,\,\theta)}\mathcal{E}]. \tag{2.34}$$

For $(\phi_1,\ \theta_1),\ (\phi_2,\ \theta_2) \in \mathrm{Aut}(H) \times \mathrm{Aut}(N)$ and $[\mathcal{E}] \in \mathrm{Ext}_\alpha(H, N)$, we have

$$\begin{aligned} ^{(\phi_1,\,\theta_1)(\phi_2,\,\theta_2)}[\mathcal{E}] &= {}^{(\phi_1\phi_2,\,\theta_1\theta_2)}[\mathcal{E}] \\ &= [^{(\phi_1\phi_2,\,\theta_1\theta_2)}\mathcal{E}] \\ &= {}^{(\phi_1,\,\theta_1)}[^{(\phi_2,\,\theta_2)}\mathcal{E}] \\ &= {}^{(\phi_1,\,\theta_1)}\big(^{(\phi_2,\,\theta_2)}[\mathcal{E}]\big). \end{aligned}$$

If ϕ and θ are both identity automorphisms, then clearly $^{(\phi,\,\theta)}[\mathcal{E}] = [\mathcal{E}]$. Hence,

the operation (2.34) *defines on the set* $\mathrm{Ext}(H,\ N)$ *an action of the group* $\mathrm{Aut}(H) \times \mathrm{Aut}(N)$.

Let $\mathcal{E} : 1 \longrightarrow N \xrightarrow{i} G \xrightarrow{\pi} H \longrightarrow 1$ be an extension with coupling α and $t : H \to G$ a transversal. If $\chi : H \to \mathrm{Aut}(N)$ is the function (2.15) associated to t, then

$$^{\chi(x)}n = i^{-1}\big(t(x)i(n)t(x)^{-1}\big)$$

for $x \in H$ and $n \in N$. Let $t_1 : H \to G$ be given by

$$t_1(x) = t\big(\phi^{-1}(x)\big)$$

for $x \in H$. Then t_1 is a right transversal for H in G in the extension ${}^{(\phi,\,\theta)}\mathcal{E}$. Let $\chi_1 : H \to \mathrm{Aut}(N)$ be the function associated to t_1. Then

$$\begin{aligned} {}^{\chi_1(x)}n &= \theta\, i^{-1}\big(t_1(x) i \theta^{-1}(n) t_1(x)^{-1}\big) \\ &= \theta\, i^{-1}\big(t\big(\phi^{-1}(x)\big) i \theta^{-1}(n) t\big(\phi^{-1}(x)\big)^{-1}\big) \\ &= \theta\big({}^{\chi(\phi^{-1}(x))}(\theta^{-1}(n))\big) \end{aligned}$$

for all $x \in H$ and $n \in N$. Thus, $\chi_1(x) = \theta\chi(\phi^{-1}(x))\theta^{-1}$ for all $x \in H$, and hence the coupling corresponding to the extension ${}^{(\phi,\,\theta)}\mathcal{E}$ is given by

$$x \mapsto \iota_{\overline{\theta}}\alpha\phi^{-1}(x),$$

where $\overline{\theta} = \mathrm{Inn}(N)\theta$ is the image of θ under the canonical projection $\mathrm{Aut}(N) \to \mathrm{Out}(N)$. Thus, the pair $(\phi,\,\theta)$ maps elements of the set $\mathrm{Ext}_\alpha(H,\,N)$ to elements of the $\mathrm{Ext}_{\iota_{\overline{\theta}}\alpha\phi^{-1}}(H,\,N)$.

Given a coupling $\alpha : H \to \mathrm{Out}(N)$, let $C_\alpha(H,\,N)$ denote the set of all pairs $(\phi,\,\theta) \in \mathrm{Aut}(H) \times \mathrm{Aut}(N)$ which keep the subset $\mathrm{Ext}_\alpha(H,\,N)$ of $\mathrm{Ext}(H,\,N)$ invariant under the action given in (2.34). More precisely,

$$\begin{aligned} C_\alpha(H,\,N) &= \big\{(\phi,\,\theta) \in \mathrm{Aut}(H) \times \mathrm{Aut}(N) \mid \iota_{\overline{\theta}}\alpha\phi^{-1} = \alpha\big\} \qquad (2.35) \\ &= \big\{(\phi,\,\theta) \in \mathrm{Aut}(H) \times \mathrm{Aut}(N) \mid \overline{\theta}\alpha(x)\overline{\theta}^{-1} = \alpha\big(\phi(x)\big) \\ &\qquad \text{for all } x \in H\big\}. \end{aligned}$$

In other words, a pair $(\phi,\,\theta) \in C_\alpha(H,\,N)$ if and only if the following diagram is commutative

$$\begin{tikzcd} H \arrow[r, "\alpha"] \arrow[d, "\phi"] & \mathrm{Out}(N) \arrow[d, "\iota_{\overline{\theta}}"] \\ H \arrow[r, "\alpha"] & \mathrm{Out}(N). \end{tikzcd}$$

We refer to elements of $C_\alpha(H,\,N)$ as *α-compatible pairs* (see [73, 126]). It is easily seen that $C_\alpha(H,\,N)$ is a subgroup of $\mathrm{Aut}(H) \times \mathrm{Aut}(N)$, which we call *the group of α-compatible pairs*.

Notice that, if $\alpha : H \to \mathrm{Out}(N)$ is the trivial homomorphism, then

$$C_\alpha(H,\,N) = \mathrm{Aut}(H) \times \mathrm{Aut}(N).$$

The effect of triviality of the coupling α on a given extension is investigated later in Theorem 2.59. In case of no ambiguity, that is, when the groups H and N are clear from the context, we write C_α in place of $C_\alpha(H, N)$.

2.5 Action of Automorphism Group on Cohomology

Given two groups H, N and a coupling $\alpha : H \to \mathrm{Out}(N)$, as observed by Robinson [104], the group C_α acts on the group $\mathrm{H}^2\big(H, \mathrm{Z}(N)\big)$ in a natural way, which we discuss in this section.

For $(\phi, \theta) \in C_\alpha$ and $\nu \in \mathrm{Z}^2\big(H, \mathrm{Z}(N)\big)$, we define

$$^{(\phi,\theta)}\nu(x, y) = \theta\big(\nu(\phi^{-1}(x), \phi^{-1}(y))\big) \tag{2.36}$$

for all $x, y \in H$. It is easy to check that $^{(\phi,\theta)}\nu \in \mathrm{Z}^2\big(H, \mathrm{Z}(N)\big)$; and further that if $\nu \in \mathrm{B}^2\big(H, \mathrm{Z}(N)\big)$, then $^{(\phi,\theta)}\nu \in \mathrm{B}^2\big(H, \mathrm{Z}(N)\big)$. Thus, for $(\phi, \theta) \in C_\alpha$ and $[\nu] \in \mathrm{H}^2\big(H, \mathrm{Z}(N)\big)$, setting

$$^{(\phi,\theta)}[\nu] = [^{(\phi,\theta)}\nu] \tag{2.37}$$

defines a map

$$C_\alpha \times \mathrm{H}^2\big(H, \mathrm{Z}(N)\big) \to \mathrm{H}^2\big(H, \mathrm{Z}(N)\big)$$

which turns out to be a well-defined action of C_α on $\mathrm{H}^2\big(H, \mathrm{Z}(N)\big)$.

It is worth noting that the above action is simply the action of C_α on $\mathrm{Ext}_\alpha(H, N)$ transferred to $\mathrm{H}^2\big(H, \mathrm{Z}(N)\big)$ via the bijection $\mathrm{Ext}_\alpha(H, N) \leftrightarrow \mathrm{H}^2\big(H, \mathrm{Z}(N)\big)$ of Corollary 2.30.

We set

$$\Gamma = C_\alpha \ltimes \mathrm{H}^2\big(H, \mathrm{Z}(N)\big),$$

the semi-direct product of C_α and $\mathrm{H}^2\big(H, \mathrm{Z}(N)\big)$ with respect to the action as defined in (2.37). By definition, the elements of Γ are formal products ch with $c \in C_\alpha$ and $h \in \mathrm{H}^2\big(H, \mathrm{Z}(N)\big)$. For $c_1h_1, c_2h_2 \in \Gamma$, we have

$$(c_1h_1)(c_2h_2) = (c_1c_2)(h_1{}^{c_1}h_2).$$

The above action of C_α on $\mathrm{Ext}_\alpha(H, N)$ and the action of $\mathrm{H}^2\big(H, \mathrm{Z}(N)\big)$ on $\mathrm{Ext}_\alpha(H, N)$, as given in Theorem 2.26, together yield an action of Γ on $\mathrm{Ext}_\alpha(H, N)$ [74, Theorem 2.3]. More precisely, given a coupling $\alpha : H \to \mathrm{Out}(N)$, we have

Theorem 2.38 *There is an action of the group* Γ *on the set* $\mathrm{Ext}_\alpha(H, N)$ *defined by setting*

$$^{ch}[\mathcal{E}] = {}^{h}\big({}^{c}[\mathcal{E}]\big),$$

for $h \in \mathrm{H}^2\big(H, \mathrm{Z}(N)\big)$*,* $c \in C_\alpha$ *and* $[\mathcal{E}] \in \mathrm{Ext}_\alpha(H, N)$.

Further, the stabilizer $\Gamma_{[\mathcal{E}]}$ *of* $[\mathcal{E}]$ *in* Γ *is a complement of* $\mathrm{H}^2\big(H,\, \mathrm{Z}(N)\big)$ *in* Γ *and* $\{\Gamma_{[\mathcal{E}]} \mid [\mathcal{E}] \in \mathrm{Ext}_\alpha(H,\, N)\}$ *is a single conjugacy class of subgroups of* Γ.

Proof To prove that Γ acts on $\mathrm{Ext}_\alpha(H,\, N)$, it suffices to show that

$$^{c}\big(^{h}[\mathcal{E}]\big) = {}^{^{c}h}\big(^{c}[\mathcal{E}]\big)$$

for each $[\mathcal{E}] \in \mathrm{Ext}_\alpha(H,\, N)$, $c \in C_\alpha$ and $h \in \mathrm{H}^2\big(H,\, \mathrm{Z}(N)\big)$.

By Theorem 2.23, there is an associated pair $(\chi,\, \mu)$ for the extension $\mathcal{E}$. By the same theorem, there is an associated pair $(^{c}\chi,\, ^{c}\mu)$ for the extension $^{c}\mathcal{E}$, where $^{c}\mu$ is precisely the action given in (2.36). Further, the corresponding extensions $\mathcal{E}(^{c}\chi,\, ^{c}\mu)$ and $^{c}\mathcal{E}(\chi,\, \mu)$ are equivalent. Let $h = [\nu] \in \mathrm{H}^2\big(H,\, \mathrm{Z}(N)\big)$ for some $\nu \in \mathrm{Z}^2\big(H,\, \mathrm{Z}(N)\big)$. Then, by Theorem 2.26, we have

$$\begin{aligned} ^{c}\Big(^{h}[\mathcal{E}]\Big) &= {}^{c}\Big(^{[\nu]}[\mathcal{E}(\chi,\, \mu)]\Big) = {}^{c}[\mathcal{E}(\chi,\, \nu\mu)] = \big[\mathcal{E}\big(^{c}\chi,\, ^{c}(\nu\mu)\big)\big] \\ &= \big[\mathcal{E}\big(^{c}\chi,\, ^{c}\nu\, ^{c}\mu\big)\big] = {}^{[^{c}\nu]}\big[\mathcal{E}\big(^{c}\chi,\, ^{c}\mu\big)\big] = {}^{^{c}[\nu]}\Big(^{c}[\mathcal{E}\big(\chi,\, \mu\big)]\Big) \\ &= {}^{^{c}h}\Big([^{c}\mathcal{E}]\Big). \end{aligned}$$

Let $\gamma \in \Gamma$. Since $\mathrm{H}^2\big(H,\, \mathrm{Z}(N)\big)$ acts transitively on $\mathrm{Ext}_\alpha(H,\, N)$, there is an element $h \in \mathrm{H}^2\big(H,\, \mathrm{Z}(N)\big)$ such that $^{\gamma}[\mathcal{E}] = {}^{h}[\mathcal{E}]$. Thus, $^{h^{-1}\gamma}[\mathcal{E}] = [\mathcal{E}]$, and hence $h^{-1}\gamma \in \Gamma_{[\mathcal{E}]}$, the stabilizer of $[\mathcal{E}]$ in Γ. Consequently, $\gamma = h\delta$ for some $\delta \in \Gamma_{[\mathcal{E}]}$, and hence $\Gamma = \mathrm{H}^2\big(H,\, \mathrm{Z}(N)\big)\Gamma_{[\mathcal{E}]}$. Further, let $h \in \mathrm{H}^2\big(H,\, \mathrm{Z}(N)\big) \cap \Gamma_{[\mathcal{E}]}$. Then $^{h}[\mathcal{E}] = [\mathcal{E}]$ and the freeness of the action implies that $h = 1$. Thus, $\Gamma_{[\mathcal{E}]}$ is a complement of $\mathrm{H}^2\big(H,\, \mathrm{Z}(N)\big)$ in Γ.

Finally, given $[\mathcal{E}]$ and $[\mathcal{E}']$ in $\mathrm{Ext}_\alpha(H,\, N)$, we have $^{h}[\mathcal{E}] = [\mathcal{E}']$ for some $h \in \mathrm{H}^2\big(H,\, \mathrm{Z}(N)\big)$. Therefore, $h\Gamma_{[\mathcal{E}]}h^{-1} = \Gamma_{[\mathcal{E}']}$, and the proof is complete. □

2.6 Wells Map

Let H and N be two groups. Let $\alpha : H \to \mathrm{Out}(N)$ be a coupling, $[\mathcal{E}]$ an element of $\mathrm{Ext}_\alpha(H,\, N)$ and c an element of C_α such that $^{c}[\mathcal{E}] \in \mathrm{Ext}_\alpha(H, N)$. Since $\mathrm{H}^2\big(H,\, \mathrm{Z}(N)\big)$ acts transitively on $\mathrm{Ext}_\alpha(H,\, N)$, there exists an element $h \in \mathrm{H}^2\big(H,\, \mathrm{Z}(N)\big)$ such that

$$^{h}\big(^{c}[\mathcal{E}]\big) = [\mathcal{E}].$$

Further, the freeness of the action implies that such an h is unique. Thus, we have a map, called *Wells map*,

$$\omega\big([\mathcal{E}]\big) : C_\alpha \to \mathrm{H}^2\big(H,\, \mathrm{Z}(N)\big) \tag{2.39}$$

given by

$$\omega\big([\mathcal{E}]\big)(c) = h.$$

For notational convenience, we write $\omega(\mathcal{E})$ in place of $\omega\big([\mathcal{E}]\big)$.

Wells map was first considered in the literature by Wells [126], and subsequently studied by many authors: Robinson [104, 106, 107], Buckley [14], Malfait [87], Jin [73], Passi–Singh–Yadav [99] and Jin-Liu [74]. For the present formulation of Wells map, we follow the one due to Jin-Liu [74].

It must be noted that the map $\omega(\mathcal{E})$ is not a homomorphism, in general. However, its set-theoretic kernel is the stabilizer in C_α of the class $[\mathcal{E}]$; for,

$$\begin{aligned} \operatorname{Ker}\big(\omega(\mathcal{E})\big) &= \big\{c \in C_\alpha \mid \omega(\mathcal{E})(c) = 1\big\} \\ &= \big\{c \in C_\alpha \mid {}^{c}[\mathcal{E}] = [\mathcal{E}]\big\} \\ &= (\mathrm{C}_\alpha)_{[\mathcal{E}]}. \end{aligned} \tag{2.40}$$

An interesting consequence of Theorem 2.38 is the following result.

Corollary 2.41 *If $\mathcal{E}$ represents an element of* $\operatorname{Ext}_\alpha(H, N)$*, then*

$$\omega(\mathcal{E}) : C_\alpha \to \mathrm{H}^2\big(H, \mathrm{Z}(N)\big)$$

is a derivation with respect to the action of C_α *on* $\mathrm{H}^2\big(H, \mathrm{Z}(N)\big)$.

Furthermore, if $\mathcal{E}'$ represents another element of $\operatorname{Ext}_\alpha(H, N)$*, then $\omega(\mathcal{E})$ and $\omega(\mathcal{E}')$ differ by an inner derivation. More precisely, there exists an element $h \in$* $\mathrm{H}^2\big(H, \mathrm{Z}(N)\big)$ *such that*

$$\omega(\mathcal{E})(c) = \omega(\mathcal{E}')(c)(h^c h^{-1})$$

for all $c \in C_\alpha$.

Proof We begin by observing that the complements of $\mathrm{H}^2\big(H, \mathrm{Z}(N)\big)$ in the semidirect product $\Gamma = C_\alpha \ltimes \mathrm{H}^2\big(H, \mathrm{Z}(N)\big)$ are in one-to-one correspondence with $\operatorname{Der}\big(C_\alpha, \mathrm{H}^2(H, \mathrm{Z}(N))\big)$ ([103, 11.1.2]).

Let $\mathcal{E}$ represent an element of $\operatorname{Ext}_\alpha(H, N)$ and $\lambda \in \operatorname{Der}\big(C_\alpha, \ \mathrm{H}^2(H, \mathrm{Z}(N))\big)$ the derivation corresponding to the complement $\Gamma_{[\mathcal{E}]}$ of $\mathrm{H}^2\big(H, \ \mathrm{Z}(N)\big)$ in Γ (Theorem 2.38). Then, under the above correspondence, we have

$$\Gamma_{[\mathcal{E}]} = \{c\lambda(c) \mid c \in C_\alpha\}.$$

Since $\Gamma_{[\mathcal{E}]}$ is the stabilizer of $[\mathcal{E}]$ in Γ, we have

$${}^{\lambda(c)}\big({}^{c}[\mathcal{E}]\big) = {}^{\lambda(c)c}[\mathcal{E}] = [\mathcal{E}]$$

for all $c \in C_\alpha$. By definition (2.39), we have

$$\omega(\mathcal{E})(c) = \lambda(c)$$

for all $c \in C_\alpha$, and hence $\omega(\mathcal{E}) = \lambda$ is a derivation.

Let $\mathcal{E}'$ represent another element of $\mathrm{Ext}_\alpha(H, N)$. Then, by definition (2.39), we have

$$^{\omega(\mathcal{E})(c)}\big({}^{c}[\mathcal{E}]\big) = [\mathcal{E}] \quad \text{and} \quad {}^{\omega(\mathcal{E}')(c)}\big({}^{c}[\mathcal{E}']\big) = [\mathcal{E}'] \tag{2.42}$$

for all $c \in C_\alpha$. Further, there exists an element $h \in \mathrm{H}^2\big(H, \mathrm{Z}(N)\big)$ such that

$$^{h}[\mathcal{E}] = [\mathcal{E}']. \tag{2.43}$$

Using (2.42) and (2.43), we obtain

$$^{\omega(\mathcal{E}')(c)}\Big({}^{c}\big({}^{h}[\mathcal{E}]\big)\Big) = {}^{h}[\mathcal{E}].$$

We also have ${}^{c}\big({}^{h}[\mathcal{E}]\big) = {}^{{}^{c}h}\big({}^{c}[\mathcal{E}]\big)$. It therefore follows that

$$^{\omega(\mathcal{E}')(c)}\Big({}^{{}^{c}h}\big({}^{c}[\mathcal{E}]\big)\Big) = {}^{h}[\mathcal{E}],$$

and hence

$$^{h^{-1}\omega(\mathcal{E}')(c)}\Big({}^{{}^{c}h}\big({}^{c}[\mathcal{E}]\big)\Big) = {}^{\omega(\mathcal{E})(c)}\big({}^{c}[\mathcal{E}]\big).$$

Since $\mathrm{H}^2\big(H, \ \mathrm{Z}(N)\big)$ is abelian and acts freely on $\mathrm{Ext}_\alpha(H, N)$, we get

$$\omega(\mathcal{E}')(c)({}^{c}hh^{-1}) = h^{-1}\omega(\mathcal{E}')(c)({}^{c}h) = \omega(\mathcal{E})(c)$$

for all $c \in C_\alpha$, and the proof is complete. □

The above corollary shows that, given a coupling $\alpha : H \to \mathrm{Out}(N)$, Wells map defines a unique element, say,

$$[\alpha] \in \mathrm{H}^1\big(C_\alpha, \ \mathrm{H}^2(H, \ \mathrm{Z}(N))\big),$$

which is independent of elements in $\mathrm{Ext}_\alpha(H, N)$.

From the application point of view, it is desirable to write a 2-cocycle representing the image of a compatible pair under the Wells map explicitly.

Proposition 2.44 *Let* $\alpha : H \to \mathrm{Out}(N)$ *be a coupling and*

$$\mathcal{E} : 1 \to N \to G \to H \to 1$$

an extension representing an element in $\mathrm{Ext}_\alpha(H, \ N)$*. Let* $(\chi, \ \mu)$ *be an associated pair for the extension* $\mathcal{E}$*. If* $(\phi, \ \theta) \in C_\alpha$ *is an* α*-compatible pair, then there exists a map* $\lambda : H \to N$ *such that* $\omega(\mathcal{E})(\phi, \ \theta) = [\nu]$*, where*

$$\nu(x,\ y) = \lambda(x)\ {}^{\chi(x)}\lambda(y)\mu(x,\ y)\lambda(xy)^{-1}\theta\big(\mu(\phi^{-1}(x),\ \phi^{-1}(y))\big)^{-1},$$

for all $x,\ y \in H$.

Proof Let $c = (\phi,\ \theta) \in \mathrm{Aut}(H) \times \mathrm{Aut}(N)$. Let $t : H \to G$ be a transversal inducing the associated pair $(\chi,\ \mu)$. Then ${}^{c}\mathcal{E}$ has associated pair $({}^{c}\chi,\ {}^{c}\mu)$ induced by the transversal $t\phi^{-1} : H \to G$. Since $\overline{\chi} = \alpha = \overline{{}^{c}\chi}$, there exists a map $\lambda : H \to N$ such that

$${}^{c}\chi(x) = \iota_{\lambda(x)}\chi(x)$$

for all $x \in H$. Define a transversal $t' : H \to G$ by $t'(x) = \lambda(x)t(x)$ for $x \in H$. We then have an associated pair $(\chi',\ \mu')$, which is equivalent to $(\chi,\ \mu)$. Further,

$$\chi'(x) = \iota_{\lambda(x)}\chi(x) = {}^{c}\chi(x)$$

for all $x \in H$. We set

$$\nu(x,\ y) = \mu'(x,\ y)\ {}^{c}\mu(x, y)^{-1}$$

for $x,\ y \in H$. As in Theorem 2.26, $\nu(x,\ y)$ is a 2-cocycle with

$$[\mathcal{E}] = [\mathcal{E}(\chi,\ \mu)] = [\mathcal{E}(\chi',\ \mu')] = [\mathcal{E}({}^{c}\chi,\ \nu\ {}^{c}\mu)] = {}^{[\nu]}[\mathcal{E}({}^{c}\chi,\ {}^{c}\mu)] = {}^{[\nu]}\big({}^{c}[\mathcal{E}]\big).$$

By the definition of Wells map, we get $\omega(\mathcal{E})(c) = [\nu]$. By (2.36), we have

$${}^{c}\mu(x,\ y) = \theta\big(\mu(\phi^{-1}(x),\ \phi^{-1}(y))\big)$$

for all $x,\ y \in H$. Further, by Proposition 2.19(2), we have

$$\mu'(x, y) = \lambda(x)\ {}^{\chi(x)}\lambda(y)\mu(x,\ y)\lambda(xy)^{-1}$$

for all $x,\ y \in H$. Therefore,

$$\nu(x,\ y) = \lambda(x)\ {}^{\chi(x)}\lambda(y)\mu(x,\ y)\lambda(xy)^{-1}\theta\big(\mu(\phi^{-1}(x),\ \phi^{-1}(y))\big)^{-1},$$

and the proof is complete. □

The preceding result shows that the map $\omega(\mathcal{E})$ defined in (2.39) is precisely the same as the map originally defined by Wells in [126].

2.7 Wells Exact Sequence

Our aim in this section is to present the fundamental exact sequence (Theorem 2.52) due to Wells [126].

Let H and N be two groups. Let $\alpha : H \to \mathrm{Out}(N)$ be a coupling and

$$\mathcal{E} : 1 \to N \to G \to H \to 1$$

an extension representing an element in $\mathrm{Ext}_\alpha(H, N)$. Let

$$\tilde{\alpha} : H \to \mathrm{Aut}\big(\mathrm{Z}(N)\big)$$

be the homomorphism obtained by composing α with the restriction homomorphism $\mathrm{Out}(N) \to \mathrm{Aut}\big(\mathrm{Z}(N)\big)$.

Let $\mathrm{Der}\big(H, \mathrm{Z}(N)\big)$ be the group of derivations from H to $\mathrm{Z}(N)$ with respect to the action $\tilde{\alpha}$. Recall that $\mathrm{Aut}^{N, H}(G)$ consists of the automorphisms of G whose restriction to N and the induced automorphism on H are both identity. With these notations, we have the following result.

Proposition 2.45 $\mathrm{Der}\big(H, \mathrm{Z}(N)\big) \cong \mathrm{Aut}^{N, H}(G)$.

Proof Let $t : H \to G$ be a transversal with $t(1) = 1$ and inducing the given action $\tilde{\alpha} : H \to \mathrm{Aut}\big(\mathrm{Z}(N)\big)$. Define

$$\psi : \mathrm{Der}\big(H, Z(N)\big) \to \mathrm{Aut}^{N, H}(G)$$

by setting $\psi(\lambda) = \gamma_\lambda$ for $\lambda \in \mathrm{Der}\big(H, \mathrm{Z}(N)\big)$, where $\gamma_\lambda : G \to G$ is given by

$$\gamma_\lambda\big(nt(x)\big) = n\lambda(x)t(x)$$

for all $x \in H$ and $n \in N$. It is an easy exercise to check that $\gamma_\lambda \in \mathrm{Aut}^{N, H}(G)$.

Next, we show that ψ is a homomorphism. For $\lambda_1, \lambda_2 \in \mathrm{Der}\big(H, \mathrm{Z}(N)\big)$, and $x \in H, \ n \in N$, we have

$$\begin{aligned} \gamma_{\lambda_1\lambda_2}\big(nt(x)\big) &= n\, \lambda_1\lambda_2(x)t(x) \\ &= n\lambda_1(x)\lambda_2(x)t(x) \\ &= \gamma_{\lambda_1}\big(n\lambda_2(x)t(x)\big) \\ &= \gamma_{\lambda_1}\big(\gamma_{\lambda_2}(nt(x))\big). \end{aligned}$$

Hence, ψ is a homomorphism. Further, $\psi(\lambda) = 1$ implies that $\lambda(x) = 1$ for all $x \in H$, and it follows that ψ is injective.

If $\gamma \in \mathrm{Aut}^{N, H}(G)$, then $\gamma\big(t(x)\big) = \lambda(x)t(x)$ for all $x \in H$ and for some map $\lambda : H \to N$ with $\lambda(1) = 1$. Let $g_1 = n_1t(x_1)$ and $g_2 = n_2t(x_2)$ with $x_1, x_2 \in H$ and $n_1, n_2 \in N$. Then

$$\gamma(g_1g_2) = n_1\, {}^{\chi(x_1)}n_2\mu(x_1, x_2)\lambda(x_1x_2)t(x_1x_2)$$

and

$$\gamma(g_1)\gamma(g_2) = n_1\lambda(x_1)\,{}^{\chi(x_1)}n_2\,{}^{\chi(x_1)}\lambda(x_2)\mu(x_1, x_2)t(x_1x_2).$$

Now, γ being a homomorphism yields

$${}^{\chi(x_1)}n_2\mu(x_1, x_2)\lambda(x_1x_2) = \lambda(x_1)\,{}^{\chi(x_1)}n_2\,{}^{\chi(x_1)}\lambda(x_2)\mu(x_1, x_2). \tag{2.46}$$

Let $x \in H$ and $n \in N$. Then we have

$$\gamma\big(t(x)n\big) = \gamma\big({}^{\chi(x)}nt(x)\big) = {}^{\chi(x)}n\lambda(x)t(x),$$

and

$$\gamma\big(t(x)n\big) = \lambda(x)t(x)n.$$

Therefore,

$$\lambda(x)\,{}^{\chi(x)}n = {}^{\chi(x)}n\lambda(x).$$

It follows that $\lambda(x)n = n\lambda(x)$, and hence $\lambda(H) \leq \mathrm{Z}(N)$. Consequently, by (2.46) it follows that λ is a derivation and $\psi(\lambda) = \gamma$. Hence, ψ is an isomorphism, and the proof is complete. □

Since there is an inclusion $\mathrm{Aut}^{N,H}(G) \hookrightarrow \mathrm{Aut}_N(G)$, Proposition 2.45 gives the following exact sequence

$$1 \to \mathrm{Der}\big(H,\ \mathrm{Z}(N)\big) \longrightarrow \mathrm{Aut}_N(G). \tag{2.47}$$

Let $\mathcal{E} : 1 \to N \to G \xrightarrow{\pi} H \to 1$ be an extension, and $t : H \to G$ a transversal. Consider the inducing homomorphism

$$\rho(\mathcal{E}) : \mathrm{Aut}_N(G) \to \mathrm{Aut}(H) \times \mathrm{Aut}(N),$$

defined, for $\gamma \in \mathrm{Aut}_N(G)$, by

$$\rho(\mathcal{E})(\gamma) = (\overline{\gamma},\ \gamma|_N),$$

where $\overline{\gamma}(x) = \pi\big(\gamma(t(x))\big)$ for all $x \in H$ and $\gamma|_N$ is the restriction of γ to N.

A pair of automorphisms $(\phi,\ \theta) \in \mathrm{Aut}(H) \times \mathrm{Aut}(N)$ is called *inducible* if

$$(\phi,\ \theta) \in \mathrm{Im}\,\big(\rho(\mathcal{E})\big). \tag{2.48}$$

Notice that $\mathrm{Im}\,\big(\rho(\mathcal{E})\big)$ lies in C_α, the group of α-compatible pairs. We thus have the following sequence of groups

$$\mathrm{Aut}_N(G) \xrightarrow{\rho(\mathcal{E})} C_\alpha \xrightarrow{\omega(\mathcal{E})} \mathrm{H}^2\big(H,\ \mathrm{Z}(N)\big). \tag{2.49}$$

The following observation is crucial in the construction of the fundamental exact sequence of Wells.

Proposition 2.50 $\operatorname{Im}\big(\rho(\mathcal{E})\big) = \operatorname{Ker}\big(\omega(\mathcal{E})\big)$.

Proof Let $\gamma \in \operatorname{Aut}_N(G)$ and $\rho(\mathcal{E})(\gamma) = (\phi,\ \theta)$. Then ${}^{(\phi,\,\theta)}[\mathcal{E}] = [\mathcal{E}]$, and we have $\omega(\mathcal{E})(\phi,\ \theta) = 1$. Hence, $(\phi,\ \theta)$ lies in $\operatorname{Ker}\big(\omega(\mathcal{E})\big)$.

Conversely, if $(\phi,\ \theta)$ lies in $\operatorname{Ker}\big(\omega(\mathcal{E})\big)$, then we have

$$[{}^{(\phi,\,\theta)}\mathcal{E}] = {}^{(\phi,\,\theta)}[\mathcal{E}] = [\mathcal{E}].$$

It follows that there exists $\gamma \in \operatorname{Aut}(G)$ such that the following diagram commutes

$$\begin{tikzcd}
{}^{(\phi,\,\theta)}\mathcal{E}: & 1 \arrow[r] & N \arrow[r, "i\theta^{-1}"] \arrow[d, "\mathrm{id}_N"] & G \arrow[r, "\phi\pi"] \arrow[d, "\gamma"] & H \arrow[r] \arrow[d, "\mathrm{id}_H"] & 1 \\
\mathcal{E}: & 1 \arrow[r] & N \arrow[r, "i"] & G \arrow[r, "\pi"] & H \arrow[r] & 1.
\end{tikzcd}$$

Therefore, we have $\rho(\mathcal{E})(\gamma) = (\phi,\ \theta)$, and hence (ϕ, θ) lies in $\operatorname{Im}\big(\rho(\mathcal{E})\big)$. □

Before proceeding further, we provide a module-theoretic reformulation of Proposition 2.50 for abelian extensions. Let $\alpha : H \to \operatorname{Aut}(N)$ be a coupling, where N is abelian. Then N can be regarded as an H-module via α. For each $\phi \in \operatorname{Aut}(H)$, we define a new coupling

$$\alpha' = \alpha\phi^{-1} : H \to \operatorname{Aut}(N).$$

Then N is also an H-module via α', which we denote by N_ϕ for notational convenience. The automorphism ϕ induces an isomorphism of cohomology groups

$$\phi^* : \mathrm{H}^2(H,\ N) \to \mathrm{H}^2(H,\ N_\phi)$$

given by

$$\phi^*\big([\xi]\big) = [\xi_\phi],$$

where

$$\xi_\phi(x,\ y) = \xi\big(\phi^{-1}(x),\ \phi^{-1}(y)\big)$$

for $x,\ y \in H$.

Let $\theta : N \to N_\phi$ be an isomorphism of H-modules. Then it induces an isomorphism

$$\theta^* : \mathrm{H}^2(H,\ N) \to \mathrm{H}^2\left(H,\ N_\phi\right)$$

given by

$$\theta^*\big([\xi]\big) = [\xi_\theta],$$

where

$$\xi_\theta(x, y) = \theta^{-1}\big(\xi(x, y)\big)$$

for $x, y \in H$.

Notice that $\theta : N \to N_\phi$ being an H-module homomorphism means that

$$\theta({}^{\alpha(x)}n) = {}^{\alpha'(x)}\theta(n)$$

for all $x \in H$ and $n \in N$. This is precisely the condition for the pair (ϕ, θ) to be α-compatible (see (2.35)).

We now present a reformulation of Proposition 2.50 for abelian extensions (compare with [116, Chapter II, Proposition 4.3]).

Proposition 2.51 *Let $1 \to N \to G \to H \to 1$ be an abelian extension and μ a corresponding 2-cocycle. Let $(\phi, \theta) \in \mathrm{Aut}(H) \times \mathrm{Aut}(N)$ be a pair of automorphisms. Then (ϕ, θ) is inducible if and only if the following conditions hold:*

(1) $\theta : N \to N_\phi$ is a homomorphism of H-modules;
(2) $\theta^*\big([\mu]\big) = \phi^*\big([\mu]\big)$.

Proof Let $\gamma \in \mathrm{Aut}_N(G)$ be such that $\overline{\gamma} = \phi$ and $\gamma|_N = \theta$. Then the following diagram commutes

$$\begin{tikzcd}
1 \arrow[r] & N \arrow[r] \arrow[d, "\theta"] & G \arrow[r, "\pi"] \arrow[d, "\gamma"] & H \arrow[r] \arrow[d, "\phi"] & 1 \\
1 \arrow[r] & N \arrow[r] & G \arrow[r, "\pi"] & H \arrow[r] & 1.
\end{tikzcd}$$

It follows that $\pi\big(\gamma(t(x))\big) = \phi(x)$ for all $x \in H$. Thus, $\gamma\big(t(x)\big) = \lambda(x)t\big(\phi(x)\big)$ for some element $\lambda(x) \in N$. Since $\lambda(x)$ is unique for a given $x \in H$, it follows that λ is a map from H to N with $\lambda(1) = 1$. Let $g = nt(x)$ for $x \in H$ and $n \in N$. Applying γ, we have

$$\gamma(g) = \theta(n)\gamma\big(t(x)\big) = \theta(n)\lambda(x)t\big(\phi(x)\big).$$

We first prove the condition (1) as follows

$$\begin{aligned}
\theta({}^x n) &= \theta\big(t(x)nt(x)^{-1}\big) \\
&= \gamma\big(t(x)nt(x)^{-1}\big) \\
&= \gamma\big(t(x)\big)\theta(n)\gamma\big(t(x)^{-1}\big) \\
&= \lambda(x)t\big(\phi(x)\big)\theta(n)t\big(\phi(x)\big)^{-1}\lambda(x)^{-1} \\
&= \lambda(x)\, {}^{\phi(x)}\theta(n)\lambda(x)^{-1} \\
&= {}^{\phi(x)}\theta(n).
\end{aligned}$$

Let $g_1 = n_1t(x_1)$ and $g_2 = n_2t(x_2)$. Notice that

$$g_1 g_2 = n_1 \, {}^{x_1}n_2 \mu(x_1, x_2) t(x_1 x_2),$$

and hence

$$\gamma(g_1 g_2) = \theta(n_1)\theta({}^{x_1}n_2)\theta\big(\mu(x_1, x_2)\big)\lambda(x_1 x_2) t\big(\phi(x_1)\phi(x_2)\big).$$

On the other hand, we have

$$\begin{aligned}\gamma(g_1)\gamma(g_2) &= \theta(n_1)\lambda(x_1)t\big(\phi(x_1)\big)\theta(n_2)\lambda(x_2)t\big(\phi(x_2)\big)\\ &= \theta(n_1)\lambda(x_1) \, {}^{\phi(x_1)}\theta(n_2) \, {}^{\phi(x_1)}\lambda(x_2)t\big(\phi(x_1)\big)t\big(\phi(x_2)\big)\\ &= \theta(n_1) \, {}^{\phi(x_1)}\theta(n_2)\lambda(x_1) \, {}^{\phi(x_1)}\lambda(x_2)\mu\big(\phi(x_1), \phi(x_2)\big)t\big(\phi(x_1)\phi(x_2)\big).\end{aligned}$$

Since γ is a homomorphism, we have $\gamma(g_1 g_2) = \gamma(g_1)\gamma(g_2)$, which yields

$$\theta\big(\mu(x_1, x_2)\big)\lambda(x_1 x_2) = \lambda(x_1) \, {}^{\phi(x_1)}\lambda(x_2)\mu\big(\phi(x_1), \phi(x_2)\big).$$

In other words,

$$\mu_\theta(x_1, x_2) = \mu_\phi(x_1, x_2)\lambda(x_1 x_2)^{-1}\lambda(x_1) \, {}^{\phi(x_1)}\lambda(x_2).$$

More precisely, μ_θ and μ_ϕ differ by a coboundary, and hence $\theta^*([\mu]) = \phi^*([\mu])$, which is the condition (2).

For the converse, by condition (2), we have

$$\mu_\theta(x_1, x_2) = \mu_\phi(x_1, x_2)\lambda(x_1 x_2)^{-1}\lambda(x_1) \, {}^{\phi(x_1)}\lambda(x_2)$$

for some map $\lambda : H \to N$ with $\lambda(1) = 1$. For $g = nt(x) \in G$, define

$$\gamma(g) = \theta(n)\lambda(x)t(\phi(x)).$$

That γ is an automorphism of G inducing the pair (ϕ, θ) is left as an exercise for the reader. □

The sequences (2.47) and (2.49) together with Propositions 2.45 and 2.50 give the following fundamental result due to Wells [126].

Theorem 2.52 *Let* $\alpha : H \to \mathrm{Out}(N)$ *be a coupling and*

$$\mathcal{E} : 1 \to N \to G \to H \to 1$$

an extension representing an element in $\mathrm{Ext}_\alpha(H, N)$. *Then there exists the following exact sequence*

$$1 \longrightarrow \mathrm{Der}\big(H, \mathrm{Z}(N)\big) \longrightarrow \mathrm{Aut}_N(G) \xrightarrow{\rho(\mathcal{E})} C_\alpha \xrightarrow{\omega(\mathcal{E})} \mathrm{H}^2\big(H, \mathrm{Z}(N)\big). \tag{2.53}$$

As a consequence of the preceding theorem, we obtain the dimension two case of a well known result of MacLane [85, Proposition 5.6].

Proposition 2.54 *Let* $\alpha : H \to \operatorname{Out}(N)$ *be a coupling. Suppose that* α *is induced by a map* $\chi : H \to \operatorname{Aut}(N)$. *Then for each* $x \in H$*, the action of the pair* $\big(\iota_x,\ \chi(x)\big)$ *on* $\mathrm{H}^2\left(H,\ \mathrm{Z}(N)\right)$ *is trivial.*

Proof Let $x \in H$ and $[\nu] \in \mathrm{H}^2\left(H,\ \mathrm{Z}(N)\right)$. Let $[\mathcal{E}] \in \operatorname{Ext}_\alpha(H,\ N)$ correspond to $[\nu]$ under the bijection given by Theorem 2.26. If

$$\mathcal{E} : 1 \to N \to G \to H \to 1$$

is a representative of $[\mathcal{E}]$, then we can choose a transversal $t : H \to G$ such that

$${}^{\chi(x)}n = t(x)nt(x)^{-1}$$

for each $n \in N$, that is, $\chi(x) = \iota_{t(x)}|_N$. Also $\iota_{t(x)}$ induces ι_x on H. Therefore, the pair $\big(\iota_x,\ \chi(x)\big)$ is induced by $\iota_{t(x)}$. By the exactness of Wells sequence, we have

$$\omega(\mathcal{E})\big(\iota_x, \chi(x)\big) = 1,$$

and the definition of Wells map gives ${}^{(\iota_x,\,\chi(x))}[\mathcal{E}] = [\mathcal{E}]$. Hence, ${}^{(\iota_x,\,\chi(x))}[\nu] = [\nu]$, and the proof is complete. □

Given an extension $1 \to N \to G \to H \to 1$ of groups and a corresponding 2-cocycle μ, set

$$Y = \big\langle \mu(x, y) \mid x, y \in H \big\rangle.$$

For central extensions, we have the following result.

Corollary 2.55 *Let* $1 \to N \to G \to H \to 1$ *be a central extension. Then every automorphism* $\theta \in \operatorname{Aut}^Y(N)$ *can be extended to an automorphism* $\gamma \in \operatorname{Aut}^H(G)$.

Proof Let $\theta \in \operatorname{Aut}^Y(N)$. Since $1 \to N \to G \to H \to 1$ is a central extension, it follows that $(1, \theta)$ is a α-compatible pair, where $\alpha : H \to \operatorname{Aut}(N)$ is the trivial coupling. Further, by Proposition 2.44, we have

$$\omega(\mathcal{E})(1, \theta) = 1.$$

Hence, by Theorem 2.52, $(1,\ \theta)$ is an inducible pair, that is, θ extends to an automorphism $\gamma \in \operatorname{Aut}^H(G)$. □

Setting $\mathcal{I} = \operatorname{Im}\big(\rho(\mathcal{E})\big)$, Wells exact sequence can be modified into the following short exact sequence

$$1 \longrightarrow \operatorname{Der}\big(H, \mathrm{Z}(N)\big) \longrightarrow \operatorname{Aut}_N(G) \xrightarrow{\rho(\mathcal{E})} \mathcal{I} \longrightarrow 1. \tag{2.56}$$

If $1 \to N \to G \to H \to 1$ is a split extension with N central, then the short exact sequence (2.56) splits. For, if N is central, G is a direct product of H and N. Further, in this case,

$$C_\alpha = \mathcal{I} = \operatorname{Aut}(H) \times \operatorname{Aut}(N).$$

Now, for a given pair $(\phi, \theta) \in \operatorname{Aut}(H) \times \operatorname{Aut}(N)$, we can define $f \in \operatorname{Aut}(G)$ by

$$f(hn) = \phi(h)\theta(n)$$

for $g = hn \in G$. Consequently, we obtain a section of the short exact sequence (2.56).

In view of the preceding discussion the following problem seems natural.

Problem 2.57 Find necessary and sufficient conditions on $\mathcal{E}$ under which the short exact sequence (2.56) splits.

It is obvious that the automorphism group of a finite group is finite. Groups which have finite automorphism groups have been the subject of investigation in the literature, see for example [4, 8, 92, 102] and the references therein.

Recall that, for a central extension

$$1 \to N \to G \to H \to 1,$$

we have $\operatorname{Der}\big(H, \mathrm{Z}(N)\big) = \operatorname{Hom}\big(H, \mathrm{Z}(N)\big)$ and $\mathrm{C}_\alpha = \operatorname{Aut}(H) \times \operatorname{Aut}(N)$. Further, by Proposition 2.50 and (2.40), we have

$$\operatorname{Im}\big(\rho(\mathcal{E})\big) = \operatorname{Ker}\big(\omega(\mathcal{E})\big) = (\mathrm{C}_\alpha)_{[\mathcal{E}]}.$$

As an immediate consequence of the short exact sequence (2.56), we obtain the following result of Robinson [102, Theorem 2.4] which gives necessary and sufficient conditions for the automorphism group of a group to be finite.

Theorem 2.58 *Let G be a group, $H = G/\mathrm{Z}(G)$ and $\mathcal{E}$ the central extension*

$$1 \to \mathrm{Z}(G) \to G \to H \to 1.$$

Then $\operatorname{Aut}(G)$ *is finite if and only if* $\operatorname{Hom}\big(H, \mathrm{Z}(G)\big)$ *and* $\big(\operatorname{Aut}(H) \times \operatorname{Aut}\big(\mathrm{Z}(G)\big)\big)_{[\mathcal{E}]}$ *are finite.*

2.8 Extensions with Trivial Coupling

An extension $1 \to N \to G \to H \to 1$ of groups for which the induced coupling $\alpha : H \to \operatorname{Out}(N)$ is trivial is called a *quasi-central extension*. In [14], Buckley gave some characterisations of such extensions, which we now proceed to mention.

We begin by recalling the definition of central product of groups. Let N, S and A be groups such that there are embeddings $A \overset{i}{\hookrightarrow} \mathrm{Z}(N)$ and $A \overset{j}{\hookrightarrow} \mathrm{Z}(S)$. We set

$$A^* = \big\{\big(i(a),\ j(a^{-1})\big) \mid a \in A\big\}.$$

Then the quotient group

$$N \times_A S := (N \times S)/A^*$$

is called the *central product* of groups N and S over the group A. Let $\overline{N}$ and $\overline{S}$ denote images of N and S respectively in $N \times_A S$. Then $N \times_A S = \overline{N}\,\overline{S}$, $[\overline{N},\ \overline{S}] = 1$ and $\overline{N} \cap \overline{S} \cong A$. For example, any extraspecial p-group of order p^5 is a central product of two non-abelian groups N and S of order p^3 with $A = \mathrm{Z}(N) = \mathrm{Z}(S)$.

The following result is due to Buckley [14, Theorem 2.1].

Theorem 2.59 *Let $\mathcal{E} : 1 \to N \to G \to H \to 1$ be an extension with coupling $\alpha : H \to \mathrm{Out}(N)$. Then the following statements are equivalent:*

(1) $\mathcal{E}$ is a quasi-central extension.
(2) $G = N\,\mathrm{C}_G(N)$.
(3) There exists a subgroup S of G such that $G = NS$ and $[N,\ S] = 1$.
(4) G is isomorphic to some central product $N \times_A S$.

Proof If the coupling α is trivial, then it follows that for each $g \in G$, there exists $n \in N$ such that $\iota_g|_N = \iota_n$. Thus, $gag^{-1} = nan^{-1}$ for all $a \in N$. Hence, $g \in N\,\mathrm{C}_G(N)$ for all $g \in G$, and we have $G = N\,\mathrm{C}_G(N)$. Notice, that the steps are reversible, and hence (1) and (2) are equivalent. The equivalence of (2), (3) and (4) readily follows by taking $S = \mathrm{C}_G(N)$. □

For the rest of this section, the coupling $\alpha : H \to \mathrm{Out}(N)$ is assumed to be *trivial*. In this case, $\mathrm{Ext}_\alpha(H,\ N)$ is the set of equivalence classes of quasi-central extensions of H by N. Clearly, this set is non-empty as the class of split extension

$$1 \to N \to N \times H \to H \to 1$$

belongs to $\mathrm{Ext}_\alpha(H,\ N)$. Further, in this case, $\mathrm{Ext}_{\tilde{\alpha}}\big(H,\ \mathrm{Z}(N)\big)$ is the set of equivalence classes of central extensions of H by $\mathrm{Z}(N)$.

By Remark 2.32, there is a bijection between $\mathrm{Ext}_\alpha(H,\ N)$ and $\mathrm{Ext}_{\tilde{\alpha}}\big(H,\ \mathrm{Z}(N)\big)$, but it is not canonical. For trivial coupling, Buckley [14] gave an explicit bijection between $\mathrm{Ext}_\alpha(H,\ N)$ and $\mathrm{Ext}_{\tilde{\alpha}}\big(H,\ \mathrm{Z}(N)\big)$, which is described as follows.

Let $\mathcal{E} : 1 \to N \xrightarrow{i} G \xrightarrow{\pi} H \to 1$ represent an element of $\mathrm{Ext}_\alpha(H,\ N)$. Then, by Theorem 2.59, $G = N\,\mathrm{C}_G(N)$ and $N \cap \mathrm{C}_G(N) = \mathrm{Z}(N)$. Hence,

$$H \cong G/N \cong \mathrm{C}_G(N)/\mathrm{Z}(N)$$

and

$$\mathcal{E}^* : 1 \to \mathrm{Z}(N) \overset{i^*}{\to} \mathrm{C}_G(N) \overset{\pi^*}{\to} H \to 1$$

is a central extension representing an element of $\mathrm{Ext}_{\tilde{\alpha}}\big(H, \mathrm{Z}(N)\big)$. Further, we have the following commutative diagram

$$\begin{tikzcd}
\mathcal{E}^* : & 1 \arrow[r] & \mathrm{Z}(N) \arrow[r, "i^*"] \arrow[d] & \mathrm{C}_G(N) \arrow[r, "\pi^*"] \arrow[d] & H \arrow[r] \arrow[d, "\mathrm{id}_H"] & 1 \\
\mathcal{E} : & 1 \arrow[r] & N \arrow[r, "i"] & G \arrow[r, "\pi"] & H \arrow[r] & 1.
\end{tikzcd}$$

Now, let $\mathcal{E} : 1 \to \mathrm{Z}(N) \overset{i}{\to} S \overset{\pi}{\to} H \to 1$ represent an element of $\mathrm{Ext}_{\tilde{\alpha}}\big(H, \mathrm{Z}(N)\big)$. Then

$$\mathcal{E}^\circ : 1 \to N \overset{i^\circ}{\to} N \times_{\mathrm{Z}(N)} S \overset{\pi^\circ}{\to} H \to 1$$

is a quasi-central extension of N by H. Here $i^\circ(n) = \overline{(n, 1)}$ and $\pi^\circ\big(\overline{(n, s)}\big) = \pi(s)$ for all $n \in N$ and $s \in S$. As before, we have the following commutative diagram

$$\begin{tikzcd}
\mathcal{E} : & 1 \arrow[r] & \mathrm{Z}(N) \arrow[r, "i"] \arrow[d] & S \arrow[r, "\pi"] \arrow[d] & H \arrow[r] \arrow[d, "\mathrm{id}_H"] & 1 \\
\mathcal{E}^\circ : & 1 \arrow[r] & N \arrow[r, "i^\circ"] & N \times_{\mathrm{Z}(N)} S \arrow[r, "\pi^\circ"] & H \arrow[r] & 1.
\end{tikzcd}$$

With this set-up, we have the following result of Buckley [14, Theorem 2.2].

Theorem 2.60 *Let $\alpha : H \to \mathrm{Out}(N)$ be the trivial coupling. Then the map $\phi : \mathrm{Ext}_\alpha(H, N) \to \mathrm{Ext}_{\tilde{\alpha}}\big(H, \mathrm{Z}(N)\big)$ given by $\phi\big([\mathcal{E}]\big) = [\mathcal{E}^*]$ is a bijection with the map $\psi : \mathrm{Ext}_{\tilde{\alpha}}\big(H, \mathrm{Z}(N)\big) \to \mathrm{Ext}_\alpha(H, N)$ given by $\psi\big([\mathcal{E}]\big) = [\mathcal{E}^\circ]$ as its inverse.*

Proof We see that both ϕ and ψ are well-defined. It only remains to show that ϕ and ψ are inverses of each other. If

$$\mathcal{E} : 1 \to N \to G \to H \to 1$$

represents an element of $\mathrm{Ext}_\alpha(H, N)$, then $(\mathcal{E}^*)^\circ$ is equivalent to $\mathcal{E}$ by Theorem 2.59, and hence $\psi\phi$ is identity.

Conversely, if

$$\mathcal{E} : 1 \to \mathrm{Z}(N) \to S \to H \to 1$$

represents an element of $\mathrm{Ext}_{\tilde{\alpha}}\big(H, \mathrm{Z}(N)\big)$, then we have

$$(\mathcal{E}^\circ)^* : 1 \to \mathrm{Z}(N) \to \mathrm{C}_G(\overline{N}) \to H \to 1,$$

where $G = N \times_{Z(N)} S$ and $\overline{N}$ is the image of N in G. It is evident that $C_G(\overline{N}) = \overline{S}$, the image of S in G. Hence, $(\mathcal{E}^\circ)^*$ is equivalent to $\mathcal{E}$, and $\phi\psi$ is identity too. □

An extension $1 \to N \to G \to H \to 1$ is called a *commutator extension* of H by N if

$$N \cap \gamma_2(G) = 1.$$

Clearly, every commutator extension is a central extension. For example, the central extension

$$1 \to \mathrm{Z}\big(\mathrm{GL}(n,k)\big) \to \mathrm{GL}(n,k) \to \mathrm{PGL}(n,k) \to 1,$$

where k is a finite field with p^m elements such that n does not divide $p^m - 1$, is a commutator extension. We set

$$\mathcal{C}\big(H,\ \mathrm{Z}(N)\big) = \big\{[\mathcal{E}] \in \mathrm{Ext}_{\tilde{\alpha}}(H,\ \mathrm{Z}(N)) \mid \mathcal{E} \text{ is a commutator extension}\big\}.$$

Since $\mathrm{Z}(N)$ is a trivial H-module via $\tilde{\alpha}$, we have the following exact sequence by Universal Coefficient Theorem [116, p. 25]

$$1 \to \mathrm{Ext}\left(H/\gamma_2(H),\ \mathrm{Z}(N)\right) \to \mathrm{H}^2\left(H,\ \mathrm{Z}(N)\right) \xrightarrow{\pi} \mathrm{Hom}\left(\mathrm{H}_2(H,\ \mathbb{Z}),\ \mathrm{Z}(N)\right) \to 1.$$

By Theorem 2.24, there is a bijection

$$\mathrm{Ext}_{\tilde{\alpha}}(H,\ \mathrm{Z}(N)) \longleftrightarrow \mathrm{H}^2\left(H,\ \mathrm{Z}(N)\right),$$

under which the set $\mathcal{C}\big(H,\ \mathrm{Z}(N)\big)$ corresponds to $\mathrm{Ker}(\pi)$, which is further isomorphic to $\mathrm{Ext}\left(H/\gamma_2(H),\ \mathrm{Z}(N)\right)$ (see [116, Proposition V.3.2]).

By Theorem 2.60, we have a bijection

$$\mathrm{Ext}_{\tilde{\alpha}}\left(H,\ \mathrm{Z}(N)\right) \xrightarrow{\psi} \mathrm{Ext}_{\alpha}(H,\ N).$$

An extension representing an element in the image of $\mathcal{C}\big(H,\ \mathrm{Z}(N)\big)$ under the map ψ is called a *special quasi-central extension*. Set

$$\mathcal{S}(H,\ N) = \big\{[\mathcal{E}] \in \mathrm{Ext}_{\alpha}(H,\ N) \mid \mathcal{E} \text{ is a special quasi-central extension}\big\}.$$

The following result, whose proof is analogous to that of Theorem 2.59, characterises special quasi-central extensions.

Theorem 2.61 *Let $\mathcal{E} : 1 \to N \to G \to H \to 1$ be an extension with trivial coupling $\alpha : H \to \mathrm{Out}(N)$. Then the following statements are equivalent:*

(1) $\mathcal{E}$ is a special quasi-central extension.
(2) $N \cap \gamma_2\big(\mathrm{C}_G(N)\big) = 1$.
(3) There exists a subgroup S of G such that $G = NS$, $[N,\ S] = 1$ and $N \cap \gamma_2(S) = 1$.

(4) There exists an abelian group A and embeddings $A \hookrightarrow \mathrm{Z}(N)$ and $A \hookrightarrow \mathrm{Z}(S)$ such that $G \cong N \times_A S$. Further,

$$1 \to A \to S \to S/A \to 1$$

is a commutator extension.

Remark 2.62 In view of the preceding discussion, we have the following commutative diagram

$$\begin{tikzcd}
\mathrm{Ext}_\alpha(H,N) \arrow[r, leftrightarrow] & \mathrm{Ext}_{\tilde{\alpha}}\big(H,\mathrm{Z}(N)\big) \arrow[r, leftrightarrow] & \mathrm{H}^2\big(H,\ \mathrm{Z}(N)\big) \\
\mathcal{S}(H,N) \arrow[u, hook] \arrow[r, leftrightarrow] & \mathcal{C}\big(H,\mathrm{Z}(N)\big) \arrow[u, hook] \arrow[r, leftrightarrow] & \mathrm{Ext}\big(H/\gamma_2(H),\mathrm{Z}(N)\big). \arrow[u, hook]
\end{tikzcd}$$

If the coupling $\alpha : H \to \mathrm{Out}(N)$ is trivial, then $C_\alpha = \mathrm{Aut}(H) \times \mathrm{Aut}(N)$, and $\mathrm{Der}\big(H,\ \mathrm{Z}(N)\big) = \mathrm{Hom}\big(H,\ \mathrm{Z}(N)\big)$. Thus, the sequence (2.56) takes the following simpler form, which is used in Sect. 4.1 of Chap. 4.

Theorem 2.63 *Let $\mathcal{E} : 1 \to N \to G \to H \to 1$ be an extension representing an element in $\mathrm{Ext}_\alpha(H,\ N)$, where α is the trivial coupling. Then there is an exact sequence*

$$1 \to \mathrm{Hom}\big(H,\ \mathrm{Z}(N)\big) \longrightarrow \mathrm{Aut}_N(G) \xrightarrow{\rho(\mathcal{E})} \mathrm{Aut}(H) \times \mathrm{Aut}(N).$$

Further, $\mathrm{Im}\big(\rho(\mathcal{E})\big)$ *is the stabilizer of* $[\mathcal{E}]$ *under the action of* $\mathrm{Aut}(H) \times \mathrm{Aut}(N)$ *on* $\mathrm{Ext}_\alpha(H,\ N)$.

2.9 Extension and Lifting of Automorphisms

In this section, as an application of Wells exact sequence developed in the preceding sections, we discuss the following fundamental problem in the extension theory of groups.

Problem 2.64 Let $1 \to N \to G \to H \to 1$ be a short exact sequence of groups and $(\phi,\ \theta) \in \mathrm{Aut}(H) \times \mathrm{Aut}(N)$ a pair of automorphisms. Under what conditions is the pair $(\phi,\ \theta)$ induced by an automorphism $\gamma \in \mathrm{Aut}_N(G)$?

The most recent result in this direction, using Wells exact sequence, which we are going to present here, is due to Robinson [106, 107].

For a finite group G, let $\pi(G)$ denote the set of primes dividing the order of G. Let

$$\mathcal{E} : 1 \to N \to G \to H \to 1$$

be an extension of groups with H finite and inducing the coupling $\alpha : H \to \mathrm{Out}(N)$. Let $\pi(H) = \{p_1, p_2, \ldots, p_k\}$ and $P_i = R_i/N$ be a Sylow p_i-subgroup of H for each $1 \leq i \leq k$. Let α_i be the coupling induced by the extension

$$\mathcal{E}_i : 1 \to N \to R_i \to P_i \to 1$$

for each $1 \leq i \leq k$, and $(\phi, \theta) \in \mathrm{Aut}(H) \times \mathrm{Aut}(N)$.

Lemma 2.65 *With the preceding set-up, the following statements hold:*

(1) $\phi(P_i) = \overline{g}_i P_i (\overline{g}_i)^{-1}$ *for some* $g_i \in G$*, where* $\overline{g}_i = Ng_i$*;*
(2) (ϕ, θ) *is* α*-compatible if and only if* $(\iota_{\overline{g}_i}\phi|_{P_i}, \iota_{g_i}\theta)$ *is* α_i*-compatible for each* $1 \leq i \leq k$*.*

Proof Since $P_i = R_i/N$ is a Sylow p_i-subgroup of H for each $1 \leq i \leq k$ and $\phi \in \mathrm{Aut}(H)$, there exist elements $\overline{g}_i = Ng_i \in G/N$ such that $\phi(P_i) = \overline{g}_i P_i (\overline{g}_i)^{-1}$, proving (1).

Observe that $\alpha_i = \alpha|_{P_i}$. Set $\phi_i = \iota_{\overline{g}_i}\phi|_{P_i}$ and $\theta_i = \iota_{g_i}\theta$. Then notice that $\phi_i \in \mathrm{Aut}(P_i)$ and $\theta_i \in \mathrm{Aut}(N)$. For $\theta \in \mathrm{Aut}(N)$, set $\overline{\theta} = \mathrm{Inn}(N)\theta$. Assume that (ϕ_i, θ_i) is α_i-compatible, that is,

$$\overline{\theta}_i \alpha_i(x)(\overline{\theta}_i)^{-1} = \alpha_i\big(\phi_i(x)\big)$$

for all $x \in P_i$. Notice that we have $\alpha(\overline{g}_i) = \overline{\iota}_{g_i}$, where $\overline{\iota}_{g_i} = \mathrm{Inn}(N)\iota_{g_i}$. Then, for all $x \in P_i$, we have

$$\begin{aligned} \alpha(\overline{g}_i)\overline{\theta}\alpha(x)\overline{\theta}^{-1}\alpha(\overline{g}_i)^{-1} &= \alpha(\overline{g}_i)\overline{\iota}_{g_i}^{-1}\overline{\theta}_i\alpha_i(x)\overline{\theta}_i^{-1}\overline{\iota}_{g_i}\alpha(\overline{g}_i)^{-1} \\ &= \overline{\theta}_i\alpha_i(x)\overline{\theta}_i^{-1} \\ &= \alpha_i\big(\phi_i(x)\big) \\ &= \alpha\big(\overline{g}_i\phi(x)\overline{g}_i^{-1}\big) \\ &= \alpha(\overline{g}_i)\alpha(\phi(x))\alpha(\overline{g}_i)^{-1}. \end{aligned} \tag{2.66}$$

Therefore,

$$\overline{\theta}\alpha(x)\overline{\theta}^{-1} = \alpha\big(\phi(x)\big)$$

for all $x \in P_i$. Further, notice that $H = \langle P_1, P_2, \ldots, P_k\rangle$. Thus, for each $x \in H$, we have $x = \prod_{j=1}^{l} x_j$ for some $x_j \in P_{i_j}$. Therefore,

$$\overline{\theta}\alpha(x)\overline{\theta}^{-1} = \prod_{j=1}^{l}\overline{\theta}\alpha(x_j)\overline{\theta}^{-1} = \prod_{j=1}^{l}\alpha\big(\phi(x_j)\big) = \alpha\big(\phi(x)\big),$$

and hence (ϕ, θ) is α-compatible. The converse follows by reversing the above arguments. □

We now present the following main result of Robinson [106, Theorem 2].

Theorem 2.67 *Let $\mathcal{E} : 1 \to N \to G \to H \to 1$ be an extension of groups with H finite and inducing the coupling α. Let $\pi(H) = \{p_1, p_2, \ldots, p_k\}$ and $P_i = R_i/N$ be a Sylow p_i-subgroup of H for each $1 \le i \le k$. Let α_i be the coupling induced by the extension*

$$\mathcal{E}_i : 1 \to N \to R_i \to P_i \to 1$$

for each $1 \le i \le k$ and $(\phi, \theta) \in \mathrm{Aut}(H) \times \mathrm{Aut}(N)$. Then (ϕ, θ) is inducible in $\mathcal{E}$ if and only if $(\iota_{\overline{g}_i}\phi|_{P_i}, \iota_{g_i}\theta)$ is inducible in $\mathcal{E}_i$ for each $1 \le i \le k$.

Proof Set $\phi_i = \iota_{\overline{g}_i}\phi|_{P_i}$ and $\theta_i = \iota_{g_i}\theta$. Assume that (ϕ_i, θ_i) is inducible in $\mathcal{E}_i$ for all $1 \le i \le k$. Then the pair (ϕ_i, θ_i) is α_i-compatible for all $1 \le i \le k$ and by the preceding lemma (ϕ, θ) is α-compatible. In view of Wells exact sequence (2.53), it remains to show that $\omega(\mathcal{E})(\phi, \theta) = 1$.

Restricting to the subgroup of $\mathrm{Aut}(G)$ consisting of those automorphisms of G which normalize R_i and N, denoted by $\mathrm{Aut}_{N,R_i}(G)$, we obtain from Wells exact sequence arising from $\mathcal{E}$, the following exact sequence

$$1 \to \mathrm{Der}_{\overline{\alpha}}\big(H, \mathrm{Z}(N)\big) \longrightarrow \mathrm{Aut}_{N,R_i}(G) \xrightarrow{\rho(\mathcal{E})} \mathrm{C}_i \xrightarrow{\omega(\mathcal{E})} \mathrm{H}^2\big(H, \mathrm{Z}(N)\big),$$

where

$$\mathrm{C}_i = \big\{(\phi, \theta) \in \mathrm{C}_\alpha \mid \phi(P_i) = P_i\big\}.$$

Notice that $(\iota_{\overline{g}_i}, \iota_{g_i})$ is inducible in $\mathcal{E}$ for all $1 \le i \le k$, and hence is α-compatible. Since (ϕ, θ) is also α-compatible and $\iota_{\overline{g}_i}\phi(P_i) = P_i$, we have $(\iota_{\overline{g}_i}\phi, \iota_{g_i}\theta) \in \mathrm{C}_i$. Let

$$res^H_{P_i} : \mathrm{H}^2\big(H, \mathrm{Z}(N)\big) \to \mathrm{H}^2\big(P_i, \mathrm{Z}(N)\big)$$

be the restriction map in cohomology, and

$$r^H_{P_i} : \mathrm{C}_i \to \mathrm{C}_{\alpha_i}$$

be the map $(\phi, \theta) \mapsto (\phi|_{P_i}, \theta)$. Then we have the following commutative diagram

$$\begin{tikzcd}
\mathrm{C}_i \arrow[r, "\omega(\mathcal{E})"] \arrow[d, "r^H_{P_i}"'] & \mathrm{H}^2\big(H, \mathrm{Z}(N)\big) \arrow[d, "res^H_{P_i}"] \\
\mathrm{C}_{\alpha_i} \arrow[r, "\omega(\mathcal{E}_i)"] & \mathrm{H}^2\big(P_i, \mathrm{Z}(N)\big).
\end{tikzcd}$$

Now $r^H_{P_i}(\iota_{\overline{g}_i}\phi, \iota_{g_i}\theta) = (\phi_i, \theta_i) \in \mathrm{C}_{\alpha_i}$. Since (ϕ_i, θ_i) is inducible in $\mathcal{E}_i$, we have

$$\omega(\mathcal{E}_i)\big(r^H_{P_i}(\iota_{\overline{g}_i}\phi, \iota_{g_i}\theta)\big) = \omega(\mathcal{E}_i)(\phi_i, \theta_i) = 1.$$

Therefore, by commutativity of the preceding square, we have

$$res^H_{P_i}\big(\omega(\mathcal{E})(\iota_{\overline{g}_i}\phi,\ \iota_{g_i}\theta)\big) = 1.$$

By Proposition 2.54, $(\iota_{\overline{g}_i},\ \iota_{g_i})$ acts trivially on $\mathrm{H}^2\left(H,\ \mathrm{Z}(N)\right)$, and hence

$$^{(\iota_{\overline{g}_i}, \iota_{g_i})}\omega(\mathcal{E})(\phi, \theta) = \omega(\mathcal{E})(\phi, \theta).$$

By Corollary 2.41, the map $\omega(\mathcal{E})$ is a derivation, and hence

$$\begin{aligned}\omega(\mathcal{E})(\iota_{\overline{g}_i}\phi, \iota_{g_i}\theta) &= \omega(\mathcal{E})(\iota_{\overline{g}_i},\ \iota_{g_i})\ ^{(\iota_{\overline{g}_i}, \iota_{g_i})}\omega(\mathcal{E})(\phi,\ \theta)\\ &= {}^{(\iota_{\overline{g}_i}, \iota_{g_i})}\omega(\mathcal{E})(\phi,\ \theta),\ \text{ since } (\iota_{\overline{g}_i},\ \iota_{g_i}) \text{ is inducible}\\ &= \omega(\mathcal{E})(\phi, \theta).\end{aligned}$$

It follows that $res^H_{P_i}\big(\omega(\mathcal{E})(\phi, \theta)\big) = 1$. Applying the corestriction map

$$cores^H_{P_i} : \mathrm{H}^2\left(P_i,\ \mathrm{Z}(N)\right) \to \mathrm{H}^2\left(H,\ \mathrm{Z}(N)\right),$$

and using Theorem 2.8, we get

$$\omega(\mathcal{E})(\phi,\ \theta)^{|H:P_i|} = 1$$

for each $1 \leq i \leq k$. Since $p_1,\ p_2,\ \ldots,\ p_k$ are distinct primes, we get $\omega(\mathcal{E})(\phi,\ \theta) = 1$, and hence (ϕ, θ) is inducible in $\mathcal{E}$.

Conversely, suppose that the pair $(\phi,\ \theta)$ is induced by $\gamma \in \mathrm{Aut}_N(G)$. By Lemma 2.65(1), we have $\iota_{\overline{g}_i}\phi(P_i) = P_i$ for some $g_i \in G$ and for each $1 \leq i \leq k$. It follows that $\iota_{g_i}\gamma(R_i) = R_i$. Thus, $\iota_{g_i}\gamma \in \mathrm{Aut}_N(R_i)$ and induces $(\phi_i,\ \theta_i)$ in $\mathcal{E}_i$ for each $1 \leq i \leq k$. This completes the proof of the theorem. □

The special cases of Theorem 2.67 for finite groups where one of the automorphisms in the pair $(\phi,\ \theta)$ is identity have been dealt with in [73, Theorem D] and [99, Theorem 7, Theorem 4].

Corollary 2.68 *Let* $\mathcal{E} : 1 \to N \to G \to H \to 1$ *be an extension of groups with* H *finite. Then the pair* $(1,\ \theta) \in \mathrm{Aut}(H) \times \mathrm{Aut}(N)$ *is inducible in* $\mathcal{E}$ *if and only if the pair* $(1,\ \theta) \in \mathrm{Aut}(P_i) \times \mathrm{Aut}(N)$ *is inducible in* $\mathcal{E}_i$ *for each* $1 \leq i \leq k$.

Corollary 2.69 *Let* $\mathcal{E} : 1 \to N \to G \to H \to 1$ *be an extension of groups with* H *finite. Let* $\phi \in \mathrm{Aut}(H)$ *such that* $\phi|_{P_i} \in \mathrm{Aut}(P_i)$. *Then* $(\phi,\ 1)$ *is inducible in* $\mathcal{E}$ *if and only if* $(\phi|_{P_i},\ 1)$ *is inducible in* $\mathcal{E}_i$ *for each* $1 \leq i \leq k$.

Remark 2.70 A number of conditional generalizations of Theorem 2.67 (for example, when H is a countable, locally finite or an FC-group) have been given by Robinson [106, 107].

Remark 2.71 We have seen that the cohomology of groups plays a crucial role in the study of automorphisms of finite groups. It is worth mentioning that, in the reverse direction, automorphism groups too play an important role in the study of cohomology of groups. We just mention some notable results in this direction; a detailed study is beyond the focus of this monograph.

Notice that an automorphism of a group G induces an automorphism of its cohomology ring $\mathrm{H}^*(G,\ R)$, where R is a commutative ring, thus inducing a homomorphism

$$\mathrm{Aut}(G) \to \mathrm{Aut}\left(\mathrm{H}^*(G,\ R)\right)$$

whose kernel we denote by $\mathrm{Aut}^*(G,\ R)$. It is known that $\mathrm{Inn}(G) \leq \mathrm{Aut}^*(G,\ R)$, and understanding $\mathrm{Aut}^*(G,\ R)$ has been a subject of investigation in many works. In [71], besides other results, Jackowski and Marciniak proved that for a finite solvable group G the order of $\mathrm{Aut}^*(G, \mathbb{Z})$ is divisible only by primes dividing the order of G. In [72], Jespers and Zimmermann proved that any conjugacy class preserving automorphism of a finite p-group G which is a semi-direct product of a cyclic p-group by an abelian p-group and induces the identity on $\mathrm{H}^*(G,\ \mathbb{F}_p)$ is in fact inner.

The mod-p cohomology $\mathrm{H}^*(G,\ \mathbb{F}_p)$ of a finite p-group G is a finitely generated graded commutative algebra with Krull dimension $\dim\left(\mathrm{H}^*(G,\ \mathbb{F}_p)\right) = \mathrm{rk}(G)$, where $\mathrm{rk}(G)$ is the maximum rank of an elementary abelian p-subgroup of G. Since $\mathrm{Inn}(G)$ acts trivially on cohomology, there is an action of the outer automorphism group $\mathrm{Out}(G)$ on $\mathrm{H}^*(G,\ \mathbb{F}_p)$ turning it into an $\mathbb{F}_p[\mathrm{Out}(G)]$-module. It was proved in [48, 120] that every simple $\mathbb{F}_p[\mathrm{Out}(G)]$-module appears as a composition factor in $\mathrm{H}^*(G,\ \mathbb{F}_p)$. If e_M is the idempotent associated to a simple $\mathbb{F}_p[\mathrm{Out}(G)]$-module M, then $\dim\left(e_M\,\mathrm{H}^*(G,\ \mathbb{F}_p)\right) \geq 1$. In [88], Martino and Priddy conjectured that $\dim\left(e_M\,\mathrm{H}^*(G,\ \mathbb{F}_p)\right) = \mathrm{rk}(G)$ for every finite p-group G and simple $\mathbb{F}_p[\mathrm{Out}(G)]$-module M. The conjecture was proved by Kuhn [78] for all p-groups with $p > 2$ and for some 2-groups. For discrete groups G of finite cohomological dimension, Adem [2] gave a method for constructing non-trivial cohomology classes in $\mathrm{H}^*(G,\ \mathbb{F}_p)$ by using finite p-subgroups of $\mathrm{Aut}(G)$.

Chapter 3
Orders of Automorphism Groups of Finite Groups

The object of study in this chapter is the relation between the order of a finite group and that of its group of automorphisms. In 1954, Scott [114] conjectured that a finite group has at least a prescribed number of automorphisms if the order of the group is sufficiently large. The conjecture was confirmed by Ledermann and Neumann [80, Theorem 6.6] in 1956 by constructing an explicit function $f : \mathbb{N} \to \mathbb{N}$ with the property that if the finite group G has order $|G| \geq f(n)$, then $|\operatorname{Aut}(G)| \geq n$. In the same year, building on their techniques from [80], the authors [81] proved the following local version of Scott's conjecture:

Conjecture 3.1 *There exists a function $f : \mathbb{N} \to \mathbb{N}$ such that, for each $h \in \mathbb{N}$ and each prime p, if G is any finite group such that $p^{f(h)}$ divides $|G|$, then p^h divides $|\operatorname{Aut}(G)|$.*

Later on, Green [49], Howarth [63] and Hyde [68] successively improved the function f to a quadratic polynomial function. The aim of this chapter is to give an exposition of these developments. Schur multiplier plays a significant role in these investigations.

3.1 Schur Multiplier

In his investigation of projective representations of a finite group G, Schur [112, 113] came up with an abelian group $\mathcal{M}(G)$, now known as the *Schur multiplier* of G. This group is a basic object of study in the theory of groups and can be viewed as having led to the development of (co)homology theory of groups. Apart from representation theory of groups, it occurs in (i) the cohomology of groups as the second cohomology group $\mathrm{H}^2(G, \mathbb{C}^\times)$ of G with coefficients in the multiplicative group $\mathbb{C}^\times$ of non-zero complex numbers with the trivial G-action, (ii) the homology of groups as $\mathrm{H}_2(G, \mathbb{Z})$, the second homology group of the group G with coefficients in the additive group $\mathbb{Z}$ of integers with the trivial G-action, (iii) combinatorial group theory as $(R \cap [F, F])/[R, F]$ for a free presentation

$$1 \to R \to F \to G \to 1$$

I. B. S. Passi et al., *Automorphisms of Finite Groups*, Springer Monographs
in Mathematics, https://doi.org/10.1007/978-981-13-2895-4_3

of the group G. Schur multiplier plays a major role in the investigation of automorphism groups of finite groups.

In this section, we present the basic definitions and some of the properties of Schur multiplier, and list a few of the best known results on its order and exponent. For detailed discussion of this topic the reader is referred to [10, 66, 76].

Let G be a group. Recall that, a *free presentation* of G is a surjective homomorphism $\psi : F \to G$, where F is a free group. Let $R = \operatorname{Ker}(\psi)$, so that

$$G \cong F/R.$$

Then $[R,\ F]$ is contained in R and is a normal subgroup of F. For each subgroup $S \leq F$, let $\overline{S}$ denote the quotient of S modulo $[R,\ F]$:

$$\overline{S} = S[R,\ F]/[R,\ F].$$

Let $\overline{\psi} : \overline{F} \to G$ be the homomorphism induced by ψ, that is, $\overline{\psi}(\overline{x}) = \psi(x)$ for all $\overline{x} \in \overline{F}$, where $\overline{x} = [R,\ F]x$ for $x \in F$. Then $\operatorname{Ker}(\overline{\psi}) = \overline{R}$, and we have the following central extension

$$1 \to \overline{R} \longrightarrow \overline{F} \xrightarrow{\overline{\psi}} G \to 1. \tag{3.2}$$

It is well-known that the abelian group $\overline{\gamma_2(F)} \cap \overline{R}$, depends only on the group G and not on the central extension (3.2) (see [59, p. 204]). The abelian group

$$\mathcal{M}(G) := \overline{\gamma_2(F)} \cap \overline{R}$$

is called the *Schur multiplier* of the group G. In the language of homology,

$$\mathcal{M}(G) \cong \mathrm{H}_2(G,\ \mathbb{Z}), \tag{3.3}$$

the second homology group of G with coefficients in the trivial G-module $\mathbb{Z}$ (see [59, p. 204]). The isomorphism (3.3) is known as *Hopf's formula*; it was originally proved by Hopf [62] for finitely presented groups.

In general, the character group $\mathrm{H}_2\widehat{(G,\ \mathbb{Z})}$ is isomorphic to $\mathrm{H}^2(G,\ \mathbb{C}^\times)$, the second cohomology group of G with coefficients in $\mathbb{C}^\times$, the multiplicative group of non-zero complex numbers with the trivial G-action. However, when G is finite, there is an isomorphism

$$\mathrm{H}_2\widehat{(G,\ \mathbb{Z})} \cong \mathrm{H}_2(G,\ \mathbb{Z}),$$

and hence

$$\mathcal{M}(G) \cong \mathrm{H}^2(G,\ \mathbb{C}^\times). \tag{3.4}$$

Describing the structure of the Schur multiplier of a finite group is, in general, a difficult problem. However, a lot of work has been done by several authors on its order and exponent. For finite abelian groups, we have the following result [76, p. 37].

Theorem 3.5 *If G is a finite abelian group with cyclic decomposition $G = \bigoplus_{i=1}^{r} \mathrm{C}_{m_i}$, then*

$$\mathcal{M}(G) \cong \begin{cases} \bigoplus_{1 \le i < j \le r} \mathrm{C}_{e_{ij}} & \text{if } r \ge 2, \\ 0 & \text{if } r = 1, \end{cases} \tag{3.6}$$

where $e_{ij} = (m_i, m_j)$.

For a natural number n and prime p, let n_p denote the highest power of p that divides n. The following results were proved by Schur himself in his fundamental paper [112] (see also [76, Chapter 2]).

Theorem 3.7 *Let G be a finite group. Then the following statements hold:*

(1) $\mathcal{M}(G)$ is finite. Moreover, the elements of $\mathcal{M}(G)$ have orders dividing $|G|$.

(2) If $1 \to R \to F \to G \to 1$ is a free presentation of G, then

$$\overline{R} = \mathcal{M}(G) \oplus \overline{X},$$

with $\overline{X}$ a free abelian group.

(3) If N is a central subgroup of G and $H = G/N$, then $\gamma_2(G) \cap N$ is isomorphic to a subgroup of $\mathcal{M}(H)$.

(4) If S is a Sylow p-subgroup of G, then

$$|\mathcal{M}(G)|_p \le |\mathcal{M}(S)|_p.$$

As a consequence of Theorem 3.7, we have, in particular, the following result about the exponent of the center of a finite group.

Corollary 3.8 *If G is a finite group, then*

$$\exp\big(\mathrm{Z}(G)\big) \text{ divides } \exp\big(G/\gamma_2(G)\big)|G/\mathrm{Z}(G)|.$$

In [112], Schur showed that $|\mathcal{M}(G)| \le m^{m^2}$, where $m = |G|$. The bound was later substantially improved by Ledermann and Neumann [81, Lemma 3.6] as presented in the following result.

Theorem 3.9 *If G is a finite group, then*

$$|\mathcal{M}(G)| \le m^{(m-1)d},$$

where $d = d(G)$ is the minimum number of generators of G and $m = |G|$.

The order of Schur multiplier of a finite p-group has been intensively investigated. We mention some of the results in this direction for the curious reader.

The following result is by Jones [75, Corollary 2.3], which is a refinement of an earlier bound by Green [49, Lemma 6.2].

Theorem 3.10 *If G is a p-group of order p^n, then*

$$|\gamma_2(G)|\,|\mathcal{M}(G)| \le p^{\frac{n(n-1)}{2}}.$$

An analogue of Theorem 1.9 is as follows.

Theorem 3.11 *Let p be a prime and G a group such that $|G/\operatorname{Z}(G)|_p = p^r$. Then $|\gamma_2(G)|_p \le p^{\frac{r(r-1)}{2}}$.*

Proof Since

$$|\gamma_2(G)/\big(\operatorname{Z}(G)\cap\gamma_2(G)\big)|_p = |\gamma_2(G)\operatorname{Z}(G)/\operatorname{Z}(G)|_p \le |G/\operatorname{Z}(G)|_p = p^r,$$

the result follows by Theorem 3.7(3)-(4) and Theorem 3.10. □

The following result is due to Ellis and Wiegold [28, Theorem 2].

Theorem 3.12 *Let G be a group of order p^n. Suppose that $G/\gamma_2(G)$ has order p^m and exponent p^e. Then*

$$|\mathcal{M}(G)| \le p^{d(m-e)/2+(\delta-1)(n-m)-\max(0,\,\delta-2)}, \tag{3.13}$$

where $d = d(G)$ and $\delta = d\big(G/Z(G)\big)$.

With the hypothesis as in Theorem 3.12, observe that $e \ge m/d$ and $d \ge \delta$. A group is called *homocyclic* if it is a direct product of cyclic groups of the same order. Consequently, (3.13) together with (3.6) yield the following interesting bound.

Corollary 3.14 *With the hypothesis as in Theorem 3.12,*

$$|\mathcal{M}(G)| \le p^{(d-1)(2n-m)/2} \tag{3.15}$$

and the equality holds if G is homocyclic of exponent p^e.

A recent improvement of the bound given in Theorem 3.10 is the following result due to Niroomand [96].

Theorem 3.16 *Let G be a finite p-group of order p^n with $\gamma_2(G)$ of order $p^k > 1$. Then*

$$|\mathcal{M}(G)| \le p^{\frac{1}{2}(n+k-2)(n-k-1)+1}.$$

In particular,

$$|\mathcal{M}(G)| \le p^{\frac{1}{2}(n-1)(n-2)+1}.$$

Let G be a group and $d(G)$ the cardinality of a minimal set of generators of G. With this notation, the *rank* of G, denoted $r(G)$, is defined as

$$r(G) = \max_{H \leq G} d(H).$$

The following result is due to González-Sánchez–Nicolas [44, Theorem 2], which is a refinement of a result of Lubotzky–Mann [83, p. 494].

Theorem 3.17 *If G is a finite p-group of rank $r = r(G)$ and exponent p^e, then*

$$\exp\big(\mathcal{M}(G)\big) \textit{ divides } p^{e+r\lceil \log_2 \frac{r \log_2 p+1}{p-1} \rceil}.$$

As a generalization of Schur multiplier, the higher multipliers $\mathcal{M}^{(n)}(G)$, $n \geq 1$, called the *Baer invariants*, of the group G with free presentation F/R are defined as follows:

$$\mathcal{M}^{(n)}(G) = \frac{R \cap \gamma_{n+1}(F)}{[R, {}_nF]},$$

where $[R, {}_iF] = [[R, {}_{i-1}F], F]$ for $i > 1$.

Mashayekhy–Hokmabadi–Mohammadzadeh [90, Theorem 3.3] showed that for a finite p-group of nilpotency class c and exponent p^e,

$$\exp\big(\mathcal{M}^{(n)}(G)\big) \text{ divides } p^{e+\lfloor \log_p c \rfloor (c-1)} \text{ for } n \geq 1.$$

In particular, for Schur multiplier, we thus have the following result.

Theorem 3.18 *If G is a finite p-group of class c and exponent p^e, then*

$$\exp\big(\mathcal{M}(G)\big) \textit{ divides } p^{e+\lfloor \log_p c \rfloor (c-1)}.$$

We now proceed to study automorphism groups of finite groups in the forthcoming sections.

3.2 Automorphisms of Finite Abelian Groups

We begin with a study of the group of automorphisms of a finite abelian group. Let A be a finite abelian group and

$$A = \oplus_p A_p,$$

the decomposition of A as a product of its Sylow p-subgroups. It is easy to see that an automorphism of A induces an automorphism of A_p for every prime p dividing the order of A. Thus, we have a homomorphism

$$\operatorname{Aut}(A) \to \oplus_p \operatorname{Aut}(A_p).$$

It is not difficult to show that this homomorphism is an isomorphism.

Lemma 3.19 $\operatorname{Aut}(A) \cong \oplus_p \operatorname{Aut}(A_p)$.

It thus suffices to consider only finite abelian p-groups.

Let A be a finite abelian p-group of order p^m, where $m \geq 1$. Let

$$A = \mathrm{C}_{p^{m_1}} \oplus \cdots \oplus \mathrm{C}_{p^{m_r}}, \tag{3.20}$$

be a cyclic decomposition of A, where $\mathrm{C}_{p^{m_i}} = \langle a_i \rangle$ and $m_1 \leq \cdots \leq m_r$, so that

$$|A| = p^{m_1 + \cdots + m_r}.$$

Clearly, every endomorphism $\gamma : A \to A$ is defined by setting

$$\gamma(a_i) = \prod_{j=1}^{r} a_j^{\gamma_{ij}}$$

for each i such that $1 \leq i \leq r,\ 0 \leq \gamma_{ij} < p^{m_j}$, provided that each element $\gamma(a_i)$ has order not exceeding that of a_i. Let (γ_{ij}) denote the $r \times r$ matrix with integer entries γ_{ij}. A curious reader can work out the details of the following (see Ranum [100, Theorem 13], Howarth [63, Lemma 2.1] and Hiller–Rhea [57, Theorem 3.6]):

Exercise 3.21 γ is an automorphism if and only if $\det(\gamma_{ij}) \not\equiv 0 \mod p$.

The following result is due to Ledermann–Neumann [80, Lemma 3.1] (see also [58]).

Proposition 3.22 *Let A be a finite abelian p-group and φ the Euler's totient function. Then $\varphi\big(|A|\big)$ divides* $|\operatorname{Aut}(A)|$.

Proof With (3.20) as the cyclic decomposition of A, let $\theta : A \to A$ be the automorphism defined by setting

$$\theta(a_i) = \begin{cases} a_1^{l_1} \cdots a_r^{l_r} & \text{if } i = r,\ \text{where } 0 \leq l_j < p^{m_j} \text{ for } 1 \leq j \leq r-1 \\ & \text{and } (l_r,\ p) = 1, \\ & \\ a_i & \text{if } i \neq r. \end{cases} \tag{3.23}$$

Notice that the number of choices for l_r is $\varphi(p^{m_r})$ and the number of choices for each l_i with $i < r$ is p^{m_i}. Thus, the number of automorphisms of type θ is

$$p^{m_1} \ldots p^{m_{r-1}} \varphi(p^{m_r}) = \varphi\big(|A|\big).$$

Since the set of automorphisms θ constructed above clearly forms a subgroup of the group $\operatorname{Aut}(A)$, it follows that $\varphi\big(|A|\big)$ divides $|\operatorname{Aut}(A)|$. □

Remark 3.24 Since the function φ is multiplicative, that is, $\varphi(ab) = \varphi(a)\varphi(b)$ for natural numbers $a,\ b$ with $(a,\ b) = 1$, it follows that:

If A is a finite abelian group, then $\varphi\big(|A|\big)$ divides $|\operatorname{Aut}(A)|$.

For a finite abelian p-group A, in fact the precise order of $\operatorname{Aut}(A)$ can be easily computed. We proceed to state the result. Suppose that, for $1 \le l \le k$, A with cyclic decomposition (3.20) has r_l generators of order p^{n_l}, where $n_1 < \cdots < n_k$. Then

$$A = \underbrace{\mathrm{C}_{p^{n_1}} \oplus \cdots \oplus \mathrm{C}_{p^{n_1}}}_{r_1} \oplus \cdots \oplus \underbrace{\mathrm{C}_{p^{n_l}} \oplus \cdots \oplus \mathrm{C}_{p^{n_l}}}_{r_l} \oplus \cdots \oplus \underbrace{\mathrm{C}_{p^{n_k}} \oplus \cdots \oplus \mathrm{C}_{p^{n_k}}}_{r_k}. \tag{3.25}$$

Notice that $\sum_{l=1}^{k} r_l = r$. It follows that for each $1 \le i \le r$, there exists a unique l such that $1 \le l \le k$ and $m_i = n_l$.

For each t such that $1 \le t \le r$, set

$$d_t = \max\{s \mid m_s = m_t\} \text{ and } c_t = \min\{s \mid m_s = m_t\}. \tag{3.26}$$

With this setting, we have the following formula due to Hiller–Rhea given in their work [57] to which we refer the reader for more details.

Theorem 3.27 *Let A be an abelian p-group with cyclic decomposition (3.20), (3.25). Then*

$$|\operatorname{Aut}(A)| = \prod_{t=1}^{r}(p^{d_t} - p^{t-1}) \prod_{j=1}^{r}(p^{m_j})^{r-d_j} \prod_{i=1}^{r}(p^{m_i-1})^{r-c_i+1}. \tag{3.28}$$

Now, we proceed towards determining a Sylow p-subgroup of $\operatorname{Aut}(A)$. Let $\{a_1, \ldots, a_r\}$ be a basis of A. For each $1 \le i \le r$, we define

$$V_i = \langle a_1, \ldots, a_{i-1}, a_i^p, \ldots, a_r^p \rangle$$

and

$$A_i = V_i \cap \Omega_{m_i}(A).$$

For each $1 \le i \le r$, let l be such that $1 \le l \le k$ and $m_i = n_l$. Notice that $\Omega_{m_i}(A) = \Omega_{n_l}(A)$ for all i such that $m_i = n_l$. Setting $j = (\sum_{s=1}^{l} r_s) + 1$, we see that $\Omega_{m_i}(A)V_i = V_j$. Then

$$\Omega_{m_i}(A)/A_i = \Omega_{m_i}(A)/\big(\Omega_{m_i}(A) \cap V_i\big) \cong \Omega_{m_i}(A)V_i/V_i = V_j/V_i.$$

Since $|V_j/V_i| = p^{j-i}$, we get

$$|A_i| = |\Omega_{m_i}|\, p^{i-j} = |\Omega_{m_i}|\, p^{(i-\sum_{s=1}^{l} r_s - 1)}. \tag{3.29}$$

Let $(b_1, \ldots, b_r) \in A_1 \times \cdots \times A_r$. Define $\theta : A \to A$ by setting

$$\theta(a_i) = a_i b_i$$

for $1 \le i \le r$. Observe that θ is an endomorphism of A. Let (θ_{ij}) be the matrix corresponding to θ obtained by replacing each b_i by a product of powers of a_i's. Notice that

$$\theta_{ij} \equiv \begin{cases} 1 \mod p & \text{if } i = j, \\ 0 \mod p & \text{if } i > j. \end{cases} \tag{3.30}$$

Since $\det(\theta_{ij}) \not\equiv 0 \mod p$, it is an automorphism of A by Exercise 3.21.

Let $\Delta(A)$ denote the set of all automorphisms θ defined above. It is easy to see that $\Delta(A)$ is a subgroup of $\mathrm{Aut}(A)$ and

$$|\Delta(A)| = \prod_{i=1}^{r} |A_i|.$$

We now present the following result of Howarth [63, Lemma 2.4].

Proposition 3.31 *$\Delta(A)$ is a Sylow p-subgroup of* $\mathrm{Aut}(A)$ *of order*

$$\prod_{j=1}^{r} p^{m_j(r-d_j)} \prod_{i=1}^{r} p^{(m_i-1)(r-c_i+1)} \prod_{t=1}^{r} p^{t-1}.$$

Proof Notice that for each $1 \le l \le k$, we have

$$|\Omega_{n_l}(A)| = p^{\sum_{j=1}^{l-1} n_j r_j} p^{n_j (r - \sum_{j=1}^{l-1} r_j)}$$

and

$$\prod_{j=c_l}^{d_l} |A_j| = \left(p^{\sum_{j=1}^{l-1} n_j r_j}\ p^{n_l (r - \sum_{j=1}^{l-1} r_j)}\right)^{r_l} p^{-\frac{r_l(r_l+1)}{2}}.$$

With the preceding information, we have

$$\begin{aligned} |\Delta(A)| &= \prod_{i=1}^{r} |A_i| \\ &= \prod_{l=1}^{k} \big(\prod_{j=c_l}^{d_l} |A_j|\big) \\ &= \prod_{l=1}^{k} \left(p^{\sum_{j=1}^{l-1} n_j r_j}\ p^{n_l (r - \sum_{j=1}^{l-1} r_j)}\right)^{r_l} p^{-\frac{r_l(r_l+1)}{2}} \\ &= \prod_{l=1}^{k} \left(p^{\sum_{j=1}^{l-1} n_j r_j}\ p^{n_l (r - d_l)} p^{n_l r_l}\right)^{r_l} p^{-\frac{r_l(r_l+1)}{2}} \end{aligned}$$

$$
\begin{aligned}
&= \prod_{l=1}^{k} \left(p^{n_l(r-d_l)}\right)^{r_l} \prod_{l=1}^{k} \left(p^{\sum_{j=1}^{l} n_j r_j}\right)^{r_l} \, p^{-\frac{r_l(r_l+1)}{2}} \\
&= \prod_{l=1}^{k} \left(p^{n_l(r-d_l)}\right)^{r_l} \prod_{l=1}^{k} \, (p^{n_l r_l})^{r-c_l+1} \, p^{-\frac{r_l(r_l+1)}{2}} \\
&= \prod_{l=1}^{k} \left(p^{n_l(r-d_l)}\right)^{r_l} \prod_{l=1}^{k} (p^{(n_l-1)r_l})^{r-c_l+1} \, p^{r_l(r-c_l+1)} \, p^{-\frac{r_l(r_l+1)}{2}} \\
&= \prod_{l=1}^{k} \left(p^{n_l(r-d_l)}\right)^{r_l} \prod_{l=1}^{k} (p^{(n_l-1)r_l})^{r-c_l+1} \prod_{l=1}^{k} p^{r_l(r-c_l+1)} \, p^{-\frac{r_l(r_l+1)}{2}} \\
&= \prod_{j=1}^{r} p^{m_j(r-d_j)} \prod_{i=1}^{r} p^{(m_i-1)(r-c_i+1)} \prod_{t=1}^{r} p^{t-1}. \qquad (3.32)
\end{aligned}
$$

Comparing equations (3.28) and (3.32), it follows that $\Delta(A)$ is a maximal p-subgroup of $\operatorname{Aut}(A)$, and hence a Sylow p-subgroup. □

As a special case, we obtain the following result of Howarth [63, Corollary 2.6].

Theorem 3.33 *Let A be an abelian p-group of order p^m with cyclic decomposition as in (3.20) such that $2m_r \leq m$. Then $|\operatorname{Aut}(A)|_p \geq p^{2m-3}$.*

Proof Notice that, since $\Omega_{m_r}(A) = A$, we have

$$|A_r| = \frac{|A|}{p} = p^{m-1}.$$

If $m_r = m_{r-1}$, then

$$|A_{r-1}| = \frac{|A|}{p^2} = p^{m-2},$$

and hence

$$|\operatorname{Aut}(A)|_p \geq p^{m-1} p^{m-2} = p^{2m-3}.$$

If $m_r > m_{r-1}$, then $m_{r-2} \geq 1$. Observe that

$$|\Omega_{m_r}(A)| = p^m,$$

$$|\Omega_{m_{r-1}}(A)| = p^{m-m_r+m_{r-1}}$$

and

$$|\Omega_{m_{r-2}}(A)| = p^{m-m_r-m_{r-1}+2m_{r-2}}.$$

Therefore, we obtain

$$|\operatorname{Aut}(A)|_p \geq \prod_{i=r-1}^{r} |A_i| \geq p^{m-1} p^{m-m_r+m_{r-1}-1} p^{m-m_r-m_{r-1}+2m_{r-2}-2} > p^{2m-3},$$

and the proof is complete. □

Notice that, if, in addition, $m \geq 3$ in the preceding theorem, then $|\operatorname{Aut}(A)|_p \geq p^m$. We next present the following result which establishes this fact only with the hypothesis that $m \geq 3$. The result is originally due to Otto [98], however, the proof presented below is different.

Theorem 3.34 *Let A be a non-cyclic abelian p-group of order p^m with $m \geq 3$. Then p^m divides $|\operatorname{Aut}(A)|$.*

Proof By Proposition 3.31, $\operatorname{Aut}(A)$ has a Sylow p-subgroup of order

$$\prod_{j=1}^{r} p^{m_j(r-d_j)} \prod_{i=1}^{r} p^{(m_i-1)(r-c_i+1)} \prod_{t=1}^{r} p^{t-1},$$

which we denote by p^N. Observe that $r - c_i \geq 0$ for all $1 \leq i \leq r$, and $r - d_j \geq 1$ for all $1 \leq j \leq r - r_k$. Hence, we have

$$\begin{aligned} N &= \sum_{j=1}^{r} m_j(r-d_j) + \sum_{i=1}^{r}(m_i-1)(r-c_i+1) + \sum_{t=1}^{r}(t-1) \\ &\geq \sum_{j=1}^{r-r_k} m_j + \sum_{i=1}^{r}(m_i-1) + \frac{r(r-1)}{2} \\ &= \sum_{j=1}^{r-r_k} m_j + \sum_{i=1}^{r} m_i + \frac{r(r-1)}{2} - r \\ &= m + \sum_{i=1}^{r-r_k} m_i + \frac{r^2-3r}{2}. \end{aligned}$$

If $r \geq 3$, then $N \geq m$, and we are done. If $r = 2$, then either $k = 1$ or $k = 2$. If $k = 2$, then $N \geq m$, and we are done again. Finally, assume that $k = 1$. In this case, $G = \mathrm{C}_{p^{m_1}} \times \mathrm{C}_{p^{m_2}}$ with $m_1 = m_2 \geq 2$. Thus,

$$N = \sum_{i=1}^{2}(m_i - 1)2 + 1 = n + 2m_1 - 3 > m,$$

and the proof is complete. □

Notice that the preceding theorem establishes the fact that non-cyclic abelian p-groups of order greater than p^2 admit the Divisibility Property (as stated in the introduction). This property for non-abelian finite p-groups is dealt with in detail in the next two chapters.

It is easy to see that:

(1) If A is a cyclic group of order p^n, then p^n does not divide $|\operatorname{Aut}(A)|$, but p^{n-1} divides $|\operatorname{Aut}(A)|$.
(2) If $A = \mathrm{C}_p \oplus \mathrm{C}_p$, then p divides $|\operatorname{Aut}(A)|$.

As a consequence, we retrieve the following result of Hilton [58].

Theorem 3.35 *If A is a finite abelian group such that p^n divides $|A|$, then p^{n-1} divides $|\operatorname{Aut}(A)|$. In other words, if $|A|_p \geq p^n$, then $|\operatorname{Aut}(A)|_p \geq p^{n-1}$.*

We next present an important result [49, Lemma 7.1], which according to Green, was originally proved by Howarth, and a simpler proof of which, presented below, was given by Hall.

Theorem 3.36 *Let A be a finite abelian group and B, C subgroups of A. Let p be any prime. Then*

$$|\operatorname{Aut}^{A/B,\,C}(A)|_p \geq \frac{|B|_p}{p\,|C|_p}.$$

Proof Since A is abelian, it is sufficient to consider the case when A is a p-group. Let p^r be the exponent of A/C. Then there exists an element $Cu \in A/C$ of order p^r and we can write

$$A/C = \langle Cu\rangle \oplus C_1/C$$

for some subgroup C_1 of A containing C. Notice that A/C_1 is cyclic of order p^r. Setting $A_1 = \langle u^p,\ C_1\rangle$, we see that $|A/A_1| = p$. Let

$$B_1 = \{x \in B \cap A_1 \mid x^{p^r} = 1\}.$$

For each $x \in B_1$, define $\gamma_x : A \to A$ by setting

$$\gamma_x(a) = ax^{n_a}$$

for all $a \in A$, where the integer n_a is determined by the congruence $a \equiv u^{n_a} \mod C_1$ and $0 \leq n_a < p^r$. It is straightforward to see that γ_x is an endomorphism of A. Notice that $\gamma_x(c) = c$ for all $c \in C_1$. Let $1 \neq a = u^l c \in A$ for some $0 \leq l < p^r$ and $c \in C_1$. Then $\gamma_x(a) = 1$ implies that

$$1 = \gamma_x(u^l c) = \gamma_x(u^l)c = \gamma_x(u)^l c = (ux)^l c,$$

and hence

$$(ux)^l \in C_1.$$

Since $x \in B_1$, we can write $x = u^{pk}c'$ for some $c' \in C_1$ and for $0 \le k < p^{r-1}$. Thus, we get $(u^{pk+1}c')^l \in C_1$, and hence $u^{(pk+1)l} \in C_1$. It follows that p^r divides $(pk+1)l$, which is a contradiction. Hence, γ_x is injective, and consequently an isomorphism. Since $a^{-1}\gamma_x(a) = x^{n_a} \in B$, we have that $\gamma_x \in \mathrm{Aut}^{A/B,\,C}(A)$.

The set of all such automorphisms form a group and is in bijection with B_1. For, if $x,\ y \in B_1$, then

$$\gamma_x\gamma_y(a) = \gamma_x(ay^{n_a}) = \gamma_x(a)\gamma_x(y^{n_a}) = ax^{n_a}(yx^{n_y})^{n_a} = az^{n_a} = \gamma_z(a),$$

where $z = yx^{1+n_y}$, $a \equiv u^{n_a} \mod C_1$ and $y \equiv u^{n_y} \mod C_1$. Obviously the map $x \mapsto \gamma_x$ is a surjection. Further, if $x,\ y \in B_1$ are such that $\gamma_x = \gamma_y$, then $\gamma_x(u) = \gamma_y(u)$. Since $n_u = 1$, we have $x = y$ and the map $x \mapsto \gamma_x$ is a bijection.

Set $E = B \cap C$. Then $B/E \cong BC/C \le A/C$, and hence the exponent of B/E is at most p^r. Notice that B has a subgroup $B_0 \cong B/E$ and $B_0 \cap A_1 \le B_1$. Hence, we obtain

$$|\,\mathrm{Aut}^{A/B,\,C}(A)|_p \ge |B_1| \ge |B_0 \cap A_1| \ge \frac{|B_0|}{p} = \frac{|B|}{p\,|E|} \ge \frac{|B|}{p\,|C|},$$

which completes the proof. □

As a consequence of the preceding result, we get another proof of Theorem 3.35 by taking $A = B$ and $C = 1$. We need the following basic result which is of independent interest.

Lemma 3.37 *Let A be an abelian p-group and M a maximal subgroup of A. Then there exists an element $x \in A$ and a subgroup H of M such that $A = H \oplus \langle x\rangle$ and $M = H \oplus \langle x^p\rangle$.*

Proof We proceed by induction on $|A|$. Notice that, if $|A| \le p$, then the claim holds trivially.

Let $\exp(A) = q = p^e > p$. Any element $y \in A$ with order q lies in a basis of A. Therefore, there exists a subgroup K of A such that $A = \langle y\rangle \oplus K$. Furthermore, $|K| < |A|$, since y has order $q > 1$.

Let M be a maximal subgroup subgroup of A. Suppose that M contains the above element y. Then

$$M = \langle y\rangle \oplus (M \cap K),$$

where $M \cap K$ is a maximal subgroup of K. By induction, there exist a subgroup $L < K$ and an element $x \in K$ such that $K = L \oplus \langle x\rangle$ and $M \cap K = L \oplus \langle x^p\rangle$. The claim now follows with this $\langle x\rangle$ and the subgroup $H = L \oplus \langle y\rangle$ of A. We have handled every case where M contains some element y of order q.

Assume that no element y of order q lies in M. Let $\{x_1, \ldots, x_d\}$ be a basis of A with $|x_1| = \exp(A) = q$. Since M contains no element of order q, it is contained in the subgroup $N = \langle x_1^p\rangle \oplus \cdots \oplus \langle x_d\rangle$, which has index p in A. Since M is maximal in A, we must have $M = N$. Then the claim follows with $\langle x_1\rangle$ and $H = \langle x_2\rangle \oplus \cdots \oplus \langle x_d\rangle$. □

The following two results provide lower bounds on the automorphism groups of finite abelian p-groups.

Proposition 3.38 *Let A be a finite abelian group of order p^n with $n \geq 2$, and M a maximal subgroup of A. Then*

$$|\operatorname{Aut}^{A/M}(A)|_p \geq p^{n-2}.$$

Proof By Lemma 3.37, there exists an element $x \in A$ and a subgroup H of M such that

$$A = H \oplus \langle x \rangle.$$

Let $|\langle x \rangle| = p^i$ and $|H| = p^j$. By Theorem 3.35, there exists a subgroup U' of $\operatorname{Aut}(H)$ of order at least p^{j-1}. Let V' be the group of automorphisms of $\langle x \rangle$ of the form

$$x \mapsto x^{1+kp}$$

for $0 \leq k < p^{i-1}$. Notice that V' is the Sylow p-subgroup of $\operatorname{Aut}\big(\langle x \rangle\big)$. Let U and V be the subgroups of $\operatorname{Aut}(A)$ obtained by extending elements of U' and V' to automorphisms of A, respectively. Since $\langle U, V \rangle \leq \operatorname{Aut}^{A/M}(A)$, we obtain

$$|\operatorname{Aut}^{A/M}(A)|_p \geq |\langle U, V \rangle| \geq p^{i+j-2} = p^{n-2},$$

and the proof is complete. □

Proposition 3.39 *Let A be a finite abelian p-group and $B \leq A$. If $d(B) < d(A)$, then $\operatorname{Aut}^B(A)$ has a subgroup of order $p^{d(A)-1}$. In particular,*

$$|\operatorname{Aut}^B(A)|_p \geq p^{d(A)-1}.$$

Proof Choose a maximal subgroup M of A containing B. Then, by Lemma 3.37, we can write $A = H \oplus \langle x \rangle$ and $M = H \oplus \langle x^p \rangle$ for some $x \in A$ and subgroup H of M. Notice that $|\Omega_1(H)| = p^{d(A)-1}$. For each $z \in \Omega_1(H)$, define a map $\theta : A \to A$ by setting

$$\theta(a) = \begin{cases} az & \text{if } a = x, \\ a & \text{if } a \in H. \end{cases}$$

It is easy to see that $\theta \in \operatorname{Aut}^M(A)$, and hence $|\operatorname{Aut}^B(A)| \geq |\operatorname{Aut}^M(A)| \geq p^{d(A)-1}$. □

We conclude this section by noticing that Theorem 3.35 confirms Conjecture 3.1 for finite abelian groups. The conjecture in full generality is dealt with in the next section.

3.3 Ledermann–Neumann's Theorem

In this section, we present a slight improvement of a theorem of Ledermann–Neumann [81, Theorem 8.6], which confirms Conjecture 3.1, and is essentially the culmination of the initial work by Herstein–Adney [55] and Scott [114]. The result is formulated as follows.

Theorem 3.40 *The function* $f : \mathbb{N} \to \mathbb{N}$ *defined by*

$$f(h) = \begin{cases} 2 & \textit{if } h = 1, \\ 3 & \textit{if } h = 2, \\ \frac{h(h-1)^2}{2} + h & \textit{if } h \geq 3, \end{cases}$$

satisfies the property that, for each $h \in \mathbb{N}$ *and each prime* p*, if* G *is any finite group such that* $p^{f(h)}$ *divides* $|G|$*, then* p^h *divides* $|\operatorname{Aut}(G)|$.

For proving the preceding theorem, a number of preparatory steps are needed, the first being the following result [80, Lemma 4.9].

Proposition 3.41 *Let* $1 \to N \to G \to H \to 1$ *be a central extension of finite groups. Let* $|H| = |G/N| = m$ *and* $d(N) = s$*. Then there exists a central extension* $1 \to N^* \to G^* \to H \to 1$ *such that the following conditions hold:*

(1) $G \leq G^*$ *and* $N \leq N^*$*;*
(2) $d(N^*) = s$*,* $|N^*/N| = m^s$ *and every element of* N *has an* m^{th} *root in* N^**;*
(3) N^* *has a relative complement* X^* *in* G^* *such that the exponent of*

$$Y^* := X^* \cap N^*$$

divides m*;*
(4) $d(Y^*) \leq (m-1)\lfloor \log_2 m \rfloor$.

Proof Since N is a finite abelian group, there exists a divisible abelian group in which every element is of finite order, say T, such that N embeds in T (see [103, p. 91]). Let $\{a_1, \ldots, a_s\}$ be a basis of N. Choose $b_i \in T$ satisfying $b_i^m = a_i$ for each $1 \leq i \leq s$. Let

$$N^* = \langle b_1, \ldots, b_s \rangle.$$

Then $N \leq N^*$, and, by standard extension theory of groups, the given central extension induces a central extension

$$1 \to N^* \to G^* \to H \to 1$$

with $G \leq G^*$.

It is immediate from the above construction that the statements (1) and (2) hold. We thus proceed to prove (3) and (4).

Let $t : H \to G$ be a transversal with $t(1) = 1$ and $\mu : H \times H \to N$ the associated 2-cocycle:

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

for all $x,\ y \in H$. For $x \in H$, set

$$u(x) = \prod_{y \in H} \mu(x, y).$$

Then the element $u(x)^{-1} \in N$, and hence there exists $l^*(x) \in N^*$ such that $u(x)l^*(x)^m = 1$. The map $t^* : H \to G^*$ given by $t^*(x) = t(x)l^*(x)$ is a transversal for the extension

$$1 \to N^* \to G^* \to H \to 1$$

satisfying $t^*(1) = 1$. Further, the associated 2-cocycle μ^* is given by

$$\mu^*(x,\ y) = \mu(x,\ y)l^*(x)l^*(y)l^*(xy)^{-1}$$

for all $x,\ y \in H$ and satisfies

$$\mu^*(xy,\ z)\mu^*(x,\ y) = \mu^*(x,\ yz)\mu^*(y,\ z) \tag{3.42}$$

for all $x,\ y,\ z \in H$.

Notice that

$$u^*(x) := \prod_{y \in H} \mu^*(x, y) = u(x)l^*(x)^m = 1 \tag{3.43}$$

for all $x \in H$. From the products of both the sides of (3.42) for fixed x, y and for z ranging over H, we have

$$u^*(xy)\mu^*(x,\ y)^m = u^*(x)u^*(y) \tag{3.44}$$

for all $x,\ y \in H$. Combining (3.43) and (3.44), we have $\mu^*(x,\ y)^m = 1$ for all $x,\ y \in H$. Let

$$X^* = \langle t^*(x) \mid x \in H \rangle$$

and

$$Y^* = \langle \mu^*(x,\ y) \mid x,\ y \in H \rangle.$$

Then it can be easily seen that $Y^* = X^* \cap N^*$. Further, the above discussion shows that the exponent of Y^* divides m.

Finally, we prove (4). Let U be a minimal generating set for H of cardinality r. Then an induction argument on the length, with respect to U, of elements in the second co-ordinate of μ^*, shows, in view of (3.43), that

$$Y^* = \langle \mu^*(x, y) \mid x \in H \setminus \{1\} \text{ and } y \in U \rangle.$$

It is an elementary fact that, for any finite group S,

$$2^{d(S)} \le |S|.$$

Thus, $2^r \le m$, and hence

$$d(Y^*) \le (m-1)\lfloor \log_2 m \rfloor,$$

completing the proof. □

Let G be a finite group and $N \le \mathrm{Z}(G)$ a central subgroup. For a given prime p dividing the order of the group G, let $P \le N$ be a Sylow p-subgroup of N. Then we have the central extension

$$1 \to P \to G \to Q \to 1,$$

where $Q \cong G/P$. Notice that $\gamma_2(Q) \cong \big(P\gamma_2(G)\big)/P$. Set

$$E = Q/\gamma_2(Q) \cong G/P\gamma_2(G).$$

Then E is an abelian group and thus is the internal direct product of its subgroups E_0 and E_p, where E_p is the Sylow p-subgroup of E and E_0 is the complement of E_p in E. Thus, there exist subgroups Q_0 and Q_p of Q such that $E_0 = Q_0/\gamma_2(Q)$ and $E_p = Q_p/\gamma_2(Q)$ so that $Q = Q_0Q_p$ and $Q_0 \cap Q_p = \gamma_2(Q)$.

We set $|Q|_p = p^k$. With the preceding set-up, we have the following result.

Lemma 3.45 *There exists a transversal $t : Q \to G$ with the following property: If μ is the 2-cocycle associated to t and*

$$Y = \langle \mu(x, y) \mid x, y \in Q \rangle, \tag{3.46}$$

then $d(Y) \le \frac{k(k+1)}{2}$.

Proof We construct the transversal in a special way depending on whether an element of the group Q belongs to $\gamma_2(Q)$, Q_0 or Q_p.

Step 1: Since $\gamma_2(Q) \cong \big(P\gamma_2(G)\big)/P$, we can always choose a coset representative of an element $\tau \in \gamma_2(Q)$ from $\gamma_2(G)$, which we denote by $t'(\tau)$.

Before proceeding to the next step, we observe the following:

Let C be any group, $D \le C$ a subgroup and p a prime. If $c \in C$ such that $c^l \in D$ for some positive integer l with $(l, p) = 1$, then there exists an element $d \in D$ such that $cd = dc$ and $\big(|cd|, p\big) = 1$.

For, let $|c| = p^s m$ such that $p \nmid m$. Then there exist integers x, y such that $1 = p^s x + ly$. Let $d = c^{-ly}$, so that $cd = c^{1-ly} = c^{p^s x}$ has order dividing m, and therefore is coprime to p. Clearly $cd = dc$.

Step 2: Let $\{\epsilon_1, \ldots, \epsilon_a\}$ be a basis of E_0. For each $1 \leq i \leq a$, let ρ_i be a coset representative of ϵ_i in the extension

$$1 \to \gamma_2(Q) \to Q_0 \to E_0 \to 1.$$

Notice that $(|\epsilon_i|, p) = 1$, and hence $\rho_i^{|\epsilon_i|} \in \gamma_2(Q)$. We can modify ρ_i, if necessary, to ensure that $(|\rho_i|, p) = 1$.

Similarly, let $\{\varepsilon_1, \ldots, \varepsilon_b\}$ be a basis of E_p. Notice that

$$|E_p| \leq |Q_p| = |Q|_p = p^k,$$

and hence $b \leq k$. For each $1 \leq i \leq b$, let σ_i be a coset representative of ε_i in the extension

$$1 \to \gamma_2(Q) \to Q_p \to E_p \to 1.$$

Consider an arbitrary element

$$e = \prod_{i=1}^{a} {\epsilon_i}^{a_i} \prod_{j=1}^{b} {\varepsilon_j}^{b_j}$$

of E. We define a transversal $s : E \to Q$ for the extension

$$1 \to \gamma_2(Q) \to Q \to E \to 1$$

by setting

$$s(e) = \prod_{i=1}^{a} {\rho_i}^{a_i} \prod_{j=1}^{b} {\sigma_j}^{b_j}. \tag{3.47}$$

Step 3: Consider the extension

$$1 \to P \to G \to Q \to 1.$$

Let $t_0(\rho_i)$ be a coset representative of ρ_i in G. Notice that $(|\rho_i|, p) = 1$. Again, if necessary, we can modify $t_0(\rho_i)$ to ensure that $(|t_0(\rho_i)|, p) = 1$. Similarly, let $t_p(\sigma_i)$ be a coset representative of σ_i in G. Now we define the coset representative of the element $s(e)$, given in (3.47), by setting

$$t''\big(s(e)\big) = \prod_{i=1}^{a} t_0(\rho_i)^{a_i} \prod_{j=1}^{b} t_p(\sigma_j)^{b_j}.$$

Notice that every element $x \in Q$ can be uniquely written as $x = \tau s(e)$ for some $e \in E$ and $\tau \in \gamma_2(Q)$. Setting $t(x) = t'(\tau)t''\big(s(e)\big)$, we get a transversal $t : Q \to G$.

It only remains to show that t is the desired transversal, that is, $d(Y) \leq \frac{k(k+1)}{2}$. Let

$$Y_p = \langle \mu(\sigma_i^{b_i}, \sigma_i^{b'_i}) \mid 1 \leq i \leq b \text{ and } b_i, b'_i \in \mathbb{Z} \rangle.$$

Recall that $Y = \langle \mu(x, y) \mid x, y \in Q \rangle$. We claim that

$$Y \leq Y_p \gamma_2(G) \cap P = Y_p\big(\gamma_2(G) \cap P\big).$$

Pick an arbitrary generator ϵ_i of E_0. Recall that ρ_i is a coset representative of ϵ_i in the extension

$$1 \to \gamma_2(Q) \to Q \to E \to 1.$$

Then $t(\rho_i)^{a_i}$ and $t(\rho_i)^{a'_i}$ are coset representatives of $\rho_i^{a_i}$ and $\rho_i^{a'_i}$, respectively, where $0 \leq a_i, a'_i \leq |\epsilon_i|$, and we have

$$t(\rho_i)^{a_i} t(\rho_i)^{a'_i} = \mu(\rho_i^{a_i}, \rho_i^{a'_i}) t(\rho_i)^{a''_i}, \tag{3.48}$$

where

$$a''_i = \begin{cases} a_i + a'_i & \text{if } a_i + a'_i < |\epsilon_i|, \\ a_i + a'_i - |\epsilon_i| & \text{if } a_i + a'_i \geq |\epsilon_i|. \end{cases}$$

It follows that $t(\rho_i)^{a_i + a'_i - a''_i} = \mu(\rho_i^{a_i}, \rho_i^{a'_i}) \in P$, and hence the order of $t(\rho_i)$ is a power of p. Recall from Step 3 that $(|t(\rho_i)|, p) = 1$, which implies $\mu(\rho_i^{a_i}, \rho_i^{a'_i}) = 1$.

Similarly, for each generator ε_i of E_p, we can prove that

$$\mu(\sigma_i^{b_i}, \sigma_i^{b'_i}) = t(\sigma_i)^{b_i + b'_i - b''_i}, \tag{3.49}$$

where

$$b''_i = \begin{cases} b_i + b'_i & \text{if } b_i + b'_i < |\varepsilon_i|, \\ b_i + b'_i - |\varepsilon_i| & \text{if } b_i + b'_i \geq |\varepsilon_i|. \end{cases}$$

Notice that $\mu(\sigma_i^{b_i}, \sigma_i^{b'_i})$ need not be a trivial element in general. It is clear that Y_p can be generated by at most b elements, and hence $d(Y_p) \leq b \leq k$.

Next, we consider two arbitrary elements

$$e = \prod_{i=1}^{a} {\epsilon_i}^{a_i} \prod_{j=1}^{b} {\varepsilon_j}^{b_j} \text{ and } e' = \prod_{i=1}^{a} {\epsilon_i}^{a'_i} \prod_{j=1}^{b} {\varepsilon_j}^{b'_j}$$

of E. Then we have the following, in which, for ease of computations we read modulo $\gamma_2(G)$.

$$\begin{aligned}
t\big(s(e)\big)t\big(s(e')\big) &= \prod_{i=1}^{a} t(\rho_i)^{a_i} \prod_{j=1}^{b} t(\sigma_j)^{b_j} \prod_{i=1}^{a} t(\rho_i)^{a'_i} \prod_{j=1}^{b} t(\sigma_j)^{b'_j} \\
&= \prod_{i=1}^{a} t(\rho_i)^{a_i} t(\rho_i)^{a'_i} \prod_{j=1}^{b} t(\sigma_j)^{b_j} t(\sigma_j)^{b'_j} \\
&= \prod_{i=1}^{a} t(\rho_i)^{a''_i} \prod_{j=1}^{b} \mu(\sigma_j^{b_j}, \sigma_j^{b'_j}) \prod_{j=1}^{b} t(\sigma_j)^{b''_j} \text{ by (3.48) and (3.49)} \\
&= \prod_{j=1}^{b} \mu(\sigma_j^{b_j}, \sigma_j^{b'_j}) \prod_{i=1}^{a} t(\rho_i)^{a''_i} \prod_{j=1}^{b} t(\sigma_j)^{b''_j}.
\end{aligned}$$

Now consider the element

$$e'' = \prod_{i=1}^{a} \epsilon_i{}^{a''_i} \prod_{j=1}^{b} \varepsilon_j{}^{b''_j}.$$

Notice that $e'' = ee'$, and hence, by the definition of t, we get

$$t\big(s(e'')\big) = \prod_{i=1}^{a} t(\rho_i)^{a''_i} \prod_{j=1}^{b} t(\sigma_j)^{b''_j}.$$

Thus, modulo $\gamma_2(G)$, we get

$$t\big(s(e)\big)t\big(s(e')\big) = y(\sigma_1, \dots, \sigma_b)t\big(s(e'')\big),$$

where $y(\sigma_1, \dots, \sigma_b) \in Y_p$.

We can now move to the general case. Let $x = \tau s(e)$ and $y = \tau' s(e')$ for $e, e' \in E$ and $\tau, \tau' \in \gamma_2(Q)$. Then $xy = \tau^{s(e)}\tau' s(e)s(e')$. Notice that, by the construction, $t(\tau)$ and $t(\tau')$ lie in $\gamma_2(G)$. Therefore,

$$\begin{aligned}
\mu(x, y) &= t(x)t(y)t(xy)^{-1} \\
&= t(\tau)t\big(s(e)\big)t(\tau')t\big(s(e')\big)t\big(s(e)s(e')\big)^{-1}t\big(\tau^{s(e)}\tau'\big)^{-1} \\
&\equiv t\big(s(e)\big)t\big(s(e')\big)t\big(s(e)s(e')\big)^{-1} \mod \gamma_2(G) \\
&\equiv y(\sigma_1, \dots, \sigma_b) \mod \gamma_2(G).
\end{aligned}$$

It follows that $\mu(x, y) \in Y_p\gamma_2(G)$. Since $Y_p \le Y \le P$, we get the desired claim, namely

$$Y \le Y_p\gamma_2(G) \cap P = Y_p\big(\gamma_2(G) \cap P\big).$$

By Theorem 3.10, we have

$$|\mathcal{M}(S)| \leq p^{\frac{k(k-1)}{2}},$$

where S is a Sylow p-subgroup of Q having order p^k. By Theorem 3.7, we have

$$|\gamma_2(G) \cap P| = |\gamma_2(G) \cap P|_p \leq |\mathcal{M}(Q)|_p \leq |\mathcal{M}(S)|_p \leq |\mathcal{M}(S)| \leq p^{\frac{k(k-1)}{2}}.$$

Hence,

$$d(Y) \leq d\big(\gamma_2(G) \cap P\big) + d(Y_p) \leq \frac{k(k+1)}{2},$$

and the proof is complete. □

The following problem naturally arises at this point.

Problem 3.50 Let $1 \to N \to G \to H \to 1$ be an abelian extension of groups. Let $t_1,\ t_2 : H \to G$ be two transversals and $Y_1,\ Y_2$ be the groups generated by the images of the corresponding 2-cocycles. How are the groups $Y_1,\ Y_2$ related? In particular, if G is finite, then how are $d(Y_1),\ d(Y_2)$ related?

An automorphism γ of a group G is said to be *central* if it induces the identity automorphism on the central quotient $G/\operatorname{Z}(G)$. The set of all such automorphisms forms a normal subgroup of $\operatorname{Aut}(G)$ which we denote by $\operatorname{Autcent}(G)$. More specifically

$$\operatorname{Autcent}(G) = \big\{\phi \in \operatorname{Aut}(G) \ \mid \ g^{-1}\phi(g) \in \operatorname{Z}(G) \text{ for all } g \in G\big\}.$$

Notice that $g^{-1}\phi(g) \in \operatorname{Z}(G)$ if and only if $\phi(g)g^{-1} \in \operatorname{Z}(G)$. The group of central automorphisms is going to play a crucial role in the rest of this monograph. The following result [81, Lemma 8.5] gives a procedure for constructing non-inner central automorphisms of certain finite groups.

Proposition 3.51 *Let G be a finite group and P a Sylow p-subgroup of* $\operatorname{Z}(G)$ *with $|G/P|_p = p^k,\ k \geq 1$. Let $\{v_1, \ldots, v_r\}$ be a basis of P, $|v_i| = p^{s_i}$, and $c_i = \max\{1,\ p^{s_i-k}\}$ for each integer i such that $1 \leq i \leq r$. Then the following statements hold:*

(1) There exist automorphisms $\gamma_{i,l}$ for $0 \leq l \leq c_i - 1$ which form an abelian group Γ_i of non-inner automorphisms of G with $|\Gamma_i| = c_i$.

(2) If $i \neq j$, then $\gamma_{i,l} \neq \gamma_{j,l'}$ for all l and l', unless $l = l' = 0$.

(3) Each $\gamma_{i,l} \in$ $\operatorname{Autcent}(G)$.

Proof The main idea is to embed G in a larger group G^* and then construct certain automorphisms of G^* which restrict to G as non-inner automorphisms. The general construction of G^* is carried out at the beginning of this section. Let $\{v_1, \ldots, v_r\}$ be a basis of P. Let

$$Y^* \leq P^* \leq \operatorname{Z}(G^*) \leq G^*$$

be the corresponding groups as constructed in Proposition 3.41 after adjoining the $(p^k)^{th}$ roots of $\{v_1, \ldots, v_r\}$ to P. More precisely,

$$P^* = \langle w_1, \ldots, w_r \rangle,$$

where $w_i^{p^k} = v_i$ for each $1 \leq i \leq r$.

For each fixed $1 \leq i \leq r$ and each fixed integer l, define a homomorphism

$$\theta_{i,l} : P^* \to P^*$$

by setting

$$\theta_{i,l}(w_j) = \begin{cases} w_i^{1+lp^k} & \text{if } j = i, \\ w_j & \text{if } j \neq i. \end{cases} \tag{3.52}$$

Notice that $(1 + lp^k, p) = 1$, and consequently $\theta_{i,l}$ is an automorphism.

Next we show that $\theta_{i,l}$ leaves Y^* element-wise fixed. Let $y^* = \prod_{j=1}^{r} w_j^{n_j}$ be an element of Y^*. Then

$$\theta_{i,l}(y^*) = \prod_{j=1}^{r} \theta_{i,l}(w_j^{n_j}) = y^* w_i^{n_i l p^k}.$$

By Proposition 3.41, $(y^*)^{p^k} = 1$, and hence $(w_j^{n_j})^{p^k} = 1$ for all $1 \leq j \leq r$. In particular, $w_i^{n_i p^k} = 1$, and hence $\theta_{i,l}(y^*) = y^*$. Thus, $\theta_{i,l} \in \mathrm{Aut}^{Y^*}(P^*)$. By Corollary 2.55, $\theta_{i,l}$ can be extended to an automorphism $\gamma_{i,l}^* \in \mathrm{Aut}^{Q}(G^*)$, given by

$$\gamma_{i,l}^*\big(z^* t^*(x)\big) = \theta_{i,l}(z^*) t^*(x)$$

for all $z^* \in P^*$ and $x \in Q$.

Next we show that $\gamma_{i,l}^*$ keeps G invariant. Let

$$g = z^* t^*(x) = \left(\prod_{j=1}^{r} w_j^{m_j} \right) t^*(x)$$

be an element of G. Then

$$\gamma_{i,l}^*(g) = \theta_{i,l}(z^*) t^*(x) = \big(z^* w_i^{m_i l p^k}\big) t^*(x) = w_i^{m_i l p^k} \big(z^* t^*(x)\big) = w_i^{m_i l p^k} g = v_i^{m_i l} g \in G.$$

Let $\gamma_{i,l}$ be the restriction of $\gamma_{i,l}^*$ to G. Then $\gamma_{i,l} : G \to G$ is an automorphism. Further, for $0 \leq l \leq c_i - 1$, we have

$$\gamma_{i,l}(v_i) = \theta_{i,l}(w_i^{p^k}) = \theta_{i,l}(w_i)^{p^k} = (w_i^{1+lp^k})^{p^k} = v_i^{1+lp^k}$$

and

$$\gamma_{i,l}(v_j) = v_j \text{ for } j \neq i,$$

such that $v_i^{1+lp^k} \neq v_i$. Thus, the automorphism $\gamma_{i,l}$ is non-inner as it acts non-trivially on the center $\mathrm{Z}(G)$ of G. Notice that $\gamma_{i,0}$ is the identity automorphism of G. The set Γ_i of the automorphisms $\gamma_{i,l}$, $0 \leq l \leq c_i - 1$, clearly forms an abelian group with $|\Gamma_i| = c_i$. This proves (1). The proof of (2) is clear from the definition of $\gamma_{i,l}$.

Let $g = z^*t^*(x) = (\prod_{j=1}^{r} w_j^{m_j})t^*(x)$ be an element of G. Then

$$\gamma_{i,l}(g) = \gamma_{i,l}^*(g) = \theta_{i,l}(z^*)t^*(x) = v_i^{m_i l} g.$$

It follows that $g^{-1}\gamma_{i,l}(g) = v_i^{m_i l} \in P \leq \mathrm{Z}(G)$. Hence, $\gamma_{i,l} \in \mathrm{Autcent}(G)$ proving (3), and the proof of the proposition is complete. □

Remark 3.53 The preceding result for non-abelian finite p-groups guarantees the existence of non-inner automorphisms of order a power of p in the case when $s_i > k$ for some $1 \leq i \leq r$. That there always exists a non-inner automorphism of order a power of p in a non-abelian finite p-group, was proved by Gaschutz (see Theorem 1.32).

We need the following result on extensions of automorphisms.

Proposition 3.54 *Let $G = HK$ be a finite group such that H is a subgroup, K a normal subgroup and $H \cap K = 1$. Let $\alpha \in \mathrm{Aut}(H)$ be such that $h^{-1}\alpha(h) \in \mathrm{Z}(G)$ for all $h \in H$. Then α extends to an automorphism $\tilde{\alpha}$ in $\mathrm{Aut}^K(G)$ given by $\tilde{\alpha}(hk) = \alpha(h)k$ for $h \in H$ and $k \in K$.*

Proof Let $h_1, h_2 \in H$ and $k_1, k_2 \in K$. Then

$$\begin{aligned}
\tilde{\alpha}\big((h_1k_1)(h_2k_2)\big) &= \tilde{\alpha}\big(h_1h_2[h_2^{-1}, k_1]k_1k_2\big)\\
&= \alpha(h_1h_2)[h_2^{-1}, k_1]k_1k_2\\
&= \alpha(h_1)\big(\alpha(h_2)h_2^{-1}\big)k_1h_2k_2\\
&= \alpha(h_1)k_1\alpha(h_2)k_2, \text{ since } \alpha(h_2)h_2^{-1} \in \mathrm{Z}(G)\\
&= \tilde{\alpha}(h_1k_1)\tilde{\alpha}(h_2k_2).
\end{aligned}$$

Thus, $\tilde{\alpha}$ is a homomorphism. Obviously it is injective, and hence an automorphism. □

We are now ready to prove the main result of this section.

Proof of Theorem 3.40. We first establish the assertion for $h = 1, 2$ (Herstein–Adney [55] and Scott [114, Theorem 2], respectively).

Suppose p^2 divides $|G|$ and p does not divide $|\mathrm{Aut}(G)|$. Since $G/\mathrm{Z}(G) \cong \mathrm{Inn}(G)$, it follows that p does not divide $|G/\mathrm{Z}(G)|$, which in turn implies that G has a non-trivial central Sylow p-subgroup, say P. Thus,

$$G = P \oplus Q$$

for some subgroup Q of G whose order is not divisible by p. By Proposition 3.22, p divides $|\operatorname{Aut}(P)|$, a contradiction. Hence, p must divide $|\operatorname{Aut}(G)|$.

Suppose p^3 divides $|G|$. Let P be a Sylow p-subgroup of G of order p^n, and $N = P \cap Z(G)$. If $|P/N| \geq p^2$, then $|G/Z(G)| = |\operatorname{Inn}(G)| \geq p^2$, and hence p^2 divides $|\operatorname{Aut}(G)|$. In case $N = P$, that is, P is a central Sylow p-subgroup of G, then, as in the preceding paragraph, $G = P \oplus Q$ and, invoking Proposition 3.22, p^2 divides $|\operatorname{Aut}(P)|$, and hence divides $|\operatorname{Aut}(G)|$.

Next, suppose that $|P/N| = p$. Since $N \leq Z(P)$ and $|P/Z(P)| \neq p$, it follows that P is abelian. Let $\sigma : G \to P$ be the homomorphism $g \mapsto g^{|G/P|}$ so that $\sigma(N) = N$.

If $\operatorname{Im}(\sigma) = N$, then we have $G = \operatorname{Ker}(\sigma) \oplus N$. Now by Proposition 3.22, there exists a subgroup U' of $\operatorname{Aut}(N)$ with order at least p^{n-2}. Let U be the subgroup of $\operatorname{Aut}(G)$ consisting of automorphisms of G which are extensions of automorphisms from U'. Since $|P/N| = p$, there exists an element $x \in P \setminus Z(G)$ such that $x^p \in Z(G)$. It is easy to see that $\iota_x \notin U$ and it commutes with every element of U, and hence $|\langle \iota_x, U\rangle| \geq p^{n-1}$.

If $\operatorname{Im}(\sigma) = P$, then $|\operatorname{Ker}(\sigma)| = |G/P|$ and $P \cap \operatorname{Ker}(\sigma) = 1$. Since $\operatorname{Ker}(\sigma)$ is normal in G, we have $G = \operatorname{Ker}(\sigma)P$. Further, since $|P/N| = p$, by Proposition 3.38, $\operatorname{Aut}^{P/N}(P)$ has a subgroup V' of order at least p^{n-2}. By Proposition 3.54, there exists a subgroup V of $\operatorname{Aut}(G)$ of the same order as that of V'. As above choose an element $x \in P \setminus Z(G)$, then $\iota_x \notin V$ and it commutes with every element of V. Hence, $|\langle \iota_x,\ V\rangle| \geq p^{n-1}$, and p^2 divides $|\operatorname{Aut}(G)|$.

Now we assume that $h \geq 3$ is a fixed but arbitrary integer. Let G be a group and P a Sylow p-subgroup of the center $Z(G)$ of G. Let $Q = G/P$ and $|Q|_p = p^k$. Then $G/Z(G)$ contains a subgroup of order p^k. Since $G/Z(G) \cong \operatorname{Inn}(G)$, there exists a subgroup of $\operatorname{Inn}(G)$ of order p^k, and hence p^k divides $|\operatorname{Aut}(G)|$. Now if $k \geq h$, then we are done by taking $f(h) = k$. Therefore, from now onwards we assume that

$$0 \leq k \leq h - 1.$$

If $k = 0$, Lemma 3.45 implies that the group Y occuring in its statement is trivial, and hence the extension

$$1 \to P \to G \to Q \to 1$$

splits. In other words, $G \cong Q \oplus P$. In this case, every non-trivial automorphism $\theta \in \operatorname{Aut}(P)$ can be extended to an automorphism $\gamma \in \operatorname{Aut}_P^Q(G)$ by setting

$$\gamma(zx) = \theta(z)x$$

for all $z \in P$ and $x \in Q$. Notice that all these automorphisms are in fact central. Also, as θ ranges over a subgroup of $\operatorname{Aut}(P)$, it follows that γ ranges over a subgroup of $\operatorname{Aut}_P^Q(G)$ of the same size. Notice that, if

$$|G|_p = |\mathrm{Z}(G)|_p \geq p^{h+1},$$

then $|P| \geq p^{h+1}$. By Proposition 3.22, $\mathrm{Aut}(P)$ has a subgroup of order

$$\varphi\big(|P|\big) \geq \varphi(p^{h+1}) = p^h(p-1) \geq p^h.$$

Hence, we have $|\mathrm{Aut}(G)|_p \geq p^h$. Thus, it follows that for $k = 0$, the function $f(h) = h + 1$ works.

We now assume that

$$1 \leq k \leq h - 1. \tag{3.55}$$

Set $r = d(P)$. The rest of the proof is now divided into two cases: (1) $r > \frac{h(h-1)}{2}$; (2) $r \leq \frac{h(h-1)}{2}$.

Case (1): First notice that, in this case, $|G|_p \geq p^{\frac{h(h-1)}{2}+2}$. Given conditions, together with Lemma 3.45 imply that $d(Y) < r$. Then, by Proposition 3.39, $\mathrm{Aut}^Y(P)$ has a subgroup of order p^{r-1}. By Corollary 2.55, it follows that there is a subgroup of $\mathrm{Aut}^Q(G)$ of order p^{r-1}. Notice that, since $h \geq 3$, $\frac{h(h-1)}{2} \geq h$, it therefore follows that

$$|\mathrm{Aut}(G)|_p \geq |\mathrm{Aut}^Q(G)|_p \geq p^{r-1} \geq p^{\frac{h(h-1)}{2}} \geq p^h.$$

Thus, in this case, the function $f(h) = \frac{h(h-1)}{2} + 2$ works.

Case (2): By Proposition 3.51, $\mathrm{Aut}(G)$ contains a p-subgroup $\Gamma = \Gamma_1 \oplus \cdots \oplus \Gamma_r$ of non-inner automorphisms, and

$$|\Gamma| = \prod_{j=1}^{r} |\Gamma_j| = \prod_{j=1}^{r} c_j \geq \prod_{j=1}^{r} p^{s_j - k} = p^{-rk}\,|P|.$$

Further, notice that $\mathrm{Inn}(G)$ contains a p-subgroup I such that

$$|I| = |G/\mathrm{Z}(G)|_p = p^k.$$

Thus, $\mathrm{Aut}(G)$ contains a p-subgroup $I \oplus \Gamma$, and

$$|\mathrm{Aut}(G)|_p \geq |I \oplus \Gamma| \geq p^k\,|P|\,p^{-rk} = p^{-rk}\,|G|_p.$$

Since $k \leq h - 1$ and $r \leq \frac{h(h-1)}{2}$, we obtain

$$|\mathrm{Aut}(G)|_p \geq p^{-rk}\,|G|_p \geq p^{-\frac{h(h-1)^2}{2}}\,|G|_p.$$

Thus, if $|G|_p \geq p^{\frac{h(h-1)^2}{2}+h}$, then $|\mathrm{Aut}(G)|_p \geq p^h$. Therefore, in this case, we can take $f(h) = \frac{h(h-1)^2}{2} + h$. Since $h \geq 3$, this function works in all the cases, and the proof of the theorem is complete. □

Remark 3.56 While the values $f(h)$ of the function $f : \mathbb{N} \to \mathbb{N}$ given in Theorem 3.40 are best possible for $h = 1, 2$, as can be seen by considering $\mathrm{Aut}(\mathrm{C}_p)$ and $\mathrm{Aut}(\mathrm{C}_p \oplus \mathrm{C}_p)$, improvement of this function for $h \geq 3$ has been a matter of investigation over the years. We discuss here three such attempts: Green [49], Howarth [63], Hyde [68]. The main outcome is that the function can be brought down from a cubic to a quadratic polynomial. *It is an open problem whether this function is, in general, a linear polynomial (see Problem* 3.88).

3.4 Green's Function

In this section, we present a refinement of the function in Theorem 3.40 to a quadratic polynomial, due to Green [49, Theorem 2]. The key idea in Green's approach is the standard factorisation of a 2-cocycle corresponding to a central extension of groups (see (3.59) for definition), and using it to reduce the problem to abelian groups.

Let H be a group and $s : H \to S$ a bijection onto a set S. Let F be a free group on the set $S \setminus \{s(1)\}$. Then we have the following short exact sequence

$$1 \to R \to F \overset{\psi}{\to} H \to 1,$$

where ψ is the homomorphism induced by the bijection s and R is the kernel of ψ. Notice that $s : H \to F$ is a transversal for this extension with $s(1) = 1$. Let

$$r : H \times H \to R$$

be the corresponding function satisfying the cocycle condition (2.20). It is an easy exercise to show that R is the normal closure of $\langle r(x, y) \mid x, y \in H\rangle$ in F.

We set $\overline{R} = R/[R, F]$ and $\overline{F} = F/[R, F]$. Then we obtain the following central extension

$$1 \to \overline{R} \longrightarrow \overline{F} \xrightarrow{\overline{\psi}} H \to 1.$$

Let $\overline{s} : H \to \overline{F}$ be the transversal defined as the composition of s with the natural projection from F to $\overline{F}$. Let

$$\overline{r} : H \times H \to \overline{R}$$

be the corresponding 2-cocycle. Notice that $\overline{r}(x, y) = [R, F]r(x, y)$ for all $x, y \in H$. It follows that

$$\overline{R} = \langle \overline{r}(x, y) \mid x, y \in H\rangle.$$

The following result establishes a relation between the above central extension and an arbitrary central extension of H [49, Lemma 4.4].

Lemma 3.57 *Let $1 \to N \to G \xrightarrow{\pi} H \to 1$ be a central extension. Let $t : H \to G$ be a transversal and μ be the 2-cocycle corresponding to t. Then there exists a homomorphism $\overline{\eta} : \overline{F} \to G$ satisfying the following properties:*

(1) $\overline{\eta}\big(\overline{s}(x)\big) = t(x)$ *for all* $x \in H$*;*

(2) $\overline{\eta}\big(\overline{r}(x,\ y)\big) = \mu(x,\ y)$ *for all* $x,\ y \in H$*;*

(3) $\overline{\eta}\big(\overline{\gamma_2(F)}\big) = \gamma_2(G)$ *and* $\overline{\eta}(\overline{D}) = D$*, where* $\overline{D} = \overline{\gamma_2(F)} \cap \overline{R}$ *and* $D = \gamma_2(G) \cap N$*.*

Proof Consider the following diagram

$$\begin{tikzcd}
1 \arrow[r] & N \arrow[r] & G \arrow[r, "\pi"] & H \arrow[r] \arrow[l, bend right, "t"'] \arrow[dl, "s"] & 1 \\
1 \arrow[r] & {[R,\ F]} \arrow[r] & F \arrow[u, dotted, "\eta"] \arrow[rr] & & \overline{F} \arrow[r] \arrow[ull, dotted, "\overline{\eta}"'] & 1.
\end{tikzcd}$$

The existence of η in the diagram follows from the universal property of free groups. More precisely, $\eta(s(x)) = t(x)$ for all $x \in H$. It is easy to show that $\eta([R,\ F]) = 1$; hence we get the induced homomorphism $\overline{\eta} : \overline{F} \to G$ as shown in the diagram, and we obtain assertion (1). The assertion (2) follows by applying $\overline{\eta}$ to the equation

$$\overline{r}(x,\ y) = \overline{s}(x)\overline{s}(y)\overline{s}(xy)^{-1},$$

where $x, y \in H$.

Obviously $\overline{\eta}\big(\overline{\gamma_2(F)}\big) \leq \gamma_2(G)$. Let $g,\ h \in G$, $\pi(g) = x$ and $\pi(h) = y$. Then

$$\overline{\eta}\big([\overline{s}(x), \overline{s}(y)]\big) = [t(x),\ t(y)] = [g,\ h],$$

as the extension is central. Hence, $\overline{\eta}\big(\overline{\gamma_2(F)}\big) = \gamma_2(G)$. Clearly $\overline{\eta}(\overline{D}) \leq D$. Now let $n \in D$. Then there exists an element $u \in \overline{\gamma_2(F)}$ such that $\overline{\eta}(u) = n$. Notice that $u \in \mathrm{Ker}(\overline{\psi})$, and hence $u \in \overline{R}$, which proves (3). □

Consider a central extension

$$1 \to N \to G \to H \to 1,$$

where H is finite. By Theorem 3.7(2), $\overline{R} = \mathcal{M}(H) \oplus \overline{X}$, where $\overline{X}$ is free abelian. Therefore,

$$\overline{r}(x, y) = \overline{r}'(x,\ y)\,\overline{r}''(x, y) \tag{3.58}$$

with $\overline{r}'(x,\ y) \in \mathcal{M}(H)$ and $\overline{r}''(x,\ y) \in \overline{X}$. Set

$$\overline{\eta}\big(\overline{r}'(x,\ y)\big) = \mu'(x, y)$$

and

$$\overline{\eta}\big(\overline{r}''(x,\ y)\big) = \mu''(x,\ y).$$

Since the extension

$$1 \to N \to G \to H \to 1$$

is central, it follows that both $\overline{\mu}'$ and $\overline{\mu}'' : H \times H \to N$ are 2-cocycles and

$$\mu(x,\ y) = \mu'(x,\ y)\ \mu''(x,\ y) \tag{3.59}$$

for all $x,\ y \in H$. Equation (3.59) is referred to as a *standard factorisation* of the 2-cocycle μ. Also notice that $\mu'(x,\ y) \in D$ for all $x,\ y \in H$.

Using the cocycle μ'', we now construct an extension

$$1 \to N \to K \to H \to 1 \tag{3.60}$$

satisfying $\gamma_2(K) \cap N = 1$. Define $K = K(1,\ \mu'')$ to be the group corresponding to the associated pair $(1, \mu'')$, as defined in Theorem 2.23. Using Lemma 3.57 for the central extension (3.60), there exists a homomorphism $\overline{\xi} : \overline{F} \to K$ such that

$$\overline{\xi}\big(\overline{r'}(x,\ y)\big) = 1$$

and

$$\overline{\xi}\big(\overline{r}''(x,\ y)\big) = \mu''(x,\ y)$$

for all $x,\ y \in H$ and $\overline{\xi}(\overline{D}) = \gamma_2(K) \cap N$. Since $\overline{\xi}\big(r'(x,\ y)\big) = 1$ for all $x,\ y \in H$, it follows that $\overline{\xi}(\overline{D}) = 1 = \gamma_2(K) \cap N$.

With the above set-up, we prove the following result [49, Lemma 5.7].

Lemma 3.61 *Let G and K be as above. Then*

$$\mathrm{Aut}^H(G) \cong \mathrm{Aut}^{H,\,D}(K),$$

where $D = \gamma_2(G) \cap N$.

Proof Let $\gamma \in \mathrm{Aut}^H(G)$. Since γ is a central automorphism, it follows that γ fixes $\gamma_2(G)$ element-wise. In particular, γ fixes D element-wise. Let $t : H \to G$ be a transversal inducing μ and $t'' : H \to K$ a transversal inducing μ''. Since γ is central, there exists a map $\lambda : H \to N$ such that $\gamma\big(t(x)\big) = \lambda(x)t(x)$ for all $x \in H$. Therefore,

$$\gamma\big(\mu(x,\ y)\big) = \gamma\big(t(x)t(y)t(xy)^{-1}\big) = \mu(x,\ y)\lambda(x)\lambda(y)\lambda(xy)^{-1}.$$

On the other hand

$$\gamma\big(\mu(x, y)\big) = \gamma\big(\mu'(x,\ y)\big)\gamma\big(\mu''(x,\ y)\big) = \mu'(x,\ y)\gamma\big(\mu''(x,\ y)\big).$$

Hence, we get

$$\mu(x,\ y)\lambda(x)\lambda(y)\lambda(xy)^{-1} = \mu'(x, y)\gamma\big(\mu''(x,\ y)\big),$$

and therefore

$$\gamma\big(\mu''(x,\ y)\big) = \mu''(x, y)\lambda(x)\lambda(y)\lambda(xy)^{-1}.$$

The pair $(1,\ \gamma|_N) \in \mathrm{Aut}(H) \times \mathrm{Aut}(N)$ satisfies conditions of Proposition 2.51, and hence the map $\gamma^* : K \to K$ defined by

$$\gamma^*\big(n\ t''(x)\big) = \gamma(n)\lambda(x)t''(x)$$

for all $n \in N$ and $x \in H$, is an element of $\mathrm{Aut}^H(K)$. As $\gamma = \gamma^*$ on N and $D \leq N$, we have $\gamma^* \in \mathrm{Aut}^{H,\,D}(K)$.

Next we show that the map

$$\Phi : \mathrm{Aut}^H(G) \to \mathrm{Aut}^{H,\,D}(K),$$

given by $\Phi(\gamma) = \gamma^*$, is an isomorphism. It is an easy exercise to show that Φ is an injective homomorphism. It only remains to show that Φ is surjective. Let $\delta \in \mathrm{Aut}^{H,D}(K)$. Consider the pair $(1, \delta|_N) \in \mathrm{Aut}(H) \times \mathrm{Aut}(N)$. Since $\delta \in \mathrm{Aut}^H(K)$, there exists a map $\lambda : H \to N$ such that

$$\delta\big(t''(x)\big) = \lambda(x)t''(x)$$

for all $x \in H$. Applying δ on

$$\mu''(x,\ y) = t''(x)t''(y)t''(xy)^{-1},$$

we have

$$\delta\big(\mu''(x,\ y)\big) = \mu''(x,\ y)\lambda(x)\lambda(y)\lambda(xy)^{-1}.$$

Further, since $\mu'(x,\ y) \in D$, we have $\delta\big(\mu'(x,\ y)\big) = \mu'(x,\ y)$. Thus,

$$\delta\big(\mu(x,\ y)\big) = \mu(x, y)\lambda(x)\lambda(y)\lambda(xy)^{-1}.$$

It follows that the pair $(1,\ \delta|_N)$ satisfies the conditions of Proposition 2.51, and hence defines an automorphism $\gamma \in \mathrm{Aut}^H(G)$ with $\gamma^* = \delta$. □

Set $M = K/\gamma_2(K)$, the abelianization of K. Since $\gamma_2(K) \cap N = 1$, we have $N \cong \big(N\gamma_2(K)\big)/\gamma_2(K)$. Thus, we can regard N as a subgroup of M and conclude that

$$M/N \cong \big(K/\gamma_2(K)\big)/\big(N\gamma_2(K)/\gamma_2(K)\big) \cong K/\big(N\gamma_2(K)\big) \cong H/\gamma_2(H).$$

Thus, we have an extension

$$1 \to N \to M \to \overline{H} \to 1$$

of abelian groups, where $\overline{H} = H/\gamma_2(H)$. With these notations, we have the following result [49, Lemma 5.8].

Lemma 3.62 *There exists an isomorphism*

$$\Psi : \mathrm{Aut}^{H}(K) \to \mathrm{Aut}^{\overline{H}}(M),$$

which maps $\mathrm{Aut}^{H,\,D}(K)$ *onto* $\mathrm{Aut}^{\overline{H},\,D}(M)$.

Proof We first claim that for $x_1,\ x_2 \in K$, the congruences

$$t \equiv x_1 \mod \gamma_2(K)$$

and

$$t \equiv x_2 \mod N$$

have a solution if and only if $x_1 \equiv x_2 \mod N\gamma_2(K)$; furthermore, that the solution is unique if and only if $\gamma_2(K) \cap N = 1$.

Suppose there exists a $t \in K$ such that $t = x_1k$ and $t = x_2n$ for some $k \in \gamma_2(K)$ and $n \in N$. Then equating the two equations, we get $x_1 = x_2nk^{-1}$.

Conversely, suppose that $x_1 = x_2nk$ for some $n \in N$ and $k \in \gamma_2(K)$. Then $t = x_2n$ is a common solution of the two congruences. It is easy to see that such a solution, if it exists, is unique if and only if $\gamma_2(K) \cap N = 1$.

Let $\delta \in \mathrm{Aut}^{H}(K)$. Define

$$\Psi : \mathrm{Aut}^{H}(K) \to \mathrm{Aut}^{\overline{H}}(M)$$

by setting $\Psi(\delta) = \overline{\delta}$, where $\overline{\delta} : M \to M$ is given by

$$\overline{\delta}\big(\gamma_2(K)x\big) = \gamma_2(K)\delta(x)$$

for all $x \in K$. Clearly Ψ is a homomorphism. Let $\delta \in \mathrm{Aut}^{H}(K)$ be such that $\overline{\delta} = 1$. Then

$$\delta(x) \equiv x \mod \gamma_2(K)Z$$

and

$$\delta(x) \equiv x \mod N.$$

Since $\gamma_2(K) \cap N = 1$, we get $\delta(x) = x$ for all $x \in K$, and hence Ψ is injective.

For surjectivity, let $\sigma \in \mathrm{Aut}^{\overline{H}}(M)$ and $x \in K$ be an arbitrary element. Then $\sigma\big(\gamma_2(K)x\big) = \gamma_2(K)y$ for some $y \in K$. Since

$$\sigma\big(\gamma_2(K)x\big) \equiv \gamma_2(K)x \mod \big(N\gamma_2(K)\big)/\gamma_2(K),$$

we have

$$y \equiv x \mod N\gamma_2(K).$$

Therefore, the congruences

$$t \equiv y \mod \gamma_2(K) \text{ and } t \equiv x \mod N$$

have a unique solution, say x'. Define $\delta(x) = x'$. Notice that x' is independent of the choice of a coset representative for $\gamma_2(K)y$.

Next we show that $\delta \in \mathrm{Aut}^H(K)$. Let $x_1, x_2 \in K$. Then

$$\sigma\big(\gamma_2(K)x_i\big) = \gamma_2(K)y_i$$

for $i = 1, 2$, and

$$\sigma\big(\gamma_2(K)x_1x_2\big) = \gamma_2(K)y_1y_2$$

for some $y_1, y_2 \in K$. As above, the set of congruences

$$t_1 \equiv y_1 \mod \gamma_2(K) \text{ and } t_1 \equiv x_1 \mod N,$$

$$t_2 \equiv y_2 \mod \gamma_2(K) \text{ and } t_2 \equiv x_2 \mod N,$$

$$t \equiv y_1y_2 \mod \gamma_2(K) \text{ and } t \equiv x_1x_2 \mod N$$

have unique solutions, say x_1', x_2' and x', respectively. Consequently, we get the congruences

$$x_1'x_2' \equiv y_1y_2 \mod \gamma_2(K) \text{ and } x_1'x_2' \equiv x_1x_2 \mod N$$

and

$$x' \equiv y_1y_2 \mod \gamma_2(K) \text{ and } x' \equiv x_1x_2 \mod N.$$

These congruences in turn give

$$x' \equiv x_1'x_2' \mod \gamma_2(K) \text{ and } x' \equiv x_1'x_2' \mod N.$$

Hence, $x' = x_1'x_2'$, and δ is a homomorphism.

By using the injectivity of σ, it is easy to show that δ is injective. Now we show that δ is surjective. Let $y \in K$. Then there exists $x \in K$ such that $\sigma\big(\gamma_2(K)x\big) = \gamma_2(K)y$. Consequently

$$\delta(x) \equiv y \mod \gamma_2(K).$$

Thus, $y = k_1\delta(x)$ for a unique $k_1 \in \gamma_2(K)$. Notice that $\delta(k) = k$ for all $k \in \gamma_2(K)$. Take $x_1 = k_1x$. Then

$$\delta(x_1) = \delta(k_1)\delta(x) = k_1\delta(x) = y,$$

and hence δ is surjective.

By the definition of δ, we have $\delta(x) \equiv x \mod N$, and hence $\delta \in \mathrm{Aut}^H(K)$. Also observe that

$$\Psi(\delta)\big(\gamma_2(K)x\big) = \overline{\delta}\big(\gamma_2(K)x\big) = \gamma_2(K)\delta(x) = \gamma_2(K)y = \sigma\big(\gamma_2(K)x\big)$$

for all $x \in K$, which shows that Ψ is surjective.

Since $D \leq N$, we see that if $\delta \in \mathrm{Aut}^{H,\,D}(K)$, then $\overline{\delta} \in \mathrm{Aut}^{\overline{H},\,D}(M)$, and the proof is complete. □

Combining the preceding two lemmas yields the following interesting result [49, Theorem 1].

Theorem 3.63 *Let* $1 \to N \to G \to H \to 1$ *be a central extension and* $D = \gamma_2(G) \cap N$*. Then there exists an extension of abelian groups*

$$1 \to N \to M \to \overline{H} \to 1$$

such that $\mathrm{Aut}^H(G) \cong \mathrm{Aut}^{\overline{H},\,D}(M)$.

We are now in a position to present a result of Green [49, Theorem 2], with a slight improvement, which reduces the function of Theorem 3.40 to a quadratic polynomial.

Theorem 3.64 *For integers* $h \geq 3$*, the function defined by*

$$f(h) = \frac{h(h+1)}{2} + 1$$

has the property that, for each integer $h \geq 3$ *and each prime* p*, if* G *is any finite group such that* $p^{f(h)}$ *divides* $|G|$*, then* p^h *divides* $|\mathrm{Aut}(G)|$.

Proof Let G be a finite group and $N = \mathrm{Z}(G)$. Let $H \cong G/\mathrm{Z}(G)$ and $|H|_p = p^k$. If $k \geq h$, then $\mathrm{Aut}(G)$ has a subgroup of inner automorphisms of order p^k. Hence, p^h divides $|\mathrm{Aut}(G)|$.

Assume that $k \leq h-1$. Let M and D be as in Theorem 3.63. Then, by Theorem 3.7(3)–(4),

$$|D|_p \leq |\mathcal{M}(H)|_p \leq |\mathcal{M}(P)|_p \leq p^{\frac{k(k-1)}{2}} \leq p^{\frac{(h-1)(h-2)}{2}},$$

where P is a Sylow p-subgroup of H. Since $|G/\mathrm{Z}(G)|_p = |H|_p = p^k \leq p^{h-1}$, we get

$$|\mathrm{Z}(G)|_p \geq p^{1-h}|G|_p.$$

Therefore,

$$\frac{|\operatorname{Z}(G)|_p}{|D|_p} \geq p^{1-h-\frac{(h-1)(h-2)}{2}}|G|_p = p^{-\frac{h(h-1)}{2}}|G|_p.$$

Consequently, by Theorems 3.63 and 3.36, we have

$$|\operatorname{Aut}(G)|_p \geq |\operatorname{Aut}^H(G)|_p = |\operatorname{Aut}^{\overline{H},D}(M)|_p \geq \frac{|\operatorname{Z}(G)|_p}{p|D|_p} \geq p^{-1-\frac{h(h-1)}{2}}|G|_p.$$

Hence, if $|G|_p \geq p^{\frac{h(h+1)}{2}+1}$, then $|\operatorname{Aut}(G)|_p \geq p^h$. □

3.5 Howarth's Function

In this section, we present the work of Howarth [63], wherein it is proved that, for $h \geq 12$, the function

$$f(h) = \begin{cases} \frac{h^2+3}{2} & \text{if } h \text{ is odd,} \\ \frac{h^2+4}{2} & \text{if } h \text{ is even.} \end{cases}$$

satisfies Conjecture 3.1. Notice that this function is a refinement of the function by Green Theorem 3.64 for $h \geq 12$. The key idea for getting the above improvement is to construct sufficient number of non-inner central automorphisms.

Let G be a finite group and H, K its subgroups such that $\gamma_2(G) \leq H$ and $K \leq \operatorname{Z}(G)$. Let $\{w_1, \ldots, w_t\}$ be a set of coset representatives of a minimal generating set $\{\overline{w}_1, \ldots, \overline{w}_t\}$ of G/H, where $\overline{w}_i = Hw_i$ for $1 \leq i \leq t$. With this set-up, we first present a result due to Hughes [64], the proof of which is left as an exercise to the reader.

Exercise 3.65 Let $k_1, \ldots, k_t \in K$ be such that $|k_i|$ divides $|\overline{w}_i|$ for $1 \leq i \leq t$. Then the map $\gamma : G \to G$, defined by

$$\gamma(w_i) = k_i w_i$$

for $1 \leq i \leq t$ and

$$\gamma(h) = h$$

for $h \in H$, is an endomorphism of G acting as the identity endomorphism on G/K and H. Further, γ is an automorphism if and only if $\overline{\gamma} : G/H \to G/H$ is an automorphism.

We now specialise to the situation when both G/H and K are p-groups for some p dividing $|G|$. Let $\{p^{q_1}, \ldots, p^{q_t}\}$ with $q_1 \leq \cdots \leq q_t$ be the set of invariants of G/H. Set

$$l_i = |\Omega_{q_i-1}(K)|$$

for $1 \le i \le t$. With these notations, we have the following

Proposition 3.66 $|\operatorname{Aut}^{G/\mathrm{Z}(G)}(G)|_p \ge |\operatorname{Aut}^{G/K}(G)|_p \ge l_1 \cdots l_t$.

Proof Let $W_i = \langle w_1, \ldots, w_{i-1}, w_i^p, \ldots, w_t^p, H\rangle$. For each $1 \le i \le t$, define

$$K_i = \Omega_{q_i}(K) \cap W_i.$$

Let $(k_1, \ldots, k_t) \in K_1 \times \cdots \times K_t$. Define $\theta : G \to G$ by setting

$$\theta(x) = \begin{cases} k_i w_i & \text{if } x = w_i,\ 1 \le i \le t, \\ x & \text{if } x \in H. \end{cases}$$

By Exercise 3.65, θ is an endomorphism of G. Let $\overline{\theta} : G/H \to G/H$ be the induced homomorphism

$$\overline{\theta}(\overline{w}_i) = \overline{k}_i \overline{w}_i$$

for $1 \le i \le t$. By the discussion preceding Proposition 3.31, $\overline{\theta}$ is an automorphism of G/H. Hence, it follows from Exercise 3.65 that $\theta \in \operatorname{Aut}^{G/K}(G)$. Notice that the set of all such automorphisms θ forms a p-subgroup of $\operatorname{Aut}^{G/K}(G)$, whose order is at least $|K_1| \cdots |K_t|$. It is easy to see that

$$|K_i| \ge |\Omega_{q_i-1}(K)| = l_i$$

for each $1 \le i \le t$. Hence,

$$|\operatorname{Aut}^{G/\mathrm{Z}(G)}(G)|_p \ge |\operatorname{Aut}^{G/K}(G)|_p \ge |K_1| \cdots |K_t| \ge l_1 \cdots l_t,$$

and the proof is complete □

Next we prove

Proposition 3.67 *Let G be a finite group and H, K its subgroups such that $\gamma_2(G) \le H$ and $K \le \mathrm{Z}(G)$. Then $|\operatorname{Aut}^{G/K,H}(G)|_p \ge |\operatorname{Aut}\big(K/(K \cap H)\big)|_p$.*

Proof Let D be a subgroup of K which is isomorphic to $K/(K \cap H)$, and let $\{d_1, \ldots, d_r\}$ be a minimal generating set for D. Let $\{p^{m_1}, \ldots, p^{m_r}\}$ with $m_1 \le \cdots \le m_r$ be the set of invariants of D. For each $1 \le i \le r$, define

$$V_i = \langle d_1, \ldots, d_{i-1}, d_i^p, \ldots, d_r^p\rangle$$

and

$$D_i = V_i \cap \Omega_{m_i}(D).$$

Further, for each $1 \le i \le r$ with $m_i < m_r$, let j be the smallest integer such that $m_i < m_j$, and if $m_i = m_r$, set $j = r + 1$. Then, from (3.29), we have

$$|D_i| = p^{i-j}\,|\Omega_{m_i}(D)|.$$

Since $D \cong HK/H$, it can also be viewed as a subgroup of G/H. Recall that $\{p^{q_1}, \dots, p^{q_t}\}$ is the set of invariants of G/H. For $1 \le i \le r$, set

$$s_i = t - r + i.$$

Then it follows that $r \le t$, and $m_i \le q_{s_i}$ for $1 \le i \le r$. Define

$$W_{s_i} = \langle w_1, \dots, w_{s_i-1}, w_{s_i}^p, \dots, w_t^p, H\rangle$$

and

$$E_{s_i} = W_{s_i} \cap \Omega_{q_{s_i}}(D).$$

For $1 \le i \le r$ with $q_{s_i} < q_{s_r}$, let s_k be the smallest integer such that $q_{s_i} < q_{s_k}$. And if $q_{s_i} = q_{s_r}$, set $s_k = t + 1$.

Notice that $\Omega_{q_{s_i}}(D) \le W_{s_k}$, consequently

$$\begin{aligned}|\Omega_{q_{s_i}}(D)/E_{s_i}| &= |\Omega_{q_{s_i}}(D)/\big(W_{s_i} \cap \Omega_{q_{s_i}}(D)\big)| = |\Omega_{q_{s_i}}(D)W_{s_i}/W_{s_i}|\\ &\le |\Omega_{q_{s_i}}(D)W_{s_k}/W_{s_i}| = |W_{s_k}/W_{s_i}|.\end{aligned}$$

Since $|W_{s_k}/W_{s_i}| = p^{k-i}$, we get $|E_{s_i}| \ge p^{i-k}\,|\Omega_{q_{s_i}}(D)|$.

Next we show that $|E_{s_i}| \ge |D_i|$ for each $1 \le i \le r$. For a fixed i, we have two cases, namely $m_i = q_{s_i}$ and $m_i < q_{s_i}$.

First suppose that $m_i = q_{s_i}$. If $j < k$, then $m_j > m_i = q_{s_i} = q_{s_j}$, which is a contradiction to the fact that $m_i \le q_{s_i}$ for each i. Hence, $j \ge k$, and therefore

$$|D_i| = p^{i-j}\,|\Omega_{m_i}(D)| \le p^{i-k}\,|\Omega_{q_{s_i}}(D)| \le |E_{s_i}|,$$

since $\Omega_{m_i}(D) = \Omega_{q_{s_i}}(D)$.

Now suppose that $m_i < q_{s_i}$. Then

$$|\Omega_{m_i}(D)| = p^{m_1+\cdots+m_{j-1}+m_i(r-j+1)}$$

and

$$|\Omega_{q_{s_i}}(D)| \ge p^{m_1+\cdots+m_{j-1}+(m_i+1)(r-j+1)} = p^{r-j+1}\,|\Omega_{m_i}(D)|.$$

Since $k \le r + 1$, we obtain

$$|E_{s_i}| \ge p^{i-k}\,|\Omega_{q_{s_i}}(D)| \ge p^{i-k+r-j+1}\,|\Omega_{m_i}(D)| = p^{r-k+1}\,|D_i| \ge |D_i|.$$

Further, since $D \leq K$, we have $\mathrm{Aut}^{G/D,H}(G) \leq \mathrm{Aut}^{G/K,H}(G)$. Using Proposition 3.66 for $K = D$, we get $|\mathrm{Aut}^{G/D,H}(G)|_p \geq |E_1| \cdots |E_t|$. Similarly, by the discussion preceding Proposition 3.31, we obtain

$$|\mathrm{Aut}(D)|_p = |D_1| \cdots |D_r|,$$

and hence

$$|\mathrm{Aut}^{G/K,H}(G)|_p \geq |\mathrm{Aut}(D)|_p.$$

The proof is now complete. □

A consequence of the preceding result is the following

Proposition 3.68 *Let G be a finite group and B a Sylow p-subgroup of* $\mathrm{Z}(G)/\big(\gamma_2(G) \cap \mathrm{Z}(G)\big)$. *Then*

$$|\mathrm{Aut}^{G/\mathrm{Z}(G)}(G)|_p \geq |\mathrm{Aut}(B)|_p.$$

Proof Let K and L be the Sylow p-subgroups of $\mathrm{Z}(G)$ and $\gamma_2(G) \cap \mathrm{Z}(G)$, respectively. If $G/\gamma_2(G)$ is a p-group, then the result follows by taking $H = \gamma_2(G)$ in Proposition 3.67.

Assume that $G/\gamma_2(G)$ is not a p-group. In this case, we can always choose a subgroup H of G such that $\gamma_2(G) < H$ and G/H is isomorphic to the Sylow p-subgroup of $G/\gamma_2(G)$. Observe that

$$\mathrm{Aut}^{G/K,H}(G) \leq \mathrm{Aut}^{G/\mathrm{Z}(G)}(G).$$

Since $\big(|H/\gamma_2(G)|, p\big) = 1$, we have $\gamma_2(G) \cap K = H \cap K$. Hence,

$$\begin{aligned} B &\cong K/L \\ &= K/(\gamma_2(G) \cap K) \\ &= K/(H \cap K). \end{aligned}$$

By Proposition 3.67, we get

$$|\mathrm{Aut}^{G/\mathrm{Z}(G)}(G)|_p \geq |\mathrm{Aut}\big(K/(H \cap K)\big)|_p = |\mathrm{Aut}(B)|_p,$$

and the proof is complete. □

Let m be a fixed positive integer, and t an integer such that $1 \leq t \leq m$. Let $\mathcal{L}_{m,t}$ be the collection of all finite abelian groups of order p^m and exponent p^t. For any positive integer s, define

$$L_{s,t} = \min\big\{|\Omega_s(A)| \mid A \in \mathcal{L}_{m,t}\big\}.$$

If $m = kt + d$, where $0 \leq d < t$, then it follows that

$$L_{s,t} = p^{ks+\min\{s,d\}}. \tag{3.69}$$

With these notations, we have the following number-theoretic result, proof of which is left as an exercise.

Exercise 3.70 For any positive integer s, the following statements hold:

(1) If $1 \le t \le t' \le m$, then $L_{s,t} \ge L_{s,t'}$.

(2) If $1 \le t \le m-1$, then $L_{s,t} \le L_{s+1,t+1}$.

We can now prove the main result of Howarth [63, Theorem 5.1].

Theorem 3.71 *For integers $h \ge 12$, the function defined by*

$$f(h) = \begin{cases} \frac{h^2+3}{2} & \textit{if } h \textit{ is odd}, \\[2ex] \frac{h^2+4}{2} & \textit{if } h \textit{ is even}. \end{cases}$$

has the property that, for each integer $h \ge 12$ and each prime p, if G is any finite group such that $p^{f(h)}$ divides $|G|$, then p^h divides $|\operatorname{Aut}(G)|$.

Proof For notational convenience, we denote a Sylow p-subgroup of a group G by G_p. We provide a proof only in the case when h is an odd integer with $p^{\frac{h^2+3}{2}}$ dividing $|G|$. The proof for the case h even is similar, and hence omitted.

Let $H = G/\mathrm{Z}(G)$ and $|H|_p = p^k$. If $k \ge h$, then $\operatorname{Aut}(G)$ has a subgroup of inner automorphisms of order p^k and there is nothing to prove. Therefore, let us assume that

$$0 \le k \le h-1.$$

As a result we have $|\mathrm{Z}(G)|_p \ge p^m$, where $m = \frac{h^2-2h+5}{2}$. By Theorem 3.7(3)–(4) and Theorem 3.10 we have

$$|\gamma_2(G) \cap \mathrm{Z}(G)|_p \le |\mathcal{M}(H)|_p \le |\mathcal{M}(H_p)| \le p^{\frac{k(k-1)}{2}} \le p^{\frac{(h-1)(h-2)}{2}}.$$

Consequently

$$|\mathrm{Z}(G)/\big(\gamma_2(G) \cap \mathrm{Z}(G)\big)|_p \ge p^{\frac{h+3}{2}}.$$

Denote the exponents of the groups $\big(\mathrm{Z}(G)/\big(\gamma_2(G)\cap \mathrm{Z}(G)\big)\big)_p$, $\mathrm{Z}(G)_p$ and $\big(G/\gamma_2(G)\big)_p$ by p^s, p^t and p^r respectively. It is clear that $s \le t$ and $s \le r$. Since h is odd, we have either $h \equiv 1 \mod 4$ or $h \equiv 3 \mod 4$.

First suppose that $h \equiv 1 \mod 4$. Then $\frac{h+3}{2}$ is even and we have the following two cases for s:

Case (1): $s \le \frac{h+3}{4}$. By Proposition 3.68 and Theorem 3.33, we have

$$|\operatorname{Aut}^{G/\mathrm{Z}(G)}(G)|_p \ge |\operatorname{Aut}\big(\big(\mathrm{Z}(G)/(\gamma_2(G)\cap \mathrm{Z}(G))\big)_p\big)|_p \ge p^h.$$

Case (2): $s \geq \frac{h+3}{4} + 1 = \frac{h+7}{4} = s'$ (say). Notice that $t \geq s'$ and $r \geq s'$. Let $|\Omega_{r-1}(\mathrm{Z}(G)_p)| = p^{l_r}$. Then, by Proposition 3.66, we have

$$|\operatorname{Aut}^{G/\mathrm{Z}(G)}(G)|_p \geq p^{l_r}.$$

We now have the following two subcases:
Subcase (2a): $t \leq s' + h - 1 = \frac{5h+3}{4} = t'$ (say). Using Exercise 3.70, we have

$$p^{l_r} \geq L_{r-1,t} \geq L_{s'-1,t'}.$$

Subcase (2b): $t \geq s' + h = t' + 1$. Since $r \geq t - h + 1$ by Corollary 3.8, it follows from Exercise 3.70 that

$$p^{l_r} \geq L_{r-1,t} \geq L_{t-h,t} \geq L_{t'-h,t'} \geq L_{s'-1,t'}.$$

Since $h \geq 13$, we have $4t' = 5h + 3 \leq m$. Now by (3.69) we have

$$L_{s'-1,t'} \geq p^{4(s'-1)} = p^{h+3} > p^h.$$

Next suppose that $h \equiv 3 \mod 4$. Then $\frac{h+1}{2}$ is even and again we have the following two cases for s, namely $s \leq \frac{h+1}{4}$ and $s \geq \frac{h+1}{4} + 1$. Now the proof follows as in Case (1) and (2) verbatim, and the proof of the theorem is complete for h odd. □

3.6 Hyde's Function

In this concluding section, we present a refinement of the function in Theorem 3.71. The result is due to Hyde [68]. Before proceeding further, we need the following results which are of independent interest.

Let α be a central automorphism of a group G. Then the map $f_\alpha : G \to \mathrm{Z}(G)$ given by

$$f_\alpha(g) = g^{-1}\alpha(g)$$

is a homomorphism from G to $\mathrm{Z}(G)$. The correspondence $\alpha \mapsto f_\alpha$ gives an injective map

$$\operatorname{Autcent}(G) \longrightarrow \operatorname{Hom}\big(G,\ \mathrm{Z}(G)\big).$$

Recall that a group is said to be *purely non-abelian* if it does not have any nontrivial abelian direct factor. For example, any extraspecial p-group is purely non-abelian. For purely non-abelian groups, Adney and Yen [3] proved the following result.

Theorem 3.72 *A finite group G is purely non-abelian if and only if the map* $\operatorname{Autcent}(G) \to \operatorname{Hom}\big(G,\ \mathrm{Z}(G)\big)$ *given by $\alpha \mapsto f_\alpha$ is a bijection.*

Proof Given $f \in \operatorname{Hom}\big(G, \operatorname{Z}(G)\big)$, the map $\alpha_f : G \to G$ given by

$$\alpha_f(g) = gf(g),$$

for $g \in G$, is an endomorphism. Further, α_f is an automorphism if and only if $f(g) \neq g^{-1}$ for any $g \neq 1$. We only need to show that $f(g) \neq g^{-1}$ for any $g \neq 1$ if and only if G is purely non-abelian.

If $f \in \operatorname{Hom}\big(G, \operatorname{Z}(G)\big)$ is such that $f(z) = z^{-1}$ for some $z \neq 1$, then $z \in \operatorname{Z}(G)$. We can assume that $|z| = p$ for some p dividing $|G|$. Write

$$G/\gamma_2(G) = P/\gamma_2(G) \oplus Q/\gamma_2(G),$$

where $P/\gamma_2(G)$ is the Sylow p-subgroup of $G/\gamma_2(G)$. Since $\gamma_2(G) \leq \operatorname{Ker}(f)$, $\gamma_2(G)z$ is non-trivial.

Recall that, for a finite abelian group A and an element $a \in A$, the *p-height* of a is the largest p^k such that the equation $x^{p^k} = a$ has a solution in A. Choose an element $x \in P$ such that

$$\gamma_2(G)z = \gamma_2(G)x^{p^k},$$

where p^k is the height of $z\gamma_2(G)$. Taking $y = f(x)^{-1}$, we have $z = y^{p^k}$. Further, $y \in \operatorname{Z}(G) \cap P$ and $\langle y \rangle \cap \gamma_2(G) = 1$. Now it is obvious that $\langle \gamma_2(G)y \rangle$ is a direct factor of $P/\gamma_2(G)$, and hence of $G/\gamma_2(G)$. Since $\langle y \rangle \cap \gamma_2(G) = 1$, $\langle y \rangle$ is a direct factor of G, and hence G is not purely non-abelian.

Conversely, suppose that G is not purely non-abelian. Write $G = H \oplus K$, where $H \leq \operatorname{Z}(G)$ is a non-trivial subgroup. Then the map

$$f : G \to \operatorname{Z}(G)$$

defined by $f(h) = h^{-1}$ and $f(k) = 1$ for all $h \in H$ and $k \in K$ is a homomorphism. □

Let G be a purely non-abelian group of order p^n. Let

$$G/\gamma_2(G) = \operatorname{C}_{p^{m_1}} \oplus \cdots \oplus \operatorname{C}_{p^{m_t}} \tag{3.73}$$

with $m_1 \geq \cdots \geq m_t \geq 1$ and

$$\operatorname{Z}(G) = \operatorname{C}_{p^{k_1}} \oplus \cdots \oplus \operatorname{C}_{p^{k_s}} \tag{3.74}$$

with $k_1 \geq \cdots \geq k_s \geq 1$. Then it is easy to see that

$$|\operatorname{Hom}\big(G/\gamma_2(G), \operatorname{Z}(G)\big)| = \prod_{j,\, i} |\operatorname{Hom}\big(\operatorname{C}_{p^{m_j}}, \operatorname{C}_{p^{k_i}}\big)| = \prod_{j,i} p^{\min\{m_j,\, k_i\}}.$$

Corollary 3.75 *Let G be a purely non-abelian group of order p^n with $G/\gamma_2(G)$ and $\mathrm{Z}(G)$ as in (3.73) and (3.74). Then the following statements hold:*

(1) $|\operatorname{Autcent}(G)| = p^a$, *where* $a = \sum_{j,i} \min\{m_j, k_i\}$.

(2) *If* $\exp\big(G/\gamma_2(G)\big) \le |\mathrm{Z}(G)|$, *then* $|\operatorname{Autcent}(G)| \ge |G/\gamma_2(G)|$.

Proof The proof of (1) is obvious from the preceding theorem. Set $m = \sum_j m_j$. For each fixed j, set

$$a_j = \sum_i \min\{m_j,\ k_i\}.$$

If $m_j > k_i$ for all i, then

$$p^{a_j} = p^{\sum_i k_i} = |\mathrm{Z}(G)| \ge \exp\big(G/\gamma_2(G)\big) = p^{m_1} \ge p^{m_j}.$$

Further, if $m_j \le k_i$ for some i, then $a_j \ge \min\{m_j,\ k_i\} = m_j$. Hence, by assertion (1),

$$|\operatorname{Autcent}(G)| = p^{\sum_j a_j} \ge p^m.$$

□

We need the following result of Otto [98, Theorem 1] which is proved in the next chapter as Theorem 4.6.

Theorem 3.76 *Let $G = A \times N$ be a finite p-group with A abelian and N purely non-abelian. Then*

$$|\operatorname{Aut}(G)|_p \ge |A|\,|\operatorname{Aut}(N)|_p.$$

We are now ready to discuss the bound, due to Hyde [68], for finite p-groups.

Theorem 3.77 *Let G be a finite p-group such that $|G| \ge p^{h+1}$ and $h \le 4$. Then $|\operatorname{Aut}(G)|_p \ge p^h$.*

Proof For abelian p-groups, the result follows from Theorem 3.35.

Assume that G is non-abelian. Then we have

$$|\operatorname{Inn}(G)| = |G/\mathrm{Z}(G)| \ge p^2.$$

By Theorem 1.32, there exists a non-inner automorphism of order a power of p, and therefore

$$|\operatorname{Aut}(G)|_p \ge p^3.$$

The only remaining case is $h = 4$. In this case $|G| \ge p^5$. If $|\operatorname{Inn}(G)| = |G/\mathrm{Z}(G)| \ge p^3$, then as before, $|\operatorname{Aut}(G)|_p \ge p^4$ and we are done. Suppose that $|G/\mathrm{Z}(G)| = p^2$. Then we have $|\mathrm{Z}(G)| \ge p^3$. By Theorem 1.9, $|\gamma_2(G)| = p$, and therefore

$$|G/\gamma_2(G)| \geq p^4.$$

Notice that $G/\operatorname{Z}(G)$ is elementary abelian and is isomorphic to a subgroup of $G/\gamma_2(G)$. Thus, $G/\gamma_2(G)$ has at least two cyclic factors. If G is purely non-abelian, then by Theorem 3.72, we have

$$|\operatorname{Aut}(G)|_p \geq |\operatorname{Autcent}(G)|_p = |\operatorname{Hom}\big(G/\gamma_2(G),\ \operatorname{Z}(G)\big)|_p \geq p^4.$$

If $G = H \oplus K$ with H abelian and K purely non-abelian, then by Theorem 3.76 and the preceding discussion, we have

$$|\operatorname{Aut}(G)|_p \geq |H|\, |\operatorname{Aut}(K)|_p \geq p^4.$$

Thus, the proof of the theorem is complete. □

Theorem 3.78 *Let G be a p-group such that $|G| \geq p^{f(h)}$ with $f(h) = \frac{h^2-3h+6}{2}$ and $h \geq 5$. Then $|\operatorname{Aut}(G)|_p \geq p^h$.*

Proof As in the previous theorem, the result holds when G is abelian. So, assume that G is non-abelian. If

$$|\operatorname{Inn}(G)| = |G/\operatorname{Z}(G)| \geq p^{h-1},$$

then, by Theorem 1.32, we have $|\operatorname{Aut}(G)|_p \geq p^h$.

Suppose that $|\operatorname{Inn}(G)| = |G/\operatorname{Z}(G)| \leq p^{h-2}$. Then, by Theorem 1.9, we have

$$|\gamma_2(G)| \leq p^{\frac{h^2-5h+6}{2}},$$

and hence $|G/\gamma_2(G)| \geq p^h$. Further,

$$|\operatorname{Z}(G)| \geq p^{\frac{h^2-5h+10}{2}}$$

and $\frac{h^2-5h+10}{2} \geq h$ for $h \geq 5$. Since $G/\gamma_2(G)$ and $\operatorname{Z}(G)$ are abelian p-groups, it is easy to see that

$$|\operatorname{Hom}\big(G/\gamma_2(G),\ \operatorname{Z}(G)\big)|_p \geq \min\big\{|G/\gamma_2(G)|, |\operatorname{Z}(G)|\big\} \geq p^h.$$

Now, if G is purely non-abelian, then by Theorem 3.72, we get

$$|\operatorname{Aut}(G)|_p \geq |\operatorname{Autcent}(G)|_p \geq p^h.$$

Now suppose that $G = H \oplus K$ with H non-trivial abelian and K purely non-abelian, then $|H| = p^r$ for some $r \geq 1$ and $|K| \geq p^{f(h)-r}$. If $r \geq h$, then by Theorem 3.76, we have

$$|\operatorname{Aut}(G)|_p \geq |H|\, |\operatorname{Aut}(K)|_p \geq p^h$$

and we are done. If $r \leq h$, then showing that

$$|\operatorname{Aut}(K)|_p \geq p^{h-r}$$

completes the proof of the theorem. Again, we have two cases. If $h - r \geq 5$, then $f(h) - r \geq f(h-r)$ and we can apply the proof of purely non-abelian case to get

$$|\operatorname{Aut}(K)|_p \geq p^{h-r}.$$

If $h - r \leq 4$, then $f(h) - r \geq h - r + 1$, and therefore by Theorem 3.77, we get $|\operatorname{Aut}(K)|_p \geq p^{h-r}$. □

Before presenting Hyde's function in the general case, we prove the following results, which are of independent interest.

Proposition 3.79 *Let $G = H \oplus K$, where H is an abelian group with $|H|$ divisible by p and K is a group with $|\mathrm{Z}(K) \cap \gamma_2(K)|$ divisible by p. Then*

$$|\operatorname{Aut}(G)|_p > |\operatorname{Aut}(K)|_p.$$

Proof If $|H|_p \geq p^2$, then by Theorem 3.35, we have $|\operatorname{Aut}(H)|_p \geq p$. It follows that

$$|\operatorname{Aut}(G)|_p \geq |\operatorname{Aut}(H)|_p |\operatorname{Aut}(K)|_p > |\operatorname{Aut}(K)|_p.$$

If $|H|_p = p$, then it is sufficient to consider the case when $H = \mathrm{C}_p = \langle h \rangle$. Since $\operatorname{Autcent}(G)$ is normal in $\operatorname{Aut}(G)$, we obtain

$$\begin{aligned}|\operatorname{Aut}(G)|_p &\geq |\operatorname{Autcent}(G)\operatorname{Aut}(K)|_p\\ &= \frac{|\operatorname{Autcent}(G)|_p |\operatorname{Aut}(K)|_p}{|\operatorname{Autcent}(G) \cap \operatorname{Aut}(K)|_p}\\ &= \frac{|\operatorname{Autcent}(G)|_p |\operatorname{Aut}(K)|_p}{|\operatorname{Autcent}(K)|_p}.\end{aligned}$$

Thus, it suffices to show that $|\operatorname{Autcent}(G)|_p > |\operatorname{Autcent}(K)|_p$. To this end, we proceed to construct a central automorphism of G which is not induced by a central automorphism of K. Notice that

$$G/\gamma_2(G) \cong H \oplus K/\gamma_2(K)$$

and $\mathrm{Z}(G) \cong H \oplus \mathrm{Z}(K)$. Since p divides $|\mathrm{Z}(G) \cap \gamma_2(K)|$, it has an element z of order p. Then the map sending $(h, 1) \mapsto (1, z)$ and $\big(1, \gamma_2(K)k\big) \mapsto (1, 1)$ defines a homomorphism

$$f : G/\gamma_2(G) \to \mathrm{Z}(G).$$

As in Theorem 3.72, there exists a central endomorphism σ given by

$$\sigma(g) = gf\big(\gamma_2(G)g\big).$$

We claim that σ is, in fact, an automorphism. It suffices to show that σ is injective. Let $g = (h^n, k)$ be an element of G such that

$$\sigma(g) = (h^n, kz^n) = (1, 1).$$

Then $h^n = 1$ and $n \equiv 0 \mod p$. It follows that $g = (h^n, k) = (1, 1)$. Notice that σ has order p and is not induced by an automorphism of K. Further, one can see that σ centralizes $\operatorname{Autcent}(K)$. Hence,

$$|\operatorname{Autcent}(G)|_p \geq |\operatorname{Autcent}(K)\langle\sigma\rangle|_p > |\operatorname{Autcent}(K)|_p,$$

and the proof is complete. □

We need the following well-known result [51, Theorem 14.4.7].

Theorem 3.80 *A group G has a quotient isomorphic to a Sylow p-subgroup P of G if and only if for each subgroup Q of P an element of G of order coprime to p which normalizes Q also centralizes Q.*

Next we have the following

Proposition 3.81 *Let G be a finite group such that $|\operatorname{Aut}(G)|_p = |\operatorname{Autcent}(G)|_p$. If P is a Sylow p-subgroup of G, then $G \cong P \oplus Q$ for some subgroup Q of G.*

Proof First notice that $|\operatorname{Aut}(G)|_p = |\operatorname{Autcent}(G)|_p$ implies that every Sylow p-subgroup of $\operatorname{Autcent}(G)$ is also a Sylow p-subgroup of $\operatorname{Aut}(G)$. Since $\operatorname{Autcent}(G)$ is normal in $\operatorname{Aut}(G)$, by Sylow's Theorem, every Sylow p-subgroup of $\operatorname{Aut}(G)$ is contained in $\operatorname{Autcent}(G)$. For each $x \in P$, since the order of the inner automorphism ι_x is some power of p, it lies in $\operatorname{Autcent}(G)$. Hence, it follows that $[g, x] \in \mathrm{Z}(G)$ for all $g \in G$, and consequently $[G, P] \leq \mathrm{Z}(G)$.

Let H be any subgroup of P and $y \in \mathrm{N}_G(H)$ an element of order coprime to p, where $\mathrm{N}_G(H)$ is the normalizer of H in G. Let the order of the inner automorphism ι_y be n. Then n divides the order of y, and, since $[y, h] \in \mathrm{Z}(G)$, we get

$$h = \iota_y^n(h) = y^n h y^{-n} = [y^n, h]h = [y, h]^n h.$$

Since $[y, h] \in H$ and $(n, p) = 1$, we have $[y, h] = 1$, and hence $y \in \mathrm{C}_G(H)$. It follows from Theorem 3.80 that P has a normal complement Q. Since $[G, P] \leq \mathrm{Z}(G)$, it follows that $P\,\mathrm{Z}(G)$ is normal in G. Further, P, being the unique Sylow p-subgroup of $P\,\mathrm{Z}(G)$, is characteristic in $P\,\mathrm{Z}(G)$, hence P is normal in G. □

The following result is straightforward and we leave the proof to the reader.

Exercise 3.82 Let H and K be two abelian p-groups with $|H| = p^r$, $\exp(H) \leq p^s$ and $|K| = p^t$, where $t \leq s$. Then $|\operatorname{Hom}(H,\ K)| \geq p^l$, where $l = \frac{rt}{s}$.

The following technical result is the final preparation towards Hyde's theorem.

Lemma 3.83 *Let G be a purely non-abelian finite group such that $|G|_p \geq p^{\frac{h^2-h+2}{2}}$, where $h \geq 3$ and $|\mathrm{Z}(G) \cap \gamma_2(G)|_p = 1$. Then $|\operatorname{Aut}(G)|_p \geq p^h$.*

Proof If $|\operatorname{Inn}(G)|_p = |G/\mathrm{Z}(G)|_p \geq p^h$, then the result holds trivially. If $|G/\mathrm{Z}(G)|_p \leq p^{h-2}$, then by Theorem 3.11,

$$|\gamma_2(G)|_p \leq p^{\frac{h^2-3h+2}{2}}.$$

It follows that

$$|G/\gamma_2(G)|_p \geq p^h$$

and

$$|\mathrm{Z}(G)|_p \geq p^{\frac{h^2-3h+6}{2}} \geq p^h.$$

Therefore,

$$|\operatorname{Autcent}(G)|_p = |\operatorname{Hom}\big(G/\gamma_2(G),\ \mathrm{Z}(G)\big)|_p \geq \min\big\{|G/\gamma_2(G)|_p,\ |\mathrm{Z}(G)|_p\big\} \geq p^h$$

and the result holds.

Now, suppose that $|G/\mathrm{Z}(G)|_p = p^{h-1}$. Then using the fact that $|\gamma_2(G) \cap \mathrm{Z}(G)|_p = 1$, we get

$$|\gamma_2(G)|_p = |\gamma_2(G)/\big(\gamma_2(G) \cap \mathrm{Z}(G)\big)|_p \leq |G\gamma_2(G)/\mathrm{Z}(G)|_p = |G/\mathrm{Z}(G)|_p = p^{h-1}.$$

Consequently,

$$|G/\gamma_2(G)|_p \geq p^{h-1}.$$

Notice that $|\mathrm{Z}(G)|_p \geq p^{h-1}$, and therefore we get

$$|\operatorname{Autcent}(G)|_p \geq \min\big\{|G/\gamma_2(G)|_p,\ |\mathrm{Z}(G)|_p\big\} \geq p^{h-1}.$$

If $|\operatorname{Aut}(G)|_p > |\operatorname{Autcent}(G)|_p$, then we are done.

Suppose that $|\operatorname{Aut}(G)|_p = |\operatorname{Autcent}(G)|_p$. In this case, by Proposition 3.81, $G \cong P \oplus Q$, where P is a Sylow p-subgroup of G. Since G is purely non-abelian, P must be non-abelian. Now, by Theorem 1.32, there exists a non-inner automorphism of P of order a power of p. Clearly θ then extends to a non-inner automorphism of G, and hence $|\operatorname{Aut}(G)|_p \geq p^h$. □

We now present the main result of Hyde [68].

Theorem 3.84 *The integer-valued function f defined, on natural numbers $h \geq 3$, by setting*

$$f(h) = \begin{cases} 5 & if\, h = 3, \\ \frac{h^2-h+6}{2} & if\, h \geq 4 \end{cases}$$

has the property that for each $h \geq 3$ and each prime p, if G is any finite group such that $p^{f(h)}$ divides $|G|$, then p^h divides $|\operatorname{Aut}(G)|$.

Proof We divide the proof into the following two cases:

Case (1): We first show that $f(3) = 5$. If $|\operatorname{Inn}(G)|_p = |G/\operatorname{Z}(G)|_p \geq p^3$, then the result holds trivially. Suppose that $|G/\operatorname{Z}(G)|_p \leq p^2$. By Theorem 3.11, $|\gamma_2(G)|_p \leq p^3$ and $|G/\gamma_2(G)|_p \geq p^2$.

Subcase (1a): G is purely non-abelian. In this case, by Theorem 3.72, we have

$$\begin{aligned} |\operatorname{Aut}(G)|_p \geq |\operatorname{Autcent}(G)|_p &= \left|\operatorname{Hom}\left(G/\gamma_2(G), \operatorname{Z}(G)\right)\right|_p \\ &\geq \min\left\{|G/\gamma_2(G)|_p, |\operatorname{Z}(G)|_p\right\} \\ &\geq p^2. \end{aligned} \tag{3.85}$$

If $|\operatorname{Aut}(G)|_p > p^2$, then we are done. Otherwise,

$$|\operatorname{Aut}(G)|_p = |\operatorname{Autcent}(G)|_p = p^2,$$

and so, by Proposition 3.81, $G = P \oplus Q$, where P is a Sylow p-subgroup of G. Since G is purely non-abelian, $|P| \geq p^3$. It follows that $|\operatorname{Inn}(P)| \geq p^2$, and therefore by Theorem 1.32, $|\operatorname{Aut}(G)|_p \geq p^3$, which is absurd.

Subcase (1b): $G = H \oplus K$, where H is a non-trivial abelian group and K is a purely non-abelian group. If $|H|_p \geq p^i$ for $i = 2, 3, 4, 5$, then

$$|\operatorname{Aut}(G)|_p \geq |\operatorname{Aut}(H)|_p \geq p^{i-1}$$

by Theorem 3.77. Hence, the result holds for $i = 4, 5$. For $i = 2$, we have $|K|_p \geq p^3$. Hence, using (3.85), we get $|\operatorname{Aut}(K)|_p \geq p^2$. Consequently,

$$|\operatorname{Aut}(G)|_p \geq |\operatorname{Aut}(H)|_p\, |\operatorname{Aut}(K)|_p \geq p^3.$$

The case $i = 3$ is similar. If $|H|_p = 1$, then

$$|G|_p = |K|_p \geq p^5,$$

and the result follows from Subcase (1a). Finally, if $|H|_p = p$, then $|K|_p \geq p^4$. Hence, using (3.85), we obtain $|\operatorname{Aut}(K)|_p \geq p^2$.

Now, if $|\operatorname{Z}(K) \cap \gamma_2(K)|$ is divisible by p, then by Proposition 3.79, we have

$$|\operatorname{Aut}(G)|_p > |\operatorname{Aut}(K)|_p,$$

and the result follows. In case $|\operatorname{Z}(K) \cap \gamma_2(K)|_p = 1$, by Lemma 3.83, we have $|\operatorname{Aut}(K)|_p \geq p^3$, and again the result follows.

Case (2): $h \geq 4$. If $|\operatorname{Inn}(G)|_p = |G/\operatorname{Z}(G)|_p \geq p^h$, then the result holds trivially. Assume that $|G/\operatorname{Z}(G)|_p \leq p^{h-1}$. By Theorem 3.11,

$$|\gamma_2(G)|_p \leq p^{\frac{h^2-h}{2}}.$$

It follows that

$$|G/\gamma_2(G)|_p \geq p^3$$

and

$$|\operatorname{Z}(G)|_p \geq p^{\frac{h^2-3h+8}{2}}.$$

Let $|G/\gamma_2(G)|_p = p^t$, where $t \geq 3$. Then, by Corollary 3.8,

$$\exp\big(\operatorname{Z}(G)\big)_p \leq |G/\operatorname{Z}(G)|_p \exp\big(G/\gamma_2(G)\big)_p \leq p^{h-1}\,|G/\gamma_2(G)|_p = p^{h-1+t}.$$

Now, there are two subcases:

Subcase (2a): G is purely non-abelian. If $t \geq h$, then

$$|\operatorname{Autcent}(G)|_p = |\operatorname{Hom}\big(G/\gamma_2(G),\ \operatorname{Z}(G)\big)|_p \geq \min\big\{|G/\gamma_2(G)|_p, |\operatorname{Z}(G)|_p\big\} \geq p^h,$$

and we are done. Assume that $t \leq h-1$. Then, by Exercise 3.82, we get

$$|\operatorname{Hom}\big(G/\gamma_2(G),\ \operatorname{Z}(G)\big)|_p \geq p^C,$$

where $C = \frac{(h^2-3h+8)t}{2(h-1+t)}$. We claim that $C \geq h-1$, or equivalently

$$(t-2)h^2 + (4-5t)h + 10t - 2 \geq 0.$$

Notice that the discriminant of the quadratic polynomial $(t-2)h^2 + (4-5t)h + 10t - 2$ is negative for $t \geq 4$. Thus, the claim is true for $t \geq 4$. Also, for the case $t = 3$, it can be seen that $h^2 - 11h + 28 \geq 0$ for $h = 4$ and $h \geq 7$. Thus, the remaining cases are $t = 3$ and $h = 5, 6$.

If $h = 5$, then $|\operatorname{Z}(G)|_p \geq p^9$ and by Corollary 3.8,

$$\exp\big(\operatorname{Z}(G)\big)_p \leq p^4 p^3 = p^7.$$

Now it follows that

$$|\operatorname{Hom}\big(G/\gamma_2(G),\ \operatorname{Z}(G)\big)|_p \geq |\operatorname{Hom}(\mathrm{C}_{p^3},\ \mathrm{C}_{p^7} \oplus \mathrm{C}_{p^2})| \geq p^4.$$

If $h = 6$, then $|\operatorname{Z}(G)|_p \geq p^{13}$ and by Corollary 3.8,

$$\exp\big(\mathrm{Z}(G)\big)_p \leq p^5 p^3 = p^8.$$

Again, it is easy to see that

$$|\operatorname{Hom}\big(G/\gamma_2(G),\ \mathrm{Z}(G)\big)|_p \geq |\operatorname{Hom}(\mathrm{C}_{p^3},\ \mathrm{C}_{p^8} \oplus \mathrm{C}_{p^5})| \geq p^5.$$

Thus, we have proved that

$$|\operatorname{Autcent}(G)|_p = |\operatorname{Hom}\big(G/\gamma_2(G),\ \mathrm{Z}(G)\big)|_p \geq p^{h-1}.$$

If $|\operatorname{Aut}(G)|_p > |\operatorname{Autcent}(G)|_p$, then the result holds. Suppose that $|\operatorname{Aut}(G)|_p = |\operatorname{Autcent}(G)|_p$. In this case, by Proposition 3.81,

$$G = P \oplus Q,$$

where P is a Sylow p-subgroup of G. Since G is purely non-abelian, P must be non-abelian. By Theorem 1.32, there exists a non-inner automorphism of P of order a power of p, which extends to a non-inner automorphism of G and gives $|\operatorname{Aut}(G)|_p \geq p^h$.

Subcase (2b): $G = H \oplus K$, where H is a non-trivial abelian group and K is a purely non-abelian group. Let $|H|_p = p^r$ for some $r \geq 1$. If $r \geq h+1$, then by Theorem 3.35, $|\operatorname{Aut}(H)|_p \geq p^h$ and the result holds.

If $2 \leq r \leq h$, then $\frac{h^2-h+6}{2} - r \geq \frac{(h-r+1)^2-(h-r+1)+6}{2}$, which in turn gives

$$|K|_p \geq p^{\frac{h^2-h+6}{2}-r} \geq p^{\frac{(h-r+1)^2-(h-r+1)+6}{2}}.$$

Since K is purely non-abelian, the previous case gives $|\operatorname{Aut}(K)|_p \geq p^{h-r+1}$, which together with Theorem 3.35 yields

$$|\operatorname{Aut}(G)|_p \geq |\operatorname{Aut}(H)|_p |\operatorname{Aut}(K)|_p \geq p^{r-1} p^{h-r+1} = p^h.$$

If $r = 1$, then $|K|_p \geq p^{\frac{h^2-h+6}{2}-1} = p^{\frac{h^2-h+4}{2}}$. Since $h \geq 4$, we get

$$\frac{h^2-h+4}{2} \geq \frac{(h-1)^2-(h-1)+6}{2}.$$

Consequently, we obtain $|\operatorname{Aut}(K)|_p \geq p^{h-1}$. If $|\mathrm{Z}(K) \cap \gamma_2(K)|$ is divisible by p, then by Proposition 3.79, we have $|\operatorname{Aut}(G)|_p > |\operatorname{Aut}(K)|_p$ and the result follows. If $|\mathrm{Z}(K) \cap \gamma_2(K)|_p = 1$, then by Lemma 3.83, we have $|\operatorname{Aut}(K)|_p \geq p^h$, which finally completes the proof. □

It is natural to ask whether the function f can be bounded from below. Hyde [68] provided an answer to this question using the following example, which, in particular, shows that $f(3) = 5$ *is the best possible bound for* $h = 3$.

Example 3.86 It is well known that if a and d are coprime integers, then the arithmetic progression $\{a + nd \mid n = 0, 1, 2, \dots\}$ contains an infinite number of primes [5, p. 154, Theorem 7.9]. Let p be an odd prime, $a = 1 + p^h$ and $d = p^{h+1}$. Then a and d are coprime and $q = 1 + p^h + kp^{h+1}$ is a prime for some k. If $G = \mathrm{GL}(2, \mathbb{F}_q)$, then $|G| = (q + 1)q(q - 1)^2$ and $|G|_p = p^{2h}$. Notice that $|\operatorname{Z}(G)| = q - 1$, and hence $|\operatorname{Inn}(G)| = (q + 1)q(q - 1)$. Further, since q is prime, we have $|\operatorname{Aut}(G)| = 2\,|\operatorname{Inn}(G)|$, which gives $|\operatorname{Aut}(G)|_p = p^h$.

Replacing h by $h - 1$ in the preceding example shows that the function $f(h) = 2h - 2$ does not work. Hence, the least function $f(h)$ such that $|\operatorname{Aut}(G)|_p \geq p^h$ whenever $|G|_p \geq p^{f(h)}$ satisfies $f(h) \geq 2h - 1$. We thus have the following result.

Theorem 3.87 *Let $h \geq 2$. The least function $f(h)$ such that $|\operatorname{Aut}(G)|_p \geq p^h$ whenever $|G|_p \geq p^{f(h)}$ satisfies $f(h) \geq 2h - 1$.*

The following problem remains open.

Problem 3.88 Does there exist a linear polynomial function $f : \mathbb{N} \to \mathbb{N}$ with the property that, for each prime p, if G is a finite group with $|G|_p \geq p^{f(h)}$, then $|\operatorname{Aut}(G)|_p \geq p^h$?

Exarchakaos [29] and Burmester-Exarchakos [15] further attempted to improve the functional bound in the class of p-groups, which we state here without proof. The papers are intricate case-by-case analysis of various numerical invariants of subgroups of the groups under consideration. First we state the main result of [29].

Theorem 3.89 *The function $f : \mathbb{N} \to \mathbb{N}$ defined by*

$$f(h) = \begin{cases} h & if\ h \leq 5, \\ 2h - 5 & if\ 6 \leq h \leq 8, \\ 14 & if\ h = 9, \\ 17 & if\ h = 10, \\ 20 & if\ h = 11, \\ 23 & if\ h = 12, \\ \frac{h^2}{6} & if\ h \geq 13 \end{cases}$$

satisfies the property that if G is a finite p-group with $|G| \geq p^{f(h)}$, then $|\operatorname{Aut}(G)|_p \geq p^h$.

The preceding bound was improved in [15] to the following

Theorem 3.90 *The function $f : \mathbb{N} \to \mathbb{N}$ defined by*

$$f(h) = \begin{cases} h & if\ h \leq 6, \\ 3h - 13 & if\ 7 \leq h \leq 12, \\ 5h - 39 & if\ 13 \leq h \leq 22, \\ 7h - 81 & if\ 23 \leq h \leq 31, \\ 9h - 142 & if\ 32 \leq h \leq 41, \\ \frac{h^2}{7} & if\ h \geq 42 \end{cases}$$

satisfies the property that if G is a finite p-group with $|G| \geq p^{f(h)}$, then $|\operatorname{Aut}(G)|_p \geq p^h$.

Exarchakos–Dimakos–Baralis in [31, 32] claimed to have improved the functional bound to a linear polynomial function. Unfortunately, the following key lemma [32, Lemma 2], on which the proof depends heavily, does not work and there are counterexamples to this lemma.

Lemma 3.91 *Let G be a non-abelian p-group of order p^n and nilpotency class c. Let $|G/\gamma_2(G)| = p^m$, $|\mathrm{Z}(G)| = p^k$ and $m_1 \geq m_2 \geq \cdots \geq m_t \geq 1$, $k_1 \geq k_2 \geq \cdots \geq k_s \geq 1$ be the invariants of $G/\gamma_2(G)$ and $\mathrm{Z}(G)$, respectively. Then the following statements hold:*

(1) $\exp\big(\mathrm{Z}_{i+1}(G)/\mathrm{Z}_i(G)\big) = \exp\big(\mathrm{Z}(G)\big) = p^{k_1}$ *for all* $i = 0, 1, \ldots, c-1$;
(2) $\exp\big(\gamma_i(G)/\gamma_{i+1}(G)\big) = \exp\big(\mathrm{Z}(G)\big) = p^{k_1}$ *for all* $i = 1, 2, \ldots, c-1$ *and* $m_2 \geq k_1$;
(3) $\exp\big(\mathrm{Z}_{c-i}(G)/\gamma_i(G)\big) \leq p^{k_1}$ *for all* $i = 1, 2, \ldots, c-1$;
(4) $|G/\mathrm{Z}_2(G)| \geq p^{k_1 c - 2k_1 + 2}$.

For an odd prime p, the preceding lemma does not hold for the group

$$G = \langle x, y, u \mid x^{p^2} = y^{p^2} = u^{p^2} = 1, [x, y] = u, [u, x] = u^p, [u, y] = 1 \rangle.$$

It is not difficult to show that G is generated by two elements, has order p^6 and is of nilpotency class 3. Further, $\gamma_2(G)$ and $\mathrm{Z}(G)$ are distinct cyclic subgroups of order p^2 and $\gamma_3(G)$ is of order p. Being cyclic, $\exp\big(\mathrm{Z}(G)\big) = p^2$. Obviously

$$\exp\big(\gamma_2(G)/\gamma_3(G)\big) = p \neq \exp\big(\mathrm{Z}(G)\big),$$

which contradicts Lemma 3.91(2).

We remark that Problem 3.88 is open for the class of finite p-groups.

Chapter 4
Groups with Divisibility Property-I

Every finite non-cyclic abelian p-group of order greater than p^2 has the property that its order divides that of its group of automorphisms (Theorem 3.34). The problem whether every non-abelian p-group of order greater than p^2 possesses the same property has been a subject of intensive investigation. As discussed in the introduction, this property is referred to as the *Divisibility Property*. While several classes of p-groups have been shown to have Divisibility Property, it is now known that not all finite p-groups admit this property [46]. An exposition of these developments is presented in the remaining part of this monograph.

In this chapter, some reduction results, due to Buckley [14], are presented in Sect. 4.1. Among other results, it is proved that one can confine attention to the class of purely non-abelian p-groups. In subsequent sections it is shown that Divisibility Property is satisfied by p-groups of nilpotency class 2 [33], p-groups with metacyclic central quotient [18], modular p-group [22], p-abelian p-groups [19], and groups with small central quotient [20].

In view of Theorem 3.34, it can be assumed that the groups under consideration are non-abelian p-groups. The main ingredient in verifying Divisibility Property for various classes of groups G is the subgroup

$$\mathrm{IC}(G) := \mathrm{Inn}(G)\,\mathrm{Autcent}(G)$$

of the automorphism group $\mathrm{Aut}(G)$ of G.

4.1 Reduction Results

This section is devoted to some reduction arguments which enable verification of Divisibility Property for finite p-groups with certain conditions. In what follows, most of the results are due to Buckley [14].

Recall that a group G is an *internal central product* of two subgroups N and S if $G = NS$, $[N, S] = 1$ and $N \cap S \leq \mathrm{Z}(G)$.

The following result is an interesting application of extension theory for central products and Wells exact sequence.

I. B. S. Passi et al., *Automorphisms of Finite Groups*, Springer Monographs in Mathematics, https://doi.org/10.1007/978-981-13-2895-4_4

Theorem 4.1 *Let G be a finite p-group which is a central product of non-trivial subgroups N and S. Suppose that $N < G$, $S \leq G$ and $N \cap \gamma_2(S) = 1$. Then*

$$|\operatorname{Aut}_N(G)|_p \geq p\,|\operatorname{Aut}(N)|_p\,|\operatorname{Aut}(G/N)|_p.$$

Proof Let $H = G/N$ and $\mathcal{E}$ be the extension

$$1 \to N \to G \to H \to 1.$$

Then, by Theorem 2.63, we have the following exact sequence

$$1 \to \operatorname{Hom}\big(H,\ \mathrm{Z}(N)\big) \longrightarrow \operatorname{Aut}_N(G) \xrightarrow{\rho(\mathcal{E})} \operatorname{Aut}(H) \times \operatorname{Aut}(N).$$

Consequently, Ker $\big(\rho(\mathcal{E})\big)$ is isomorphic to Hom $\big(H,\ \mathrm{Z}(N)\big)$. It follows that

$$|\operatorname{Ker}\big(\rho(\mathcal{E})\big)| = |\operatorname{Hom}\big(H,\ \mathrm{Z}(N)\big)| = |\operatorname{Hom}\big(H/\gamma_2(H),\ \mathrm{Z}(N)\big)| = p^m$$

for some $m \geq 1$. Recall that $\mathcal{S}(H,\ N)$ denotes the set of equivalence classes of special quasi-central extensions of H by N (see Sect. 2.8 of Chap. 2). In view of Remark 2.62 and the fact that both $H/\gamma_2(H)$ and $\mathrm{Z}(N)$ are finite abelian groups, we have

$$|\mathcal{S}(H, N)| = |\operatorname{Ext}\big(H/\gamma_2(H), \mathrm{Z}(N)\big)| = |\operatorname{Hom}\big(H/\gamma_2(H),\ \mathrm{Z}(N)\big)| = p^m.$$

If $\mathcal{E}$ is a split extension, then the map $\rho(\mathcal{E})$ is surjective. Again, by Theorem 2.63, we have

$$|\operatorname{Aut}_N(G)| = p^m\ |\operatorname{Aut}(N)|\,|\operatorname{Aut}(G/N)|,$$

and the result follows in this case.

Now, suppose that $\mathcal{E}$ is a non-split extension. In view of Theorem 2.61, $\mathcal{E}$ is a special quasi-central extension, and hence $[\mathcal{E}]$ is an element of $\mathcal{S}(H, N)$. Further, notice that $\mathcal{S}(H, N)$ is invariant under the action of $\operatorname{Aut}(H) \times \operatorname{Aut}(N)$ on $\operatorname{Ext}_\alpha(H, N)$, where α is the trivial coupling. Since this action of $\operatorname{Aut}(H) \times \operatorname{Aut}(N)$ on $\mathcal{S}(H, N)$ permutes non-split extensions, we can consider this as an action on the set of all non-split extensions in $\mathcal{S}(H, N)$, which is a set with $p^m - 1$ elements. Let L be the stabilizer subgroup of $\operatorname{Aut}(H) \times \operatorname{Aut}(N)$ at $[\mathcal{E}]$. Then

$$\frac{|\operatorname{Aut}(H) \times \operatorname{Aut}(N)|}{|L|} \leq p^m - 1,$$

which implies that

$$\frac{|\operatorname{Aut}(H) \times \operatorname{Aut}(N)|_p}{|L|_p} \leq p^{m-1}$$

or equivalently

$$|L|_p \geq \frac{|\operatorname{Aut}(H)|_p \ |\operatorname{Aut}(N)|_p}{p^{m-1}}.$$

Therefore, by Theorem 2.63, we obtain

$$|\operatorname{Aut}_N(G)|_p = |\operatorname{Ker}\big(\rho(\mathcal{E})\big)|_p \ |L|_p = p^m \ |L|_p \geq p \ |\operatorname{Aut}(G/N)|_p \ |\operatorname{Aut}(N)|_p,$$

and the proof is complete. □

The preceding theorem leads to the following reductions on groups with Divisibility Property.

Theorem 4.2 *Let G be a finite p-group and $1 < N \trianglelefteq G$ such that $N \cap \gamma_2(G) = 1$. Then the following statements hold:*

(1) $|\operatorname{Aut}_N(G)|_p \geq p\,|\operatorname{Aut}(N)|_p\,|\operatorname{Aut}(G/N)|_p$.
(2) If $|G/N|$ *divides* $|\operatorname{Aut}(G/N)|$, *then* $|G|$ *divides* $|\operatorname{Aut}_N(G)|$.

In particular, if both N and G/N have Divisibility Property, then so does G.

Proof Since $N \cap \gamma_2(G) = 1$, N is a central subgroup. Therefore, G can be viewed as a central product of N and G, and assertion (1) follows from Theorem 4.1.

If N is a non-cyclic abelian p-group of order greater than p^2, then $|N|$ divides $|\operatorname{Aut}(N)|$ by Theorem 3.34. If N is cyclic, then, obviously, $|N|$ divides $p\,|\operatorname{Aut}(N)|$. The assertion (2) then follows from (1). □

Remark 4.3 In view of the preceding theorem, for studying Divisibility Property, it is enough to consider finite p-groups G such that $\Omega_1\big(\mathrm{Z}(G)\big) \leq \gamma_2(G)$. For, if $\Omega_1\big(\mathrm{Z}(G)\big) \nleq \gamma_2(G)$, then we can always find a non-trivial normal subgroup $N \leq \mathrm{Z}(G)$ such that $N \cap \gamma_2(G) = 1$, and $\Omega_1\big(\mathrm{Z}(G/N)\big) \leq \gamma_2(G/N)$.

We now present the main result of Hummel [65].

Theorem 4.4 *Let G be a finite p-group which is a central product of non-trivial subgroups N and A with A abelian. If* $|N|$ *divides* $|\operatorname{Aut}(N)|$, *then* $|G|$ *divides* $|\operatorname{Aut}(G)|$.

Proof Since A is abelian, $N \cap \gamma_2(A) = 1$, and therefore,

$$|\operatorname{Aut}_N(G)|_p \geq p\ |\operatorname{Aut}(N)|_p\ |\operatorname{Aut}(G/N)|_p$$

by Theorem 4.1. If G/N is an abelian p-group of order p^r for some r, then $|\operatorname{Aut}(G/N)|_p \geq p^{r-1}$ by Theorem 3.35, and the proof follows. □

Remark 4.5 In view of Theorem 4.4, for studying Divisibility Property, it is enough to consider finite p-groups G with $\mathrm{Z}(G) \leq \Phi(G)$.

The following result of Otto [98, Theorem 1] is a special case of Theorem 4.4.

Theorem 4.6 *Let $G = A \times N$ be a finite p-group with A abelian and N purely non-abelian. Then*

$$|\operatorname{Aut}(G)|_p \geq |A|\,|\operatorname{Aut}(N)|_p.$$

Consequently, if $|\operatorname{Aut}(N)|_p \geq |N|$, then $|\operatorname{Aut}(G)|_p \geq |G|$.

Remark 4.7 In view of Theorem 4.6, for studying Divisibility Property, it is further enough to consider only purely non-abelian finite p-groups.

Next, we define the notion of isoclinism originally introduced by Hall [53]. Two groups G and H are said to be *isoclinic* if there exist isomorphisms

$$\alpha : G/\mathrm{Z}(G) \to H/\mathrm{Z}(H)$$

and

$$\beta : \gamma_2(G) \to \gamma_2(H)$$

such that the following diagram commutes

$$\begin{tikzcd}
G/\mathrm{Z}(G) \times G/\mathrm{Z}(G) \arrow[r] \arrow[d, "(\alpha,\alpha)"] & \gamma_2(G) \arrow[d, "\beta"] \\
H/\mathrm{Z}(H) \times H/\mathrm{Z}(H) \arrow[r] & \gamma_2(H),
\end{tikzcd}$$

where the horizontal maps are the commutator maps given by

$$\big(\mathrm{Z}(G)x, \mathrm{Z}(G)y\big) \mapsto [x, y].$$

It can be easily checked that isoclinism is an equivalence relation on the class of all groups. The following observations, due to Hall [53], allow us to state Theorems 4.1 and 4.2 in terms of isoclinism.

Proposition 4.8 *Let G be a group. Then the following statements hold:*

(1) If $N \leq G$, then G and N are isoclinic if and only if $G = N\,\mathrm{Z}(G)$.
(2) If $N \trianglelefteq G$, then G and G/N are isoclinic if and only if $N \cap \gamma_2(G) = 1$.
(3) If $G = N \times A$ with A abelian, then G and N are isoclinic.

We conclude this section with the following result of Weichsel [124], which is of independent interest, and states that given two isoclinic groups, we can always obtain one from the other via a sequence of three groups involving steps (1)–(3) of Proposition 4.8.

Theorem 4.9 *Let G and H be two groups. Then G and H are isoclinic if and only if there exists an abelian group A and groups $N \trianglelefteq R$ such that $R \leq G \times A$ with $R\,\mathrm{Z}(G \times A) = G \times A$, and $H = R/N$ with $N \cap \gamma_2(R) = 1$.*

Proof The sufficiency part of the statement follows from Proposition 4.8. Assume that G are H are isoclinic. Consider the subgroup

$$C = \big\{(g,h) \mid \alpha(\mathrm{Z}(G)g) = \mathrm{Z}(H)h\big\}$$

of $G \times H$. Set

$$Z_1 = C \cap \big(1 \times H\big) = 1 \times \mathrm{Z}(H)$$

and

$$Z_2 = C \cap \big(G \times 1\big) = \mathrm{Z}(G) \times 1.$$

Observe that $\gamma_2(C) = \big\langle\big([g_1, g_2], \beta([g_1, g_2])\big) \mid g_1, g_2 \in G\big\rangle$. It follows that

$$\gamma_2(C) \cap Z_1 = 1 = \gamma_2(C) \cap Z_2.$$

Also, one can see that $C/Z_1 \cong G$ and $C/Z_2 \cong H$. Now, consider the subgroup

$$\overline{C} = \big\{\big(Z_1c, \gamma_2(C)c\big) \mid c \in C\big\}$$

of $C/Z_1 \times C/\gamma_2(C)$, which is easily seen to be isomorphic to C. Notice that

$$\overline{C}\,\mathrm{Z}\big(C/Z_1 \times C/\gamma_2(C)\big) = C/Z_1 \times C/\gamma_2(C),$$

which implies that C can be viewed as a subgroup of $G \times C/\gamma_2(C)$. Taking $A = C/\gamma_2(C)$, $R = C$ and $N = Z_2$ completes the proof of the theorem. □

4.2 Groups of Nilpotency Class 2

In this section, we present a result of Faudree [33] showing that p-groups of nilpotency class 2 have Divisibility Property. We begin with the following useful result which is of independent interest, and is a slight generalization of [33, Lemma 1] and [67, Lemma].

Lemma 4.10 *Let G be a finite p-group and K a normal subgroup of G such that $G/K = \langle Kx\rangle$ is a cyclic group of order p^n. Suppose that there exists an element $z \in \mathrm{C}_G(K)$ such that $(zx)^{p^n} = x^{p^n}$ and $G = \langle K, zx\rangle$. Then the map $\phi : G \to G$ given by*

$$\phi(kx^i) = k(zx)^i$$

for $1 \le i < p^n$ is an element of $\mathrm{Aut}^K(G)$. Moreover, if $z \in \mathrm{Z}(K)$, then the order of ϕ equals the order of z.

Proof Since $(zx)^{p^n} = x^{p^n}$, it follows that the map ϕ is well-defined. Using the fact that $z \in \mathrm{C}_G(K)$, a routine computation shows that ϕ is an endomorphism of G.

That $\phi \in \mathrm{Aut}^K(G)$ follows from the fact that ϕ maps a generating set of G onto a generating set of G, and the very definition. □

We need the following well-known result [66, III.3.18 Satz].

Theorem 4.11 *Let G be a finite p-group. Then $\mathrm{Aut}^{G/\Phi(G)}(G)$ is a p-group.*

Let G be a purely non-abelian finite p-group of nilpotency class 2. Let $X = \{x_1, x_2, \ldots, x_d\}$ be a minimal generating set for G such that

$$G/\gamma_2(G) = \langle \bar{x}_1 \rangle \oplus \cdots \oplus \langle \bar{x}_d \rangle,$$

where $\bar{x}_i = \gamma_2(G)x_i$. Let p^{α_i} and p^{β_i} denote the orders of x_i modulo $\gamma_2(G)$ and $\mathrm{Z}(G)$ respectively for $1 \le i \le d$ such that $\alpha_1 \ge \cdots \ge \alpha_d$. Without loss of generality, we can assume that

$$\gamma_2(G) = \langle w_1 \rangle \oplus \cdots \oplus \langle w_n \rangle,$$

where $w_1 = [x_1, x_2]$, $|w_i| = p^{m_i}$ and $m_1 \ge \cdots \ge m_n$. Since $\exp\big(G/\mathrm{Z}(G)\big) = \exp\big(\gamma_2(G)\big)$, we have $\alpha_1 \ge \alpha_2 \ge m_1$.

Let k be the largest positive integer such that $\alpha_k > m_1$. Fix an integer i such that $1 \le i \le k$. For each $0 \le j < (\alpha_i - m_1)$, define a map

$$f : \{x_1, \ldots, x_d\} \to G$$

by setting

$$f(x_l) = \begin{cases} x_i x_i^{p^{j+m_1}} & \text{if } l = i, \\ x_l & \text{if } 1 \le l \le d \text{ and } l \ne i. \end{cases}$$

Then, by Lemma 4.10, f extends to an automorphism of G. It is easy to see that $x_i^{-1} f(x_i) \in \mathrm{Z}(G) \setminus \gamma_2(G)$ for $1 \le i \le k$. Let R_1 denote the subgroup of $\mathrm{Autcent}(G)$ generated by the set of all such automorphisms f.

Notice that each $\phi \in \mathrm{Hom}\big(G/\gamma_2(G),\ \gamma_2(G)\big)$ defines an automorphism, say f_ϕ, of G given by

$$f_\phi(g) = g\phi(g)$$

for $g \in G$. Let R_2 denote the subgroup of $\mathrm{Autcent}(G)$ corresponding to the group of homomorphisms $\mathrm{Hom}\big(G/\gamma_2(G),\ \gamma_2(G)\big)$. Then, by Theorem 3.72 or Theorem 4.11, it follows that R_1R_2 is a p-group of order

$$|R_1R_2| \ge p^{\left(\sum_{i=1}^{d} \alpha_i\right) + m_2 + \left(\sum_{i=2}^{n} m_i\right)}.$$

With the above set-up, we thus have the following result.

Proposition 4.12 *Let G be a purely non-abelian finite p-group of nilpotency class 2. Then*

$$|\,\mathrm{Autcent}(G)| \ge p^{\left(\sum_{i=1}^{d} \alpha_i\right) + m_2 + \left(\sum_{i=2}^{n} m_i\right)}.$$

In view of Proposition 4.12, we only need to produce $p^{m_1-m_2}$ more automorphisms to conclude that $|\operatorname{Aut}(G)|_p \geq |G|$. If $m_1 = m_2$, then we are done.

From now onwards, for the rest of this section, we assume that $m_1 > m_2$. Continuing with the above settings, assume further that

$$x_1^{p^{\alpha_1}} \equiv w_1^{p^{t_1}} \mod \langle w_2, \dots, w_n \rangle$$

and

$$x_2^{p^{\alpha_2}} \equiv w_1^{p^{t_2}} \mod \langle w_2, \dots, w_n \rangle$$

for some non-negative integers t_1, t_2. Now define maps

$$\sigma_1, \sigma_2 : \{x_1, \dots, x_d\} \to G$$

by setting

$$\sigma_1(x_l) = \begin{cases} x_2^{p^{m_1}} x_1 & \text{if } l = 1, \\ x_l & \text{if } l \neq 1, \end{cases}$$

and

$$\sigma_2(x_l) = \begin{cases} x_2 x_1^{p^{\kappa}} & \text{if } l = 2, \\ x_l & \text{if } l \neq 2, \end{cases}$$

where $\kappa = \max\{m_1, \alpha_1 + m_1 - \alpha_2 - t_1, \alpha_1 + m_2 - \alpha_2\}$. Using Lemma 4.10 and Theorem 4.11, we can prove the following:

Exercise 4.13 The maps σ_1, σ_2 extend to central automorphisms of G, and are of orders $p^{\alpha_2 - m_1}$ and $p^{\min\{\alpha_1 - m_1, \alpha_2 + t_1 - m_1, \alpha_2 - m_2\}}$ modulo $R_1 R_2$, respectively.

The following result is a slight generalization of [3, Lemma 1], which is valid in our situation since $m_1 > m_2$.

Lemma 4.14 *Let G be a finite p-group of nilpotency class 2 such that*

(1) $\gamma_2(G) = \langle w \rangle \oplus U$, *where* $|w| = p^{m_1} > p^{m'} \geq \exp(U)$*;*
(2) $w = [x_1, x_2]$ *and* $x_2^{p^{m_1+m''}} = 1$*;*
(3) $m'' = m'$ *if p is odd, and* $m'' = \max\{1, m'\}$ *if* $p = 2$.

Let $H = \langle x_1, x_2 \rangle$ *and* $L = \{x \in G \mid [x_1, x], [x_2, x] \in U\}$. *Then* $G = HL$ *and the map* $\sigma : G \to G$ *given by*

$$\sigma(g) = \begin{cases} x_1 x_2^{p^{m''}} & \textit{if } g = x_1, \\ g & \textit{if } g = x_2, \\ g & \textit{if } g \in L \end{cases}$$

extends to an automorphism of G centralising $Z(G)$*. Furthermore, σ has order* $p^{m_1 - m''}$ *modulo* $\operatorname{Autcent}(G)$.

Proof We first show that $G = HL$. For $g \in G$, we have

$$[x_1, g] \equiv w^s \mod U$$

and

$$[x_2, g] \equiv w^t \mod U,$$

which in turn gives

$$[x_1, x_2^{-s} x_1^t g] \equiv 1 \mod U$$

and

$$[x_2, x_2^{-s} x_1^t g] \equiv 1 \mod U.$$

By definition, $x_2^{-s} x_1^t g \in L$, and hence $g \in HL$. Thus, $G = HL$ and every element $g \in G$ can be uniquely written as

$$g = x_1^s x_2^t l,$$

where $0 \leq s < p^{m_1}$ and $l \in L$, since $\gamma_2(G) \leq \mathrm{Z}(G) \leq L$.

Showing that σ is an automorphism is a routine check using basic commutator identities in groups of nilpotency class 2, and hence left to the reader. Notice that $x_1^{p^{m_1}} \in \mathrm{Z}(G)$. Thus, to show that σ centralizes $\mathrm{Z}(G)$, it suffices to show that

$$\sigma(x_1^{p^{m_1}}) = x_1^{p^{m_1}}.$$

Observe that

$$\begin{aligned}\sigma(x_1^{p^{m_1}}) &= (x_1 x_2^{p^{m''}})^{p^{m_1}} \\ &= x_1^{p^{m_1}} x_2^{p^{m_1+m''}} [x_2, x_1]^{\frac{p^{m_1+m''}(p^{m_1}-1)}{2}} \\ &= x_1^{p^{m_1}} [x_2, x_1]^{\frac{p^{m_1+m''}(p^{m_1}-1)}{2}}.\end{aligned}$$

If p is odd, then

$$[x_2, x_1]^{\frac{p^{m_1+m''}(p^{m_1}-1)}{2}} = 1,$$

and hence

$$\sigma(x_1^{p^{m_1}}) = x_1^{p^{m_1}}.$$

Finally, if $p = 2$, then

$$[x_2, x_1]^{\frac{2^{m_1+m''}(2^{m_1}-1)}{2}} = 1$$

if and only if $m'' = \max\{1, m'\}$. By the very construction, the order of σ modulo $\mathrm{Autcent}(G)$ is $p^{m_1 - m''}$, and the proof is complete. □

Remark 4.15 For odd primes p, the preceding lemma is originally due to Adney-Yen [3, p. 138, Lemma 1], wherein they construct an automorphism as above for each $m > k \geq m'$. The case of $p = 2$ was considered by Faudree [33, Lemma 2].

Define $\eta : \mathbb{Z} \to \mathbb{N}$ by setting

$$\eta(n) = \begin{cases} 0 & \text{if } n \leq 0, \\ n & \text{if } n > 0. \end{cases}$$

Set

$$N_1 = \begin{cases} \min\left\{\eta(m_1 + t_2 - \alpha_2),\ \eta(2m_1 - \alpha_2 - m_2)\right\} & \text{if } p \text{ odd}, \\ \min\left\{\eta(m_1 + t_2 - \alpha_2),\ \eta(2m_1 - \alpha_2 - m_2),\ m_1 - 1\right\} & \text{if } p = 2, \end{cases}$$

and

$$N_2 = \begin{cases} \min\left\{\eta(m_1 + t_1 - \alpha_1),\ \eta(2m_1 - \alpha_1 - m_2)\right\} & \text{if } p \text{ odd}, \\ \min\left\{\eta(m_1 + t_1 - \alpha_1),\ \eta(2m_1 - \alpha_1 - m_2),\ m_1 - 1\right\} & \text{if } p = 2. \end{cases}$$

With the above set-up, using Theorem 4.11 and Lemma 4.14, we have

Exercise 4.16 The maps defined by

$$\tau_1(g) = \begin{cases} x_1 x_2^{p^{m''}} & \text{if } g = x_1, \\ g & \text{if } g = x_2, \\ g & \text{if } g \in L, \end{cases}$$

and

$$\tau_2(g) = \begin{cases} g & \text{if } g = x_1, \\ x_1 x_2^{p^{m''}} & \text{if } g = x_2, \\ g & \text{if } g \in L \end{cases}$$

extend to automorphisms of G of orders p^{N_1} and p^{N_2} modulo $\mathrm{Autcent}(G)$, respectively.

We are now in a position to prove the following result of Faudree [33] proof of which makes use of the automorphisms $\sigma_1, \sigma_2, \tau_1, \tau_2$ defined in the preceding discussion.

Theorem 4.17 *Let G be a finite p-group of nilpotency class 2. Then $|G|$ divides $|\operatorname{Aut}(G)|$.*

Proof In view of Remark 4.7, we can assume without loss of generality that G is purely non-abelian. We consider the following three cases:

Case (1): $t_2 = t_1 + r$ for some integer $r \geq 0$;
Case (2): $t_1 = t_2 + r$ for some integer $r \geq (\alpha_1 - \alpha_2)$;
Case (3): $t_1 = t_2 + r$ for some integer $0 < r < (\alpha_1 - \alpha_2)$.

In Case (1), we replace x_2 by $x_1^{-p^{\alpha_1-\alpha_2+r}} x_2$. Then it follows that $t_2 = m_1$ except the case when $p = 2, \alpha_1 = \alpha_2 = m_1$ and $r = 0$; and in this exceptional case $t_2 = m_1 - 1$.

In Case (2), we replace x_1 by $x_2^{-p^{r-\alpha_1+\alpha_2}} x_1$. Then $t_1 = m_1$ except the case when $p = 2$, $\alpha_1 = \alpha_2 = m_1$ and $r = 0$. Again, in this exceptional case $t_1 = m_1 - 1$.

Finally, in Case (3), we replace x_2 by $x_2 x_1^{-p^{\alpha_1-\alpha_2-r}}$ and obtain $t_2 = m_1 - r$.

Consider the following conditions:

(a) $p = 2$ and $\alpha_1 = \alpha_2 = m_1$;
(b) $p = 2, \alpha_1 > \alpha_2 = m_1$ and $m_2 = 0$.

Except in conditions (a) and (b), the result follows in Case (1) by considering orders of σ_1 and τ_1 modulo R_1R_2; in Case (2) by considering orders of σ_2 and τ_2 modulo R_1R_2; and in Case (3) by considering orders of σ_2 and τ_1 modulo R_1R_2.

It remains to prove the theorem when conditions (a) and (b) are satisfied in all the three cases (1)–(3).

First we consider Case (1) with condition (a). If $m_2 > 0$, then τ_1 has order $p^{m_1-m_2}$ modulo R_1R_2 and we are done. We assume that $m_2 = 0$.

If $t_1 \geq 1$ and $m_1 > 1$, then considering the orders of τ_1 and τ_2 gives p^{m_1} automorphisms modulo R_1R_2. If $t_1 \geq 1$ and $m_1 = 1$, then it follows that $t_1 = 1$. In this case, $r = 0$, and hence $t_2 = 1$. Therefore, we get $x_1^2 = x_2^2 = 1$. The map

$$\theta(x_l) = \begin{cases} x_2 & \text{if } l = 1, \\ x_1 & \text{if } l = 2, \\ x_l & \text{otherwise} \end{cases}$$

is an automorphism of order p^{m_1} modulo R_1R_2.

If $t_1 = 0$ and $m_1 > 1$, then $r > 0$. So, we can assume without loss of generality that $t_2 = m_1 - 1$. A direct check shows that the map

$$\theta(x_l) = \begin{cases} x_2x_1 & \text{if } l = 1, \\ x_2 & \text{if } l = 2, \\ x_l & \text{otherwise} \end{cases}$$

is an automorphism of order p^{m_1} modulo R_1R_2. Finally, suppose that $t_1 = 0$ and $m_1 = 1$. If $r = 0$, then $x_1^2 = x_2^2 = w_1$. And if $r > 0$, then $x_1^2 = w_1$ and $x_2^2 = 1$. The result now follows by considering the automorphisms

$$\theta_1(x_l) = \begin{cases} x_2 & \text{if } l = 1, \\ x_1 & \text{if } l = 2, \\ x_l & \text{otherwise} \end{cases}$$

and

$$\theta_2(x_l) = \begin{cases} x_1 & \text{if } l = 1, \\ x_1x_2 & \text{if } l = 2, \\ x_l & \text{otherwise} \end{cases}$$

respectively. Case (1) with condition (b) is analogous, and we leave it to the reader.

Cases (2) and (3) with condition (a) are analogous to Case (1) with condition (a). The result in Case (2) with condition (b) follows by considering the orders of σ_2 and τ_2 modulo R_1R_2. Finally, in Case (3) with condition (b) the result follows by considering the orders of σ_2 and τ_1 modulo R_1R_2. With this, the proof of the theorem is complete. □

4.3 Groups with Metacyclic Central Quotient

Recall that a group G is said to be *metacyclic* if it admits a cyclic normal subgroup N such that G/N is cyclic. In this section, for odd primes p, we show that finite p-groups G with metacyclic central quotient $G/\operatorname{Z}(G)$ satisfy Divisibility Property.

We begin with recalling the definition of regular p-group. A finite p-group G is said to be *regular* if for each $a, b \in G$, there exists $c \in \gamma_2(H)$ such that

$$(ab)^p = a^p b^p c^p,$$

where $H = \langle a, b \rangle$.

Throughout this section p is an odd prime. Let G be a finite p-group with metacyclic central quotient and of nilpotency class greater than 2. Set

$$\overline{G} = G/\operatorname{Z}(G).$$

Then there exists a cyclic normal subgroup B of $\overline{G}$ such that $\overline{G}/B$ is also cyclic. So we can choose elements $a, b \in G$ such that

$$B = \langle \operatorname{Z}(G)b \rangle,$$

where the order of $\operatorname{Z}(G)b$ is p^m, and

$$\overline{G}/B = \langle B\bar{a} \rangle,$$

where $\bar{a} = \operatorname{Z}(G)a$.

Let $\exp\big(G/\gamma_2(G)\big) = p^k$ and $\exp\big(\operatorname{Z}(G)\big) = p^l$. Then there exists an element $z_1 \in \operatorname{Z}(G)$ of order p^l such that

$$\operatorname{Z}(G) = \langle z_1 \rangle \oplus W_1$$

for some subgroup W_1 of $\mathrm{Z}(G)$ with

$$\exp(W_1) = p^{\beta}, \tag{4.18}$$

where $\beta \leq l$. Set

$$M = \langle b, \mathrm{Z}(G) \rangle.$$

Since $\gamma_2(G) \leq M$ and the order of Ma is p^m (by Theorem 1.16(1)), as observed in Chap. 1, it follows that the order of $\gamma_2(G)a$ is at least p^m, and therefore

$$k \geq m.$$

In the following result we derive a lower bound for $|\operatorname{Autcent}(G)|$.

Theorem 4.19 *Let G be a purely non-abelian finite p-group with metacyclic central quotient and of nilpotency class greater than 2. Then* $|\operatorname{Autcent}(G)| \geq p^{\alpha+\beta}\, |\mathrm{Z}(G)|$ *or* $|\operatorname{Autcent}(G)| \geq p^{2\alpha}\, |\mathrm{Z}(G)|$, *where α is as in (1.17) and β as in (4.18).*

Proof We have two cases: (1) $l \geq k$; (2) $l < k$.

Case (1): In this case, we decompose W_1 as

$$W_1 = \langle w_1 \rangle \oplus \cdots \oplus \langle w_n \rangle \oplus W_2,$$

where the order of each w_i is at least p^k and $\exp(W_2) < p^k$. Then

$$\begin{aligned} |\operatorname{Hom}\big(G/\gamma_2(G),\ \mathrm{Z}(G)\big)| &= |\operatorname{Hom}\big(G/\gamma_2(G),\ \langle z_1 \rangle\big)| \prod_{i=1}^{n} |\operatorname{Hom}\big(G/\gamma_2(G),\ \langle w_i \rangle\big)| \\ &\quad |\operatorname{Hom}\big(G/\gamma_2(G),\ W_2\big)| \\ &\geq |G/\gamma_2(G)|^{n+1}\, |W_2|. \end{aligned}$$

If $|\operatorname{Autcent}(G)| \geq |G| = p^{2m} |\mathrm{Z}(G)|$, then, since $m > \alpha$, $|\operatorname{Autcent}(G)| > p^{2\alpha} |\mathrm{Z}(G)|$, and we are done. So assume that $|\operatorname{Autcent}(G)| < |G|$. If $n > 0$, then by Theorem 3.72, we have

$$p^m\, |G/\gamma_2(G)| = |G| > |\operatorname{Autcent}(G)| \geq |G/\gamma_2(G)|^{n+1}.$$

Thus, we obtain

$$p^m > |G/\gamma_2(G)|^n \geq |G/\gamma_2(G)| \geq \exp\big(G/\gamma_2(G)\big) = p^k,$$

which is a contradiction to the fact that $k \geq m$. Hence, $n = 0$ and $W_1 = W_2$. Therefore, by Theorem 1.16(2), we obtain

$$|\operatorname{Autcent}(G)| \geq |G/\gamma_2(G)|\, |W_1| \geq |G/\gamma_2(G)|\, \exp(W_1) = p^{m+\beta}\, |\mathrm{Z}(G)| \geq p^{\alpha+\beta}\, |\mathrm{Z}(G)|.$$

Case (2): Decompose $G/\gamma_2(G)$ as

$$G/\gamma_2(G) = \langle \bar{x}_1 \rangle \oplus \cdots \oplus \langle \bar{x}_d \rangle,$$

where $\bar{x}_i = \gamma_2(G)x_i$ with $x_i \in G$ and

$$p^k = |\bar{x}_1| \geq |\bar{x}_2| \geq \cdots \geq |\bar{x}_d|.$$

Observe that $d \geq 2$ and assume for the moment that $|\bar{x}_1| \geq |\bar{x}_2| \geq p^\alpha$. Then

$$\begin{aligned} |\operatorname{Hom}\big(G/\gamma_2(G),\ \mathrm{Z}(G)\big)| &\geq |\operatorname{Hom}\big(\langle \bar{x}_1 \rangle,\ \mathrm{Z}(G)\big)|\,|\operatorname{Hom}\big(\langle \bar{x}_2 \rangle,\ \mathrm{Z}(G)\big)| \\ &= |\mathrm{Z}(G)|\,|\operatorname{Hom}\big(\langle \bar{x}_2 \rangle,\ \mathrm{Z}(G)\big)|. \end{aligned}$$

If $|\bar{x}_2| \geq p^l$, then

$$|\operatorname{Hom}\big(\langle \bar{x}_2 \rangle,\ \mathrm{Z}(G)\big)| = |\mathrm{Z}(G)| = p^l\,|W_1| \geq p^{\alpha+\beta}.$$

Hence, we obtain

$$|\operatorname{Autcent}(G)| \geq p^{\alpha+\beta}\,|\mathrm{Z}(G)|.$$

So we assume that $|\bar{x}_2| < p^l$. Since $|\bar{x}_2| \geq p^\alpha$, we have

$$|\operatorname{Hom}\big(G/\gamma_2(G),\ \mathrm{Z}(G)\big)| \geq |\mathrm{Z}(G)|\,|\operatorname{Hom}\big(\langle \bar{x}_2 \rangle,\ \langle z_1 \rangle\big)|\,|\operatorname{Hom}\big(\langle \bar{x}_2 \rangle,\ W_1\big)|.$$

Notice that $|\operatorname{Hom}\big(\langle \bar{x}_2 \rangle,\ W_1\big)| \geq p^\beta$ or p^α, depending on whether $|\bar{x}_2| \geq p^\beta$ or $|\bar{x}_2| < p^\beta$. Also

$$|\operatorname{Hom}\big(\langle \bar{x}_2 \rangle,\ \langle z_1 \rangle\big)| = |\langle \bar{x}_2 \rangle| \geq p^\alpha,$$

and hence we obtain

$$|\operatorname{Autcent}(G)| \geq p^{\alpha+\beta}\,|\mathrm{Z}(G)| \text{ or } p^{2\alpha}\,|\mathrm{Z}(G)|.$$

It only remains to prove that $|\bar{x}_2| \geq p^\alpha$. Suppose that $|\bar{x}_2| < p^\alpha$. Then $x_i^{p^{\alpha-1}} \in \gamma_2(G)$ for all $2 \leq i \leq d$. From the proof of Theorem 1.16, we obtain

$$|\gamma_2(G)\,\mathrm{Z}(G)/\,\mathrm{Z}(G)| = |\gamma_2(G)/\big(\gamma_2(G) \cap \mathrm{Z}(G)\big)| = p^{m-\alpha},$$

which implies that

$$\big(x_i^{p^{\alpha-1}}\big)^{p^{m-\alpha}} = x_i^{p^{m-1}} \in \mathrm{Z}(G)$$

for all $2 \leq i \leq d$. Since $[x_i, x_j]^{p^{m-1}} = 1$ for all $1 \leq i, j \leq d$, regularity of G implies that $\exp\big(\gamma_2(G)\big) \leq p^{m-1}$, a contradiction. The proof is now complete. □

We now present the following result of Davitt and Otto [21].

Theorem 4.20 *Let G be a finite p-group with $G/\mathrm{Z}(G)$ metacyclic, where p is an odd prime. Then $|G|$ divides $|\operatorname{Aut}(G)|$.*

Proof In view of Remark 4.7 and Theorem 4.17, we can assume that G is purely non-abelian of nilpotency class greater than 2. By Theorem 4.19, we have

$$|\operatorname{Autcent}(G)| \geq p^{2\alpha}\,|\mathrm{Z}(G)| \text{ or } p^{\alpha+\beta}\,|\mathrm{Z}(G)|.$$

By Theorem 1.18(1), we have

$$|\operatorname{IC}(G)| = \frac{|\operatorname{Inn}(G)|\,|\operatorname{Autcent}(G)|}{|\operatorname{Inn}(G) \cap \operatorname{Autcent}(G)|} = p^{2m-2\alpha}\,|\operatorname{Autcent}(G)|.$$

If $|\operatorname{Autcent}(G)| \geq p^{2\alpha}\,|\mathrm{Z}(G)|$, then we are done.

Assume that $|\operatorname{Autcent}(G)| \geq p^{\alpha+\beta}\,|\mathrm{Z}(G)|$, where $\beta < \alpha$. Set

$$F = \gamma_2(G)\,\mathrm{Z}(G).$$

Then $F = \langle b^{p^{\alpha}} \rangle\,\mathrm{Z}(G)$ and it is a normal subgroup of G of order $p^{m-\alpha}\,|\mathrm{Z}(G)|$. The approach for the rest of the proof is to modify the generating set for $G/\mathrm{Z}(G)$ to get a normal subgroup of G with cyclic quotient so that the hypothesis of Lemma 4.10 is satisfied. The proof is now divided into two cases: (1) $t_a \geq t_b$; (2) $t_a < t_b$, where t_a, t_b are as in Theorem 1.18.

Case (1): In this case, $t_a = t_b + r$ for some integer $r \geq 0$. Let $\tilde{a} = b^{-p^{r}}a$ and

$$K = \langle \tilde{a}, F \rangle.$$

Then K is a normal subgroup of G. Notice that $[\tilde{a}, b] = [a, b]$. If $\tilde{a}^{p^n} \in F$, then $[\tilde{a}, b]^{p^n} = 1$. It follows that the order of the element $F\tilde{a}$ is at least p^m. An easy exercise shows that $\tilde{a}^{p^m} \in \mathrm{Z}(G) \leq F$, and hence the order of $F\tilde{a}$ is precisely p^m. Thus,

$$|K| = p^{2m-\alpha}\,|\mathrm{Z}(G)|,$$

and therefore G/K is cyclic of order p^{α} generated by Kb. By Theorem 1.18(2), we obtain

$$\tilde{a}^{p^m} = b^{-p^{r+m}} a^{p^m} = z_1^{-p^{t_b+r}} z_1^{p^{t_a}} w$$

for some $w \in W_1$. Since $t_a = t_b + r$ and $\exp(W_1) = p^{\beta}$, we have

$$p^m \leq |\tilde{a}| \leq p^{m+\beta}.$$

Since $\alpha < m$, we can choose s such that $|\tilde{a}^{p^s}| = p^{\alpha}$ and $m + \beta - \alpha \geq s \geq m - \alpha$.

Notice that

$$[\tilde{a}^{p^{m-\alpha}}, b^{p^{\alpha}}] = [\tilde{a}, b]^{p^m} = 1.$$

Consequently, $\tilde{a}^{p^{m-\alpha}} \in \mathrm{Z}(K)$, and therefore $\tilde{a}^{p^s} \in \Omega_\alpha\big(\mathrm{Z}(K)\big)$. By Lemma 1.15, G is regular, and we have $(\tilde{a}^{p^s} b)^{p^\alpha} = b^{p^\alpha}$. Hence, by Lemma 4.10, there exists an automorphism ϕ of G of order p^α. Since $|F\tilde{a}| = p^m$, it follows that

$$|F\tilde{a}^{p^s}| = p^{m-s} \geq p^{\alpha-\beta}.$$

Hence, $b^{-1}\phi^{p^{\alpha-\beta-1}}(b) = \tilde{a}^{p^{s+\alpha-\beta-1}} \notin F$ and the order of ϕ modulo $\mathrm{IC}(G)$ is at least $p^{\alpha-\beta}$. Consequently, we obtain

$$|\operatorname{Aut}(G)|_p \geq |\langle \phi, \mathrm{IC}(G)\rangle| \geq p^{\alpha-\beta}\,|\,\mathrm{IC}(G)| \geq |G|.$$

Case (2): In this case, $t_b = t_a + r$ for some integer $r > 0$. Set $\tilde{b} = a^{-p^r} b$ and $L = \langle \tilde{b}, F\rangle$. It is clear that L is a normal subgroup of G. Observe that $|\tilde{b}| \geq p^m$. There are two subcases: (2a) $r + \alpha \geq m$; (2b) $r + \alpha < m$.

Subcase (2a): Notice that G/L is generated by La. We claim that $|G/L| = p^m$. Since $\mathrm{Z}(G) \leq L$ and $|\,\mathrm{Z}(G)a| = p^m$, it follows that $|La| = |G/L|$, which is at most p^m. Conversely, notice that

$$\tilde{b}^{p^\alpha} = (a^{-p^r} b)^{p^\alpha} = a^{-p^{r+\alpha}} b^{p^\alpha} g^{p^\alpha}$$

for some $g \in \gamma_2(G) \leq F$. Since $r + \alpha \geq m$, it follows that $a^{-p^{r+\alpha}} \in \mathrm{Z}(G) \leq F$, which implies that $\tilde{b}^{p^\alpha} \in F$. Consequently,

$$|L| \leq p^\alpha\,|F| = p^m\,|\mathrm{Z}(G)|,$$

and hence $|G/L| \geq p^m$. Thus, our claim is proved, and hence $|F\tilde{b}| = p^\alpha$.

As in Case (1), it follows that $\tilde{b}^{p^m} \in W_1$, which implies that

$$p^m \leq |\tilde{b}| \leq p^{m+\beta}.$$

We can now choose s with $0 \leq s \leq \beta$ such that $|\tilde{b}^{p^s}| = p^m$. Since $r + \alpha \geq m$, we have

$$[a^{-p^r}, b^{p^\alpha}] = [a^{-1}, b]^{p^{r+\alpha}} = 1.$$

Therefore, $[\tilde{b}, b^{p^\alpha}] = 1$, which in turn implies that $\tilde{b} \in \mathrm{Z}(L)$. It is now clear that $\tilde{b}^{p^s} \in \Omega_m\big(\mathrm{Z}(L)\big)$. Since G is regular, we have $(\tilde{b}^{p^s} a)^{p^m} = a^{p^m}$, and therefore by Lemma 4.10, there exists an automorphism ϕ of G of order p^m. Since $|F\tilde{b}| = p^\alpha$, it follows that $|F\tilde{b}^{p^s}| = p^{\alpha-s} \geq p^{\alpha-\beta}$. As in Case (1), the order of ϕ modulo $\mathrm{IC}(G)$ is at least $p^{\alpha-\beta}$, and we are done.

Subcase (2b): Let $\gamma = m - r - \alpha$. We claim that $|G/L| = p^{m-\gamma}$. Observe that

$$\tilde{b}^{p^{\alpha+\gamma}} = (a^{-p^r} b)^{p^{\alpha+\gamma}} = a^{-p^m} b^{p^{\alpha+\gamma}} g^{p^{\alpha+\gamma}}$$

for some $g \in \gamma_2(G) \leq F$. Thus, the order of $F\tilde{b}$ is at most $p^{\alpha+\gamma}$. If the order of $F\tilde{b}$ is less than $p^{\alpha+\gamma}$, then $\tilde{b}^{p^{\alpha+\gamma-1}} \in F$. But

$$\tilde{b}^{p^{\alpha+\gamma-1}} = (a^{-p^r}b)^{p^{\alpha+\gamma-1}} = a^{-p^{m-1}}b^{p^{\alpha+\gamma-1}}g^{p^{\alpha+\gamma-1}} \in F,$$

which implies that $a^{-p^{m-1}} \in F$. This gives

$$[a,b]^{p^{m-1}} = [a^{p^{m-1}}, b] = 1,$$

a contradiction. Hence, $|F\tilde{b}| = p^{\alpha+\gamma}$, and therefore

$$|L| = p^{m+\gamma}\,|\mathrm{Z}(G)|,$$

which further yields $|G/L| = p^{m-\gamma}$. Again observe that

$$p^m \leq |\tilde{b}| \leq p^{m+\beta},$$

which implies

$$p^{m-\gamma} \leq |\tilde{b}^{p^\gamma}| \leq p^{m+\beta-\gamma}.$$

Choose s with $\gamma \leq s \leq \gamma+\beta$ such that $|\tilde{b}^{p^s}| = p^{m-\gamma}$.

Notice that

$$[\tilde{b}^{p^\gamma}, b^{p^\alpha}] = [a^{-p^{r+\gamma}}, b^{p^\alpha}] = [a^{-p^{m-\alpha}}, b^{p^\alpha}] = [a^{-1}, b]^{p^m} = 1,$$

which implies that $\tilde{b}^{p^\gamma} \in \mathrm{Z}(L)$ and $\tilde{b}^{p^s} \in \Omega_{m-\gamma}\big(\mathrm{Z}(L)\big)$. Again, by Lemma 4.10, there exists an automorphism ϕ of G of order $p^{m-\gamma}$. Since $|F\tilde{b}| = p^{\alpha+\gamma}$, it follows that

$$|F\tilde{b}^{p^s}| = p^{\alpha+\gamma-s} \geq p^{\alpha-\beta}.$$

As before, we obtain that the order of ϕ modulo $\mathrm{IC}(G)$ is at least $p^{\alpha-\beta}$, which completes the proof of the theorem. □

As an immediate consequence we obtain the following result of Davitt [18] for metacyclic p-groups.

Corollary 4.21 *Let G be a purely non-abelian metacyclic p-group, where p is an odd prime. Then $|G|$ divides $|\operatorname{Aut}(G)|$.*

It would be interesting to explore the following:

Problem 4.22 Do purely non-abelian 2-groups with metacyclic central quotients have Divisibility Property?

4.4 Modular Groups

Recall that a group G is said to be modular if its lattice of all subgroups is modular. The aim of this section is to show that, for odd primes p, finite non-abelian modular p-groups have Divisibility Property.

Assume for the rest of the section that p is an odd prime, and G is a purely non-abelian modular p-group of nilpotency class greater than 2 such that $G/\operatorname{Z}(G)$ is not metacyclic.

Let G be a modular p-group. Then, by Theorem 1.21, there exists a normal abelian subgroup A of G and an integer $\alpha > 0$ such that $G/A = \langle Ab \rangle$ is cyclic,

$$\mho_\alpha(A) = \gamma_2(G)$$

and

$$\mho_{2\alpha}(A) = \gamma_3(G).$$

We now decompose A in a useful way as follows. Let $|G/A| = p^k$ and $\exp\big(\gamma_2(G)\big) = p^m$ for some positive integers k, m. Since $\mho_\alpha(A) = \gamma_2(G)$, we have $\exp(A) = p^{m+\alpha}$. Thus, we can write

$$A = \langle a_1 \rangle \oplus B$$

for some element a_1 of order $p^{m+\alpha}$ and some subgroup B. If $\exp(B) \le p^\alpha$, then

$$B \le \Omega_\alpha(A) = A \cap \operatorname{Z}(G) \le \operatorname{Z}(G),$$

which implies that $G/\operatorname{Z}(G)$ is metacyclic, which is contrary to our hypothesis. Hence, $\exp(B) > p^\alpha$, which also implies that $\exp\big(\operatorname{Z}(G)\big) > p^\alpha$. Consequently, we can write

$$B = \langle a_2 \rangle \oplus C$$

for some element a_2 of order $p^{m_2+\alpha}$ and some subgroup C of order p^r, where $r \ge 0$ and $m_2 > 0$. Hence, we can write

$$A = \langle a_1 \rangle \oplus \langle a_2 \rangle \oplus C. \tag{4.23}$$

If $G/\gamma_2(G)$ is generated by two elements, then G is generated by b and a_1, and hence is metacyclic, which is again contrary to our hypothesis. Hence, $G/\gamma_2(G)$ must be generated by at least 3 elements. By Theorem 1.23(1), we have $k > \alpha$. Thus, we can write

$$G/\gamma_2(G) = \langle \gamma_2(G)b_1 \rangle \oplus A/\gamma_2(G)$$

for some element $b_1 \in G$, where $|\langle \gamma_2(G)b_1 \rangle| > \exp\big(A/\gamma_2(G)\big)$. Let $|\langle \gamma_2(G)b_1 \rangle| = p^{k_1}$. Notice that $|\langle Ab_1 \rangle| = p^k$. Thus, without loss of generality, we can take $b = b_1$.

By (1.25), we have $|\langle \Omega_\alpha(A)b\rangle| = p^k$. This yields $|b| \leq p^{k+\alpha}$, which further implies that

$$k_1 \leq k + \alpha. \tag{4.24}$$

From the decomposition $A = \langle a_1 \rangle \oplus B$, we can write

$$G/\gamma_2(G) = \langle \gamma_2(G)b\rangle \oplus \langle \gamma_2(G)a_1\rangle \oplus H,$$

for some subgroup H of A of order p^s, where s is a positive integer. Notice that

$$|\langle \gamma_2(G)a_1\rangle| = p^\alpha, \tag{4.25}$$

and hence

$$|G/\gamma_2(G)| = |\langle \gamma_2(G)b\rangle \oplus \langle \gamma_2(G)a_1\rangle \oplus H| = p^{k_1+\alpha+s}. \tag{4.26}$$

Lemma 4.27 *With the above set-up, we have* $\exp\big(\mathrm{Z}(G)\big) \leq p^{k_1}$.

Proof Set $\exp\big(\mathrm{Z}(G)\big) = p^l$. Since $\Omega_\alpha(A) \leq \mathrm{Z}(G)$, we have $\alpha \leq l$. If $\alpha = l$, since $\alpha < k \leq k_1$, we obtain $l \leq k_1$. If $\alpha < l$, then from the fact that $\mathrm{Z}(G) = \langle b^{p^m}\rangle \Omega_\alpha(A)$, we obtain $|b^{p^m}| = p^l$, and hence $|b| = p^{l+m}$. Since $\exp\big(\gamma_2(G)\big) = p^m$ and $|\gamma_2(G)b| = p^{k_1}$, we get $b^{p^{m+k_1}} = 1$, which implies that $l \leq k_1$. □

Lemma 4.28 *With the above set-up, we have* $|\,\mathrm{IC}(G)| \geq p^{s-\alpha}\,|G|$.

Proof First notice that

$$\begin{aligned}
|\,\mathrm{IC}(G)| &= \frac{|G|\,|\,\mathrm{Autcent}(G)|}{|\,\mathrm{Z}_2(G)|} \\
&= \frac{p^k\,|A|\,|\,\mathrm{Autcent}(G)|}{p^{k-m+\alpha}\,|\Omega_{2\alpha}(A)|} \\
&= \frac{p^{m-\alpha}\,|\,\mathrm{Autcent}(G)|\,|A|}{|\Omega_{2\alpha}(A)|} \\
&= p^{m-\alpha}\,|\,\mathrm{Autcent}(G)|\,|\mho_{2\alpha}(A)|.
\end{aligned}$$

Since $G/\gamma_2(G) = G/\mho_\alpha(A)$, we have

$$|G/\gamma_2(G)| = |G/A|\,|A/\mho_\alpha(A)| = p^k\,|\Omega_\alpha(A)|. \tag{4.29}$$

By Lemma 4.27, we get

$$|\,\mathrm{Hom}\big(\langle \gamma_2(G)b\rangle,\ \mathrm{Z}(G)\big)| = |\,\mathrm{Z}(G)|. \tag{4.30}$$

By (4.25), it follows that

$$|\operatorname{Hom}\big(\langle\gamma_2(G)a_1\rangle,\ \mathrm{Z}(G)\big)| = |\Omega_\alpha\big(\mathrm{Z}(G)\big)| \geq |\Omega_\alpha(A)|. \tag{4.31}$$

Further, since $\exp\big(\mathrm{Z}(G)\big) \geq p^\alpha \geq \exp(H)$, we obtain

$$|\operatorname{Hom}\big(H,\ \mathrm{Z}(G)\big)| \geq p^s. \tag{4.32}$$

Now Theorem 3.72 yields

$$\begin{aligned}|\operatorname{Autcent}(G)| &= |\operatorname{Hom}\big(G/\gamma_2(G),\ \mathrm{Z}(G)\big)|\\ &= |\operatorname{Hom}\big(\langle\gamma_2(G)b\rangle,\ \mathrm{Z}(G)\big)|\,|\operatorname{Hom}\big(\langle\gamma_2(G)a_1\rangle,\ \mathrm{Z}(G)\big)|\,|\operatorname{Hom}\big(H,\ \mathrm{Z}(G)\big)|.\end{aligned}$$

Combining the preceding equality together with (4.30), (4.31), (4.32) and using Theorem 1.23(2), we get

$$|\operatorname{Autcent}(G)| \geq\ p^s\,|\mathrm{Z}(G)|\,|\Omega_\alpha(A)| \geq p^{k+s-m}\,|\Omega_\alpha(A)|^2.$$

Finally, we obtain

$$\begin{aligned}|\operatorname{IC}(G)| &= p^{m-\alpha}\,|\operatorname{Autcent}(G)|\,|\mho_{2\alpha}(A)|.\\ &\geq p^{k+s-\alpha}\,|\Omega_\alpha(A)|^2\,|\mho_{2\alpha}(A)|\\ &\geq p^{k+s-\alpha}\,|A|\ \text{ (by Exercise 1.14)}\\ &= p^{s-\alpha}\,|G|,\end{aligned} \tag{4.33}$$

which completes the proof. □

We are now in a position to prove the main result of this section, which is originally due to Davitt and Otto [22].

Theorem 4.34 *Let G be a finite non-abelian modular p-group, where p is an odd prime. Then $|G|$ divides $|\operatorname{Aut}(G)|$.*

Proof In view of Remark 4.7, Theorems 4.17 and 4.20, we can assume that G is purely non-abelian of nilpotency class greater than 2 with $G/\mathrm{Z}(G)$ not metacyclic.

In view of Lemma 4.28, it only remains to prove that $s \geq \alpha$. By (4.23), we have

$$A = \langle a_1\rangle \oplus \langle a_2\rangle \oplus C,$$

where $|a_1| = p^{m+\alpha}$, $|a_2| = p^{m_2+\alpha}$ and $|C| = p^r$. The proof is now divided into the following two cases: (1) $r \geq \alpha$; (2) $r < \alpha$.

Case (1): In this case, if $\exp(C) \geq p^\alpha$, then $|\Omega_\alpha(A)| \geq p^{3\alpha}$. If $\exp(C) < p^\alpha$, then $C \leq \Omega_\alpha(A)$, and hence

$$|\Omega_\alpha(A)| = p^{2\alpha}\,|C| = p^{2\alpha+r} \geq p^{3\alpha}.$$

Thus, in either case $|\Omega_\alpha(A)| \geq p^{3\alpha}$. By (4.29), we obtain

$$|G/\gamma_2(G)| \geq p^{k+3\alpha}.$$

By (4.26), we have $k_1 + \alpha + s \geq k + 3\alpha$. Finally, by (4.24), we get $s \geq \alpha$, and the proof is complete in this case.

Case (2): In this case, we have $C \leq \Omega_\alpha(A)$ and the decomposition of A gives

$$\Omega_\alpha(A) = \langle a_1^{p^m} \rangle \oplus \langle a_2^{p^{m_2}} \rangle \oplus C.$$

Since, $|\Omega_\alpha(A)b| = p^k$ by (1.25), we get

$$b^{p^k} = a_1^{n_1 p^m} a_2^{n_2 p^{m_2}} c,$$

where $n_1, n_2 \geq 0$ and $c \in C$. Also, $|\Omega_\alpha(A)| = p^{2\alpha+r}$. Now, we have two subcases: (2a) $m_2 \geq \alpha$; (2b) $m_2 < \alpha$.

Subcase (2a): In this subcase, since $\exp(C) \leq p^r$, we have

$$b^{p^{k+r}} = a_1^{n_1 p^{m+r}} a_2^{n_2 p^{m_2+r}}.$$

Since $m, m_2 \geq \alpha$, we obtain $b^{p^{k+r}} \in \mho_\alpha(A) = \gamma_2(G)$. Now, $|\gamma_2(G)b| = p^{k_1}$ gives $k + r \geq k_1$. Combining all these with

$$|G/\gamma_2(G)| = p^{k_1+\alpha+s} = p^k\, |\Omega_\alpha(A)|,$$

we get $k_1 + \alpha + s = k + 2\alpha + r$. This implies $k + r + \alpha + s \geq k + 2\alpha + r$ or equivalently $s \geq \alpha$.

Subcase (2b): If $\alpha - m_2 \leq r$, then $r = \alpha - m_2 + \beta$ for some $\beta \geq 0$. Since $c^{p^r} = 1$, we have

$$b^{p^{k+r}} = a_1^{n_1 p^{m+\alpha-m_2+\beta}} a_2^{n_2 p^{\alpha+\beta}}.$$

Since $\beta \geq 0$ and $\alpha > m_2$, we have $b^{p^{k+r}} \in \mho_\alpha(A) = \gamma_2(G)$. As in Subcase (2a), $k + r \geq k_1$, and hence $s \geq \alpha$.

Finally, suppose that $\alpha - m_2 > r$. In this case, we directly show that $|\operatorname{IC}(G)| \geq |G|$. Observe that

$$b^{p^{k+\alpha-m_2}} = a_1^{n_1 p^{m+\alpha-m_2}} a_2^{n_2 p^{\alpha}},$$

since $c^{p^{\alpha-m_2}} = 1$. Thus, we get $b^{p^{k+\alpha-m_2}} \in \mho_\alpha(A) = \gamma_2(G)$, and hence $k + \alpha - m_2 \geq k_1$. Again combining all these with

$$|G/\gamma_2(G)| = p^{k_1+\alpha+s} = p^k\, |\Omega_\alpha(A)|,$$

we get $k_1 + \alpha + s = k + 2\alpha + r$. Hence, $k + \alpha - m_2 + \alpha + s \geq k + 2\alpha + r$, and therefore $s \geq m_2 + r$. Since $m_2 < \alpha$, we get $\mho_{2\alpha}(A) = \langle a_1^{p^{2\alpha}} \rangle$, which implies

$$|\mho_{2\alpha}(A)| = p^{m-\alpha}.$$

By Exercise 1.14, we obtain

$$|\gamma_2(G)| = |\mho_\alpha(A)| = |A|/|\Omega_\alpha(A)| = p^{m+m_2}.$$

By (4.33), we have

$$|\operatorname{IC}(G)| \geq p^{k+s-\alpha}\, |\Omega_\alpha(A)|^2\, |\mho_{2\alpha}(A)|,$$

which yields

$$|\operatorname{IC}(G)| \geq p^{k+s-\alpha}\, (p^{2\alpha+r})^2\, p^{m-\alpha} \geq p^{k+m+2\alpha+2r+s} \geq p^{2r+(k_1+\alpha+s)+(m+m_2)} = p^{2r}\, |G|,$$

and the proof is now complete. □

The following problem remains open.

Problem 4.35 Do finite non-abelian modular 2-groups have Divisibility Property?

4.5 *p*-Abelian Groups

For a positive integer n, recall that a group G is said to be *n-abelian* if

$$(xy)^n = x^n y^n$$

for all elements $x, y \in G$. Notice that 2-abelian groups are abelian. For notational convenience, we set

$$D(G) = \operatorname{Aut}^{\Omega_1(Z(G))}(G),$$

the group of automorphisms of G which centralize $\Omega_1\big(Z(G)\big)$. Notice that

$$\operatorname{Inn}(G) \leq D(G) \leq \operatorname{Aut}(G).$$

In this section, Divisibility Property is established for p-abelian p-groups. The result is originally due to Davitt [19].

We begin with the following technical results.

Lemma 4.36 *Let G be a finite p-abelian p-group with* $\exp(G) \geq p^2$ *and*

$$\mho_1(G) = \langle a^p \rangle \oplus M,$$

where a is an element of order p^{n+1} for some $n \geq 1$ and $M \leq G$. Then the set

$$L := \{x \in G \mid x^p \in M\}$$

is a normal subgroup of G, $\Omega_1(G) \leq L$, $G = L\langle a\rangle$, $L \cap \langle a\rangle = \langle a^{p^n}\rangle \leq \Omega_1\big(\mathrm{Z}(G)\big)$ and $G/L = \langle La\rangle$ is a cyclic group of order p^n.

Proof Since the exponent of $\Omega_1(G)$ is p, $\Omega_1(G) \leq L$. By Theorem 1.26, $\gamma_2(G) \leq \Omega_1(G)$, and hence L is a normal subgroup of G. Further, it is easy to see that $G = \langle a\rangle L$. Since $a^k \notin M$ for any $k < p^{n+1}$, we have $L \cap \langle a\rangle = \langle a^{p^n}\rangle$. Consequently, by Theorem 1.26, $\langle a^{p^n}\rangle \leq \Omega_1\big(\mathrm{Z}(G)\big)$. Hence, $G/L = \langle La\rangle$ is a cyclic group of order p^n. □

Lemma 4.37 *Let G be a finite p-abelian p-group as in Lemma 4.36. Then the following statements hold:*

(1) The map $\sigma : G \to G$ defined by

$$\sigma(la^k) = l(a^{p+1})^k,$$

where $0 \leq k < p^n$ and $l \in L$, is an element of $D(G)$ of order p^n.

(2) Let $N \leq \Omega_n\big(\mathrm{Z}(L)\big)$. Then for each $x \in N$, the map $\phi_x : G \to G$ defined by

$$\phi_x(la^k) = l(xa)^k,$$

where $0 \leq k < p^n$ and $l \in L$, is an element of $D(G)$. Further, the order of ϕ_x is equal to the order of x.

(3) If $S_N := \{\phi_x \mid x \in N\}$, then $S_N \leq D(G)$ and $S_N \cong N$.

Proof Notice that the maps σ and ϕ_x satisfy the hypothesis of Lemma 4.10, and proof of first two assertions follows. The third assertion immediately follows once S_N is a group. Let $x, y \in N$. Then

$$\phi_x\phi_y(a) = \phi_x(ya) = (yx)a = \phi_{yx}(a),$$

and hence S_N is a group. □

We need the following elementary number-theoretic result.

Exercise 4.38 For a prime p, the following statements hold:

(1) If $k \geq 1$ is an integer and $r = \sum_{j=1}^{p}(p+1)^{jk}$, then p divides r.

(2) If p is odd and $k \geq 0$ an integer, then

$$(p+1)^{p^k} \equiv 1 \mod p^{k+1}$$

and

$$(p+1)^{p^k} \equiv (1 + p^{k+1}) \mod p^{k+2}.$$

If $N = \Omega_n\big(\mathrm{Z}(L)\big)$, then we denote S_N simply by S. Further, set

$$R = \langle \sigma \rangle,$$

where σ is as defined in Lemma 4.37(1).

Lemma 4.39 *Let G be a finite p-abelian p-group as in Lemma 4.36. Then the following statements hold:*

(1) R is a subgroup of $N_{\mathrm{Aut}(G)}(S)$, $RS \leq D(G)$, $R \cap S = \langle \phi_{a^{p^n}} \rangle$, $|RS| = p^{n-1}|\Omega_n\big(\mathrm{Z}(L)\big)|$ and $RS/S = \langle S\sigma \rangle$ is a cyclic group of order p^{n-1}.
(2) Let $x \in \Omega_n\big(\mathrm{Z}(L)\big)$ and $s, k \geq 1$ be integers. Then

$$(\phi_x \sigma^k)^s = \sigma^{sk} \phi_{x^r},$$

where $r = \sum_{j=1}^{s} (p+1)^{jk}$.
(3) If $\theta \in \Omega_1(RS)$, then $\theta = \phi_x$ for some $x \in \Omega_1\big(\mathrm{Z}(L)\big)$.

Proof Consider

$$\begin{aligned}\sigma^{-1}\phi_x\sigma(a) &= \sigma^{-1}\phi_x(a^{p+1})\\ &= \sigma^{-1}(xa)^{p+1}\\ &= \sigma^{-1}(x^{p+1}a^{p+1}),\ \text{since } x^p \in \mathrm{Z}(G) \text{ by Theorem 1.26}\\ &= x^{p+1}\sigma^{-1}(\sigma(a))\\ &= \phi_{x^{p+1}}(a).\end{aligned}$$

This shows that $\sigma \in \mathrm{N}_{\mathrm{Aut}(G)}(S)$. The remaining assertions of (1) are left as an exercise.

Assertion (2) is proved by induction on s. For $s = 1$, by imitating proof of (1), it follows that $\phi_x \sigma^k = \sigma^k \phi_{x^{(p+1)^k}}$ for all $k \geq 1$. Suppose that

$$(\phi_x \sigma^k)^{s-1} = \sigma^{(s-1)k} \phi_{x^{r_1}},$$

where $r_1 = \sum_{j=1}^{s-1} (p+1)^{jk}$. Then we obtain

$$\begin{aligned}(\phi_x\sigma^k)^s &= \phi_x\sigma^k(\phi_x\sigma^k)^{s-1}\\ &= \phi_x\sigma^k\sigma^{(s-1)k}\phi_{x^{r_1}}\\ &= \sigma^{sk}\phi_{x^{(p+1)^{sk}}}\phi_{x^{r_1}}\\ &= \sigma^{sk}\phi_{x^{r_1+(p+1)^{sk}}},\end{aligned}$$

where $r_1 + (p+1)^{sk} = r$, and assertion (2) is established.

Let $\theta = \phi_x\sigma^k \in \Omega_1(RS)$, where $0 \leq k < p^{n-1}$ and $x \in \Omega_n\big(\mathrm{Z}(L)\big)$. We claim that $k = 0$. Suppose that $k > 0$. Then we have

$$1 = \theta^p = (\phi_x \sigma^k)^p = \sigma^{pk} \phi_{x^r},$$

where $r = \sum_{j=1}^{p} (p+1)^{jk}$. Notice that $\sigma^{pk} \neq 1$ as the order of σ is p^n. Hence, $\phi_{x^r} \neq 1$ and lies in $R \cap S = \langle \phi_{a^{p^n}} \rangle$. Thus, $x^r \in \langle a^{p^n} \rangle \leq \langle a^p \rangle$. Since $x \in L$ and p divides r by Exercise 4.38(1), $x^r \in M \cap \langle a^p \rangle = 1$. Hence, $\phi_{x^r} = 1$, which is a contradiction. Thus, we have proved that $\theta \in \Omega_1(S)$, and therefore $x \in \Omega_1\big(\mathrm{Z}(L)\big)$ by Lemma 4.37(3). □

Let G be a non-abelian p-abelian p-group such that $\exp(G) = p^{m+1}$, where $m \geq 1$. Consequently, p must be an odd prime. Let

$$\mho_1(G) = \langle a_1^p \rangle \oplus \cdots \oplus \langle a_t^p \rangle,$$

where the order of a_i is p^{n_i+1} and $n_1 \geq \cdots \geq n_t$. For each $1 \leq i \leq t$, define

$$M_i = \langle a_1^p \rangle \oplus \cdots \oplus \langle a_{i-1}^p \rangle \oplus \langle a_{i+1}^p \rangle \oplus \cdots \oplus \langle a_t^p \rangle$$

and

$$L_i = \{x \in G \mid x^p \in M_i\}.$$

In the following result we collect interesting information about these groups, proof of which is similar to that of Lemma 4.36, and hence omitted.

Lemma 4.40 *Let G be a p-abelian p-group as in the preceding paragraph with subgroups M_i and L_i for each $1 \leq i \leq t$. Then $\Omega_1(G) \leq L_i \lhd G$, $G = L_i \langle a_i \rangle$, $L_i \cap \langle a_i \rangle = \langle a_i^{p^{n_i}} \rangle \leq \Omega_1\big(\mathrm{Z}(G)\big)$ and $G/L_i = \langle L_i a_i \rangle$ is cyclic of order p^{n_i}. Further, if $j \neq i$, then $a_j \in L_i$.*

Since $\mho_1(G) \leq \mathrm{Z}(G)$ and $\exp(G) = p^{m+1}$, it follows that $\exp\big(\mathrm{Z}(G)\big)$ is either p^m or p^{m+1}. First, we deal with the case $\exp\big(\mathrm{Z}(G)\big) = p^m$. The following result is a direct consequence of the definitions.

Lemma 4.41 *Let G be a p-abelian p-group with the above set-up and* $\exp\big(\mathrm{Z}(G)\big) = \exp\big(\mho_1(G)\big) = p^m$*. Then, for each i with $n_i = m$, the following statements hold:*

(1) $\mathrm{C}_G(L_i) = \mathrm{Z}(L_i)\langle a_i^p \rangle$ *is an abelian normal subgroup of G;*
(2) $\Omega_{n_i}\big(\mathrm{C}_G(L_i)\big) = \Omega_{n_i}\big(\mathrm{Z}(L_i)\big)\langle a_i^p \rangle$.

Remark 4.42 For each $1 \leq i \leq t$, imitating Lemma 4.37, we have the following:

(1) The map $\sigma_i : G \to G$ defined by

$$\sigma_i(l_i a_i^{k_i}) = l_i (a_i^{p+1})^{k_i},$$

where $0 \leq k_i < p^{n_i}$ and $l_i \in L_i$, is an element of $D(G)$ of order p^{n_i}.

(2) For each $x \in \Omega_{n_i}\big(\mathrm{Z}(L_i)\big)$, the map $\phi_{i,x} : G \to G$ defined by

$$\phi_{i,x}(l_i a_i^{k_i}) = l_i (x a_i)^{k_i},$$

where $0 \leq k_i < p^{n_i}$ and $l_i \in L_i$, is an element of $D(G)$.

(3) If $S_i := \{\phi_{i,x} \mid x \in \Omega_{n_i}\big(\mathrm{Z}(L_i)\big)\}$, then $S_i \leq D(G)$ and $S_i \cong \Omega_{n_i}\big(\mathrm{Z}(L_i)\big)$.

For each $1 \leq i \leq t$, set

$$R_i = \langle \sigma_i \rangle,$$

$$T = \prod_{i=1}^{t} R_i$$

and

$$W_i = \big\{\phi_{i,x} \mid x \in \Omega_1\big(\mathrm{Z}(G)\big)\big\}.$$

Lemma 4.43 *Let G be a p-abelian p-group with the preceding set-up. Then the following statements hold:*

(1) T is the direct product $R_1 \oplus \cdots \oplus R_t$.

(2) For $1 \leq i, j \leq t$, $\sigma_j \in \mathrm{N}_{\mathrm{Aut}(G)}(S_i)$.

(3) $W_i \leq D(G)$ and $W_i \cong \Omega_1\big(\mathrm{Z}(G)\big)$. Furthermore, if $j \neq i$, then $W_j \leq \mathrm{C}_{\mathrm{Aut}(G)}(W_i)$.

Proof Fix i such that $1 \leq i \leq t$. Let $j \neq i$ and $l_i \in L_i$. Then we can write $l_i = l_j a_j^k$, where $0 \leq k < p^{n_j}$ and $l_j \in L_i \cap L_j$. We obtain

$$\begin{aligned}
\sigma_j^{-1}\sigma_i\sigma_j(l_i) &= \sigma_j^{-1}\sigma_i\sigma_j\big(l_j a_j^k\big) \\
&= \sigma_j^{-1}\sigma_i\big(l_j a_j^{(p+1)k}\big) \\
&= \sigma_j^{-1}\big(l_j a_j^{(p+1)k}\big), \text{ since } a_j^{(p+1)k} l_j \in L_i \\
&= \sigma_i(l_i).
\end{aligned}$$

Further, we obtain

$$\sigma_j^{-1}\sigma_i\sigma_j(a_i) = a_i^{p+1} = \sigma_i(a_i),$$

and hence $\sigma_i\sigma_j = \sigma_j\sigma_i$. Obviously $\langle\sigma_i\rangle \cap \langle\sigma_j\rangle = 1$, and therefore T is the direct product of R_i, $1 \leq i \leq t$, establishing assertion (1).

Observe that assertion (2) for $i = j$ is simply Lemma 4.39(1). So, fix i such that $i \neq j$. Let $x \in \Omega_{n_i}\big(\mathrm{Z}(L_i)\big)$ and $l_i = l_j a_j^k$, where $0 \leq k < p^{n_j}$ and $l_j \in L_i \cap L_j$. As in assertion (1), it follows that $\sigma_j^{-1}\phi_{i,x}\sigma_j(l_i) = l_i$. Further, we have

$$\sigma_j^{-1}\phi_{i,x}\sigma_j(a_i) = \sigma_j^{-1}(x)a_i.$$

It remains to be proved that

$$y := \sigma_j^{-1}(x) \in \Omega_{n_i}\big(\mathrm{Z}(L_i)\big).$$

Writing

$$G = L_i\langle a_j^{p+1}\rangle,$$

we get $x = l'_j a_j^{r(p+1)}$, for some $0 \le r < p^{n_j}$ and $l'_j \in L_j$. Consequently, we obtain

$$y = \sigma_j^{-1}(l'_j a_j^{r(p+1)}) = l'_j a_j^r = x a_j^{-rp}.$$

Since $a_j^{-rp} \in L_i \cap \mathrm{Z}(G)$, it follows that $a_j^{-rp} \in \Omega_{n_i}\big(\mathrm{Z}(L_i)\big)$, and hence $y \in \Omega_{n_i}\big(\mathrm{Z}(L_i)\big)$.

Assertion (3) follows from Lemma 4.37 by observing that $\Omega_1\big(\mathrm{Z}(G)\big) \le \Omega_{n_i}\big(\mathrm{Z}(L_i)\big)$ for each $1 \le i \le t$. □

Theorem 4.44 *Let G be a non-abelian p-abelian p-group with* $\exp(G) = p^{m+1}$, *where* $m \ge 1$. *If* $\exp\big(\mathrm{Z}(G)\big) = \exp\big(\mho_1(G)\big) = p^m$, *then* $|G|$ *divides* $|D(G)|$.

Proof Recall that $\mho_1(G) = \langle a_1^p\rangle \oplus \cdots \oplus \langle a_t^p\rangle$, where the order of a_i is p^{n_i+1} and $m = n_1 \ge n_2 \ge \cdots \ge n_t$. We have the following two cases:

(1) $\exp\big(\mathrm{Z}(L_1)\big) \le \exp\big(\mathrm{Z}(G)\big) = p^{n_1}$;
(2) $\exp\big(\mathrm{Z}(L_1)\big) = \exp(G) = p^{n_1+1}$.

Case (1): By Lemmas 4.39(1) and 4.41, we have $R_1S_1 \le D(G)$ and

$$|R_1S_1| = p^{n_1-1}\,|\Omega_{n_1}\big(\mathrm{Z}(L_1)\big)| = p^{n_1-1}\,|\mathrm{Z}(L_1)| = |\,\mathrm{C}_G(L_1)|.$$

The idea is to show that R_1S_1 along with $\mathrm{Inn}(G)$ is big enough in this case. Since $\mathrm{C}_G(L_1)$ is a normal abelian subgroup of G, the map

$$\rho_1 : \mathrm{C}_G(L_1) \to \mathrm{C}_G(L_1)$$

given by $\rho_1(x) = [x, a_1]$ is an endomorphism of $\mathrm{C}_G(L_1)$. Then it follows that

$$|\,\mathrm{C}_G(L_1)| = |\,\mathrm{Ker}(\rho_1)|\;|\,\mathrm{Im}(\rho_1)|.$$

Since $\mathrm{Im}(\rho_1) \le \gamma_2(G) \le \Omega_1(G) \le L_1$ and $\mathrm{Im}(\rho_1) \le \mathrm{C}_G(L_1)$, we get

$$\mathrm{Im}(\rho_1) \le \Omega_1\big(\mathrm{Z}(L_1)\big).$$

Let us set

$$T = \{\phi_{1,y} \mid y \in \mathrm{Im}(\rho_1)\}.$$

Now by Lemma 4.37(3), $T \leq S_1$ and $T \cong \mathrm{Im}(\rho_1)$. We claim that $T = R_1S_1 \cap \mathrm{Inn}(G)$.

Let $\theta \in R_1S_1 \cap \mathrm{Inn}(G)$. Since $\theta \in \mathrm{Inn}(G)$, it follows that the order of θ is p, and therefore $\theta \in \Omega_1(R_1S_1)$. Now it follows by Lemma 4.39(3) that $\theta = \phi_{1,x}$ for some $x \in \Omega_1\big(\mathrm{Z}(L_1)\big)$. Let $\theta = \iota_g$ for some $g \in G$. For any element $l \in L_1$, we have

$$glg^{-1} = \theta(l) = \phi_{1,x}(l) = l,$$

and hence $g \in \mathrm{C}_G(L_1)$. On the other hand

$$\phi_{1,x}(a_1) = xa_1 = ga_1g^{-1}.$$

Hence, $x = [g, a_1] = \rho_1(g) \in \mathrm{Im}(\rho_1)$ and $\phi_{1,x} \in T$.

Conversely, if $\phi_{1,x} \in T$, then $x \in \mathrm{Im}(\rho_1)$. Thus, there exists an element $g \in \mathrm{C}_G(L_1)$ such that $\rho_1(g) = [g, a_1] = x$. Consequently, we obtain

$$\phi_{1,x}(a_1) = ga_1g^{-1}.$$

Since $g \in \mathrm{C}_G(L_1)$ and $G = L_1\langle a_1\rangle$, $\phi_{1,x}$ is an inner automorphism of G induced by g. Since $\mathrm{Im}(\rho_1) \leq \Omega_1\big(\mathrm{Z}(L_1)\big)$, it follows that $\phi_{1,x} \in S_1$, and hence $\phi_{1,x} \in R_1S_1 \cap \mathrm{Inn}(G)$, which settles the claim.

Recall that $R_1S_1\,\mathrm{Inn}(G) \leq D(G)$ and

$$|D(G)| \geq |R_1S_1\,\mathrm{Inn}(G)| = \frac{|\,\mathrm{C}_G(L_1)|\,|G/\mathrm{Z}(G)|}{|\,\mathrm{Im}(\rho_1)|} = |\,\mathrm{Ker}(\rho_1)|\,|G/\mathrm{Z}(G)|.$$

Since $\mathrm{Z}(G) \leq \mathrm{Ker}(\rho_1)$, it follows that $|G|$ divides $|D(G)|$, and the proof of theorem in Case (1) is complete.

Case (2): In this case, $n_1 = n_2 = m$, and hence we can assume that $a_2 \in \mathrm{Z}(L_1)$. Just as in Case (1), by considering L_2 instead of L_1, we prove

$$|R_2S_2\,\mathrm{Inn}(G)| = \frac{|\Omega_{n_2}\big(\mathrm{C}_G(L_2)\big)|\,|G/\mathrm{Z}(G)|}{|\,\mathrm{Im}(\rho_2)|}, \tag{4.45}$$

where the endomorphism

$$\rho_2 : \mathrm{C}_G(L_2) \to \mathrm{C}_G(L_2)$$

is given by $\rho_2(x) = [x, a_2]$. If $[b, a_2] = 1$ for all $b \in \mathrm{C}_G(L_2)$, then $\mathrm{Im}(\rho_2) = 1$. Since $|\,\mathrm{Z}(G)|$ divides $|\Omega_{n_2}\big(\mathrm{C}_G(L_2)\big)|$, it follows that $|G|$ divides $|R_2S_2\,\mathrm{Inn}(G)|$.

From this point onwards, we assume that $[b_1, a_2] \neq 1$ for some $b_1 \in \mathrm{C}_G(L_2)$. Since $G = L_1\langle a_1\rangle$, we can write $b_1 = l_1a_1^k$, where $0 \leq k < p^{n_1}$ and $l_1 \in L_1$. As $a_2 \in \mathrm{Z}(L_1) \trianglelefteq G$, it follows that $[a_1^k, a_2] \in \mathrm{Z}(L_1)$. Consequently,

$$1 \neq [b_1, a_2] = [l_1a_1^k, a_2] = [a_1^k, a_2],$$

and hence $p \nmid k$. Since $|a_1| = p^{n_1+1}$, it follows that $|b_1| = p^{n_1+1}$, and hence

$$\mho_1(G) = \langle b_1^p \rangle \oplus K$$

for some subgroup K. Therefore, we can now assume that $a_1 = b_1$.

We claim that $|\operatorname{Im}(\rho_2)| = p$. Notice that $a_1 \in \mathrm{Z}(L_2)$, $a_2 \in \mathrm{Z}(L_1)$, and therefore $1 \neq [a_1, a_2] \in \mathrm{Z}(G)$. For each $x \in \mathrm{C}_G(L_2)$, we write $x = l_1 a_1^r$, where $0 \le r < p^{n_1}$ and $l_1 \in L_1$. Then, we have

$$\rho_2(x) = [x, a_2] = [l_1 a_1^r, a_2] = [a_1^r, a_2] = [a_1, a_2]^r.$$

Since the order of $[a_1, a_2]$ is p, the claim follows. The remaining proof is divided into two subcases: (2a) $m = 1$; (2b) $m > 1$.

Subcase (2a): It is clear that $\exp(G) = p^2$ and $\mathrm{Z}(G) = \Omega_1\big(\mathrm{Z}(G)\big)$. Further, as $[a_2, a_1] \neq 1$, we have $\mathrm{C}_G(L_2) = \mathrm{Z}(L_2)$, and hence

$$\Omega_1\big(\mathrm{C}_G(L_2)\big) = \Omega_1\big(\mathrm{Z}(L_2)\big).$$

Since $\sigma_2 = \phi_{1,a_2^p}$, it follows that

$$R_2 S_2 = S_2.$$

Further, $\mathrm{Z}(G) \le \Omega_1\big(\mathrm{Z}(L_2)\big)$ implies that $|\Omega_1\big(\mathrm{Z}(L_2)\big)| = p^s\,|\mathrm{Z}(G)|$ for some $s \ge 0$. Thus, by (4.45), we get

$$|S_2 \operatorname{Inn}(G)| = \frac{|\Omega_1\big(\mathrm{C}_G(L_2)\big)|\;|G/\mathrm{Z}(G)|}{|\operatorname{Im}(\rho_2)|} = \frac{p^s\,|\mathrm{Z}(G)|\;|G/\mathrm{Z}(G)|}{p} = p^{s-1}\,|G|.$$

If $s > 0$, then we are done. Assume that $s = 0$. Recall that

$$W_i = \big\{\phi_{i,x} \mid x \in \Omega_i\big(\mathrm{Z}(G)\big)\big\}$$

for $i = 1, 2$. Notice that $W_2 = S_2$ by the very definition. Since

$$\langle a_1^p \rangle \oplus \langle a_2^p \rangle \le \Omega_1\big(\mathrm{Z}(G)\big),$$

by Lemma 4.43, we have $|W_1| \ge p^2$. It is easy to see that

$$W_1 \cap S_2 \operatorname{Inn}(G) = \langle \phi_{1,[a_1,a_2]} \rangle$$

is of order p. Therefore, we get

$$|W_1 S_2 \operatorname{Inn}(G)| = \frac{|W_1|\;|S_2 \operatorname{Inn}(G)|}{|W_1 \cap S_2 \operatorname{Inn}(G)|} \ge |G|.$$

Subcase (2b): In this case, $\exp(G) \geq p^3$ and $n_1 = n_2 = m \geq 2$. Since $\sigma_1 \in \mathrm{C}_{\mathrm{Aut}(G)}(R_2)$ and $\sigma_1 \in \mathrm{N}_{\mathrm{Aut}(G)}(S_2)$, we have

$$R_1 R_2 S_2 \,\mathrm{Inn}(G) \leq D(G).$$

Notice that $\theta(a_1^p) = a_1^p$ for each $\theta \in R_2 S_2 \,\mathrm{Inn}(G)$. On the other hand, since $|a_1| = p^{n_1+1} \geq p^3$, we have

$$\sigma_1(a_1^p) = a_1^{p+p^2} \neq a_1^p.$$

Therefore, $\sigma_1 \notin R_2 S_2 \,\mathrm{Inn}(G)$, and hence $R_2 S_2 \,\mathrm{Inn}(G) < R_1 R_2 S_2 \,\mathrm{Inn}(G)$. Consequently, we obtain

$$|R_1 R_2 S_2 \,\mathrm{Inn}(G)| \geq p\, |R_2 S_2 \,\mathrm{Inn}(G)|.$$

Then it follows that

$$|R_1 R_2 S_2 \,\mathrm{Inn}(G)| \geq \frac{p\, |\Omega_{n_2}\big(\mathrm{C}_G(L_2)\big)|\; |G/\mathrm{Z}(G)|}{|\,\mathrm{Im}(\rho_2)|} = |\Omega_{n_2}\big(\mathrm{C}_G(L_2)\big)|\; |G/\mathrm{Z}(G)|.$$

Since $|\,\mathrm{Z}(G)|$ divides $|\Omega_{n_2}\big(\mathrm{C}_G(L_2)\big)|$, the proof of the theorem is complete. □

The next result is a reformulation of a result of Ree [101, Theorem 1].

Theorem 4.46 *Let G be a non-abelian finite p-group of order greater than p^2 and of exponent p. Then $|G|$ divides $|\,\mathrm{Aut}(G)|$.*

Proof Let N be a maximal subgroup of G containing $\mathrm{Z}(G)$ such that $G/N = \langle Na \rangle$ is cyclic of order p for some $a \in G$. It follows that $\mathrm{Z}(G) \leq \mathrm{Z}(N)$. Define a map $\eta : \mathrm{Z}(N) \to \mathrm{Z}(N)$ by

$$\eta(z) = zaz^{-1}a^{-1}$$

for $z \in \mathrm{Z}(N)$. It is easy to see that η is a group homomorphism. Since $\mathrm{Z}(G) \leq \mathrm{Ker}(\eta)$, it follows that $|\,\mathrm{Z}(G)|$ divides $|\,\mathrm{Z}(N)/\,\mathrm{Im}(\eta)|$.

By Lemma 4.10, for each $z \in \mathrm{Z}(N)$, the map $\theta_z : G \to G$ defined by

$$\theta_z(xa^i) = x(za)^i,$$

for $x \in N$ and $1 \leq i \leq p$, is an automorphism of G centralising N. Thus, we get a map $\Phi : \mathrm{Z}(N) \to \mathrm{Aut}(G)$ given by

$$\Phi(z) = \theta_z$$

for $z \in \mathrm{Z}(N)$. It is easy to check that Φ is an injective group homomorphism.

Next we claim that

$$\mathrm{Im}(\Phi) \cap \mathrm{Inn}(G) = \mathrm{Im}(\Phi\eta).$$

If $\Phi(z) = \iota_g$ for some $g = xa^i \in G$, then

$$g = \theta_z(g) = x(za)^i,$$

and hence $(za)^i = a^i$. If $i \neq p$, then $za = a$, and hence $z = 1$. In this case, $\Phi(z)$, being trivial, obviously lies in $\mathrm{Im}(\Phi\eta)$. If $i = p$, then $g = x \in N$. Since

$$n = \theta_z(n) = xnx^{-1}$$

for all $n \in N$, we have $x \in \mathrm{Z}(N)$. Now

$$za = \theta_z(a) = xax^{-1}$$

implies that $z = \eta(x)$, which yields $\Phi(z) \in \mathrm{Im}(\Phi\eta)$. Conversely, for each $z \in \mathrm{Z}(N)$, we see that $\Phi\eta(z)$ is the inner automorphism induced by z, and hence the claim is proved.

Now consider

$$\begin{aligned}\mathrm{Im}(\Phi)\,\mathrm{Inn}(G)/\,\mathrm{Inn}(G) &\cong \mathrm{Im}(\Phi)/\big(\mathrm{Im}(\Phi) \cap \mathrm{Inn}(G)\big)\\ &\cong \mathrm{Im}(\Phi)/\,\mathrm{Im}(\Phi\eta)\\ &\cong \mathrm{Z}(N)/\,\mathrm{Im}(\eta), \text{ since } \Phi \text{ is injective.}\end{aligned}$$

As $\mathrm{Im}(\Phi)\,\mathrm{Inn}(G)/\,\mathrm{Inn}(G) \leq \mathrm{Aut}(G)/\,\mathrm{Inn}(G)$ and $|\,\mathrm{Z}(G)|$ divides $|\,\mathrm{Z}(N)/\,\mathrm{Im}(\eta)|$, it follows that $|G|$ divides $|\,\mathrm{Aut}(G)|$. □

Notice that, if $\exp(G) = p$, then $\Omega_1\big(\mathrm{Z}(G)\big) = \mathrm{Z}(G)$. Thus, the preceding theorem actually proves that $|G|$ divides $|D(G)|$.

We need the following result for the case $\exp(G) = \exp\big(\mathrm{Z}(G)\big) = p^{m+1}$.

Lemma 4.47 *Let G be a p-abelian p-group such that* $\exp(G) = p^{m+1}$, *where* $m \geq 1$. *Let*

$$\mho_1(G) = \langle a_1^p \rangle \oplus \cdots \oplus \langle a_t^p \rangle,$$

where the order of a_i is p^{n_i+1} for $1 \leq i \leq t$. If $a_j \in \mathrm{Z}(G)$ for some fixed j, then the following statements hold:

(1) If $\theta \in \mathrm{Aut}^{\Omega_1(\mathrm{Z}(L_j))}(L_j)$, then the map $\tilde{\theta} : G \to G$ given by

$$\tilde{\theta}(la_j^k) = \theta(l)a_j^k$$

for all $0 \leq k < p^{n_j}$ and $l \in L_j$, defines an automorphism of G extending θ.

(2) If $V_j = \big\{\tilde{\theta} \mid \theta \in \mathrm{Aut}^{\Omega_1(\mathrm{Z}(L_j))}(L_j)\big\}$, then $V_j \leq D(G)$ and

$$|V_j| = |\,\mathrm{Aut}^{\Omega_1(\mathrm{Z}(L_j))}(L_j)|.$$

(3) $R_jV_j \leq D(G)$ and $|R_jV_j| = p^{n_j}|V_j|$.

Proof Since $L_j \cap \langle a_j \rangle = \langle a_j^{p^{n_j}} \rangle$ and $\theta(a_j^{p^{n_j}}) = a_j^{p^{n_j}}$, it follows that $\tilde{\theta}$ is well-defined. Further, $G = L_j \langle a_j \rangle$ implies that $\tilde{\theta}$ extends to an automorphism of G, proving assertion (1).

Since $\Omega_1\big(\mathrm{Z}(G)\big) \leq \Omega_1\big(\mathrm{Z}(L_j)\big)$, we have $V_j \leq D(G)$. It is clear that $|V_j| = |\operatorname{Aut}^{\Omega_1\left(\mathrm{Z}(L_j)\right)}(L_j)|$, which proves assertion (2).

Observe that $R_j \leq \mathrm{C}_{\operatorname{Aut}(G)}(V_j)$, and hence $R_j V_j \leq D(G)$. Further, if $\alpha \in R_j \cap V_j$, then $\alpha(a_j) = a_j$ and $\alpha(l) = l$ for all $l \in L_j$, and hence $\alpha = 1$. Finally $|R_j V_j| = p^{n_j}|V_j|$ by Remark 4.42(1), and the proof is complete. □

With this information in hand, we prove the following

Theorem 4.48 *Let G be a finite non-abelian p-abelian p-group such that*

$$\exp(G) = \exp\big(\mathrm{Z}(G)\big) = p^{m+1},$$

where $m \geq 1$. Then $|G|$ divides $|D(G)|$.

Proof Notice that $\mho_1(G)$ is non-trivial. Recall the decomposition of $\mho_1(G)$ from Lemma 4.47. We now proceed by induction on t.

If $t = 1$, then $\mho_1(G)$ is cyclic of order p^{n_1}. Choose $a_1 \in \mathrm{Z}(G)$ such that the order of a_1 is p^{n_1+1}. Then we have $\mho_1(G) = \langle a_1^p \rangle$. Thus,

$$L_1 = \Omega_1(G)$$

and

$$G/\Omega_1(G) = \langle \Omega_1(G) a_1 \rangle,$$

the latter being cyclic of order p^{n_1}. Since G is non-abelian and $a_1 \in \mathrm{Z}(G)$, it follows that $\Omega_1(G)$ is non-abelian group of exponent p. Thus, it follows from Theorem 4.46 that $|\Omega_1(G)|$ divides $|D\big(\Omega_1(G)\big)|$. Now consider

$$V_1 = \left\{\tilde{\theta} \mid \theta \in \operatorname{Aut}^{\Omega_1\left(\mathrm{Z}(\Omega_1(G))\right)}\big(\Omega_1(G)\big)\right\}$$

as defined in Lemma 4.47(2). Since $|G| = p^{n_1}|\Omega_1(G)|$, by Lemma 4.47(3), we see that $|G|$ divides $|D(G)|$.

Now assume that the theorem holds for $t - 1$, where $t \geq 2$. Choose $a_1 \in \mathrm{Z}(G)$ of order p^{n_1+1} and $a_2, \ldots, a_t \in G$ such that the order a_i is p^{n_i} and

$$\mho_1(G) = \langle a_1^p \rangle \oplus \cdots \oplus \langle a_t^p \rangle.$$

Then $G/L_1 = \langle L_1 a_1 \rangle$ is cyclic of order p^{n_1}. Since $a_1 \in \mathrm{Z}(G)$, it follows that L_1 is a non-abelian p-abelian p-group of exponent at least p^2 such that

$$\mho_1(L_1) = \langle a_2^p \rangle \oplus \cdots \oplus \langle a_t^p \rangle.$$

If $\exp\big(\mathrm{Z}(L_1)\big) = \exp\big(\mho_1(L_1)\big)$, then, by Theorem 4.44, $|L_1|$ divides $|\operatorname{Aut}^{\Omega_1(\mathrm{Z}(L_1))}(L_1)|$. If $\exp\big(\mathrm{Z}(L_1)\big) = \exp(L_1)$, then, by the induction hypothesis, $|L_1|$ again divides $|\operatorname{Aut}^{\Omega_1\left(\mathrm{Z}(L_1)\right)}(L_1)|$. Considering V_1 as defined in Lemma 4.47, we see that

$$|D(G)| \geq |R_1V_1| = p^{n_1}|V_1| = p^{n_1}|\operatorname{Aut}^{\Omega_1\left(\mathrm{Z}(L_1)\right)}(L_1)| \geq p^{n_1}|L_1| = |G|,$$

and the proof is complete. □

Putting all the pieces together, we obtain the following result of Davitt [19, Theorem 3].

Theorem 4.49 *Let G be a finite non-abelian p-abelian p-group. Then $|G|$ divides $|\operatorname{Aut}(G)|$.*

4.6 Groups with Small Central Quotient

In this section, we show that finite non-abelian p-groups G with $|G/\mathrm{Z}(G)| \leq p^4$ satisfy Divisibility Property [20].

We begin with the special case when G is regular. See Sect. 1.2 of Chap. 1 for the definition.

Proposition 4.50 *Let G be a non-abelian regular p-group with $|G/\mathrm{Z}(G)| \leq p^4$. Then $|G|$ divides $|\operatorname{Aut}(G)|$.*

Proof Since regular 2-groups are abelian, p must be an odd prime. If G is p-abelian, then the result follows from Theorem 4.49.

Assume that G is not p-abelian. Then there exist at least two elements x and y in G such that $[x, y]^p \neq 1$. From the regularity of G, it follows that none of the two elements $[x^p, y]$ and $[x, y^p]$ is trivial, which implies that both x^p and y^p lie outside $\mathrm{Z}(G)$ and $x^p \neq y^p$ modulo $\mathrm{Z}(G)$. Since $|G/\mathrm{Z}(G)| \leq p^4$, we must have $|G/\mathrm{Z}(G)| = p^4$. Notice that $|\mho_1\big(G/\mathrm{Z}(G)\big)| = p^2$. Hence, by Proposition 1.10, $G/\mathrm{Z}(G)$ is metacyclic, and the result follows by Theorem 4.20. □

Before proceeding further, we list all possible reductions on our group. Notice that, since G is non-abelian, $|G/\mathrm{Z}(G)| \geq p^2$. If $|G/\mathrm{Z}(G)| = p^2$, then G is of nilpotency class 2, and the result follows from Theorem 4.17. Therefore, we assume that

$$p^3 \leq |G/\mathrm{Z}(G)| \leq p^4.$$

Further, by Theorem 4.17, we assume that G has nilpotency class greater than 2, and hence the nilpotency class of G is either 3 or 4. By Theorem 4.20, we assume that $G/\mathrm{Z}(G)$ is not metacyclic. Let us set

$$\exp(G) = p^m.$$

In view of Theorem 4.49, we assume that G is not p-abelian, and therefore $m \geq 2$. Additionally, by Remark 4.5, we assume that

$$\mathrm{Z}(G) \leq \Phi(G).$$

It follows that $d(G) = d(H)$, which is either 2 or 3. Finally, if $p \geq 5$, then G is regular and the result follows from Proposition 4.50. Therefore, we assume that $p = 2, 3$.

We first take up the case $p = 3$.

Proposition 4.51 *Let G be a 3-group such that $|G/\mathrm{Z}(G)| = 3^3$. Then $|G|$ divides $|\operatorname{Aut}(G)|$.*

Proof Since $H := G/\mathrm{Z}(G)$ is neither abelian nor metacyclic, it follows that H is an extraspecial 3-group of exponent 3 and $d(H) = 2$. Notice that $G = \langle a, b\rangle$ for some $a, b \in G$, and the nilpotency class of G is 3. Further, by Theorem 1.31(2), we have $\exp\big(\gamma_3(G)\big) = 3$, and a simple computation yields

$$1 = [a^3, b] = [a, b]^3[a, b, a]^3[a, b, a, a] = [a, b]^3.$$

Since G is generated by two elements, it easily follows that (see [52, Theorem 2.81])

$$\gamma_2(G) = \langle [a, b], \gamma_3(G)\rangle.$$

Consequently, $\exp\big(\gamma_2(G)\big) = 3$. By Theorem 1.31(3), $\Phi(G)$ is regular. Therefore, by Theorem 1.27, we get $\exp\big(G/\gamma_2(G)\big) \geq \exp\big(\mathrm{Z}(G)\big)$. Since

$$|\operatorname{Hom}\big(G/\gamma_2(G),\ \mathrm{Z}(G)\big)| \geq 3\,|\mathrm{Z}(G)|,$$

we obtain

$$|\operatorname{IC}(G)| = |\operatorname{Hom}\big(G/\gamma_2(G),\ \mathrm{Z}(G)\big)|\,|G/\mathrm{Z}_2(G)| \geq 3^3\,|\mathrm{Z}(G)| = |G|,$$

and the proof is complete. □

Recall that a group K is said to be *capable* if there exists a group G such that

$$K \cong G/\mathrm{Z}(G).$$

We refer the reader to [7] for some foundational results on capable groups. The following result [115, 3.2.10] gives a necessary condition for a group to be capable.

Theorem 4.52 *If G is a group containing a non-identity element w and a generating set S such that some power of each element in S equals w, then G is not capable.*

Proposition 4.53 *Let G be a 3-group such that $|G/\mathrm{Z}(G)| = 3^4$. Then $|G|$ divides $|\operatorname{Aut}(G)|$.*

Proof Let $H := G/\mathrm{Z}(G)$. We have two cases: (1) $d(G) = 3$; (2) $d(G) = 2$.

Case(1): If $|\mathrm{Z}(H)| = 3$, then H must be extraspecial, which is not possible. Hence, we have $|\mathrm{Z}(H)| = 3^2$. In this case H must be regular and $|G/\mathrm{Z}_2(G)| = 3^2$. Indeed, since $|\gamma_2(H)| = 3$, H is 3-abelian.

If $\exp(H) = 3$, then $G = \langle a, b, c\rangle$ such that the order of all three elements $\mathrm{Z}(G)a$, $\mathrm{Z}(G)b$ and $\mathrm{Z}(G)c$ is 3. It is an easy exercise to prove that

$$\gamma_2(G) = \langle [a, b], [a, c], [b, c], \gamma_3(G)\rangle.$$

Since the nilpotency class of G is 3 and $\exp\big(\gamma_3(G)\big) = 3$, we have $\exp\big(\gamma_2(G)\big) = 3$. By Theorem 1.31(3), $\Phi(G)$ is regular. It follows from Theorem 1.27 that $\exp\big(G/\gamma_2(G)\big) \geq \exp\big(\mathrm{Z}(G)\big)$. Therefore, since

$$|\operatorname{Hom}\big(G/\gamma_2(G),\ \mathrm{Z}(G)\big)| \geq 3^2\,|\mathrm{Z}(G)|,$$

we obtain

$$|\mathrm{IC}(G)| \geq 3^4\,|\mathrm{Z}(G)| = |G|.$$

If $\exp(H) = 3^2$, then we can take $H = \langle x, y, w\rangle$ with x of order 3^2 and $\mho_1(G) = \langle x^3\rangle$. Since H is regular, without loss of generality, we can assume that the order of both y and w is 3^2. So there is a generating set for H such that some power of each element in it equals x^3. Thus, by Theorem 4.52, H is not capable, and therefore this case does not arise.

Case (2): Let $G = \langle a, b\rangle$. Suppose that $|G/\mathrm{Z}_2(G)| = 3^3$. If $\mathrm{Z}(G)$ is non-cyclic or $\exp\big(G/\gamma_2(G)\big) \geq \exp\big(\mathrm{Z}(G)\big)$, then $|\mathrm{IC}(G)| \geq |G|$, and we are done.

So we assume that $\mathrm{Z}(G)$ is cyclic and

$$\exp\big(G/\gamma_2(G)\big) < \exp\big(\mathrm{Z}(G)\big).$$

Thus, by Theorem 1.27, we have $\exp\big(\gamma_2(G)\big) = 3^2$. Since $\gamma_2(G) = \langle [a, b], \gamma_3(G)\rangle$, $\mho_1\big(\gamma_2(G)\big) \leq \mathrm{Z}(G)$ and $\exp\big(\gamma_3(G)\big) = 3$, it follows that $\langle [a, b]^3\rangle$ is the unique subgroup of $\mathrm{Z}(G)$ of order 3 and

$$|\gamma_2(G)| = 3\,|\gamma_3(G)|.$$

Notice that $|\gamma_2(G) \cap \mathrm{Z}(G)| = 3$. If the nilpotency class of G is 3, then $\gamma_2(G)$ must be cyclic of order 3^2, which is not possible as G is non-regular. If the nilpotency class of G is 4, then

$$|\gamma_2(G)| = 3\,|\gamma_3(G)\,\mathrm{Z}(G)/\mathrm{Z}(G)|\,|\gamma_3(G) \cap \mathrm{Z}(G)| = 3^3.$$

Now suppose that $\exp(G) = 3^m$, where $m \geq 2$. If $m = 2$, then, since $\exp\big(G/\gamma_2(G)\big) < \exp\big(\mathrm{Z}(G)\big)$, it follows that $\exp\big(G/\gamma_2(G)\big) = 3$ and $\exp\big(\mathrm{Z}(G)\big) = 3^2$. On one hand, we have

$$|G| = |H|\,|\mathrm{Z}(G)| = 3^6.$$

On the other hand,

$$|G| = |G/\gamma_2(G)|\,|\gamma_2(G)| = 3^5,$$

which is a contradiction. Hence, $m > 2$, and it follows that $\exp\big(G/\gamma_2(G)\big) = 3^{m-2}$ and $\exp\big(\mathrm{Z}(G)\big) = p^{m-1}$. If

$$G/\gamma_2(G) = \mathrm{C}_{3^{m-2}} \oplus \mathrm{C}_3,$$

then

$$|G| = |G/\gamma_2(G)|\,|\gamma_2(G)| = 3^{m+2}.$$

Also, we have $|G| = |H|\,|\mathrm{Z}(G)| = 3^{m+3}$, which is not possible. So we must have

$$G/\gamma_2(G) = \mathrm{C}_{3^{m-2}} \oplus \mathrm{C}_{3^2},$$

and hence

$$|\,\mathrm{IC}(G)| = 3^{m+3} = |G|.$$

Finally, assume that $|G/\mathrm{Z}_2(G)| = 3^2$. Then $|\,\mathrm{Z}(H)| = 3^2$, the nilpotency class of H is 2, and so H is regular. Notice that $|\mho_1(H)| \le 3$, otherwise H is metacyclic. If $|\mho_1(H)| = 1$, then $\mathrm{Z}(H) = \gamma_2(H)$ is cyclic of order 3^2, which is absurd. Hence, $|\mho_1(H)| = 3$, and therefore there exists an element $x \in G$ having order 3^2. We can always choose another element y of order 3^2 such that $H = \langle x, y\rangle$ and $y^3 = x^3$. Hence, H is not capable by Theorem 4.52, and this case cannot occur, completing the proof of the proposition. □

We now move to 2-groups.

Proposition 4.54 *Let G be a 2-group such that $|G/\mathrm{Z}(G)| = 2^3$. Then $|G|$ divides $|\,\mathrm{Aut}(G)|$.*

Proof There are only two non-abelian groups of order 2^3 and both of these are 2-generator metacyclic groups having elements of order 2^2.

Assume that $G = \langle a, b\rangle$, where the orders of $\mathrm{Z}(G)a$ and $\mathrm{Z}(G)b$ respectively are 2^2 and 2, and $\langle \mathrm{Z}(G)a\rangle$ is normal subgroup of $G/\mathrm{Z}(G)$ with index 2. Then, by Exercise 1.28, for $A = \langle a, \mathrm{Z}(G)\rangle$, we get

$$|A| = |\gamma_2(G)|\,|\mathrm{Z}(G)|.$$

On the other hand $|A| = 2^2\,|\mathrm{Z}(G)|$, and hence $|\gamma_2(G)| = 2^2$ and $|G/\gamma_2(G)| = 2\,|\mathrm{Z}(G)|$. Now $\exp\big(G/\gamma_2(G)\big) < \exp\big(\mathrm{Z}(G)\big)$ or $\exp\big(G/\gamma_2(G)\big) \ge \exp\big(\mathrm{Z}(G)\big)$. Since $|G/\mathrm{Z}_2(G)| = 2^2$, in both the cases, we obtain $|\,\mathrm{IC}(G)| \ge |G|$, and the proof is complete. □

For the remaining case when $|G/\mathrm{Z}(G)| = |H| = 2^4$, we use the classification of non-abelian groups of order 2^4 from Hall-Senior [54]. There are 9 such groups

H listed as follows in terms of their presentation together with some other relevant information.

$$\begin{aligned} H &= \langle x, y, w \mid x^4, y^2, w^2, [x, y] = x^2 \rangle, \\ \gamma_2(H) &= \langle x^2 \rangle,\ \ \mathrm{Z}(H) = \langle x^2 \rangle \oplus \langle w \rangle. \end{aligned} \tag{4.55}$$

$$\begin{aligned} H &= \langle x, y, w \mid x^4, y^4, w^2, [x, y] = x^2 = y^2 \rangle, \\ \gamma_2(H) &= \langle x^2 \rangle,\ \ \mathrm{Z}(H) = \langle x^2 \rangle \oplus \langle w \rangle. \end{aligned} \tag{4.56}$$

$$\begin{aligned} H &= \langle x, y, w \mid x^2, y^2, w^4, [x, y] = w^2 \rangle, \\ \gamma_2(H) &= \langle w^2 \rangle,\ \ \mathrm{Z}(H) = \langle w \rangle. \end{aligned} \tag{4.57}$$

$$\begin{aligned} H &= \langle x, y \mid x^2, y^4, [x, y]^2 \rangle, \\ \gamma_2(H) &= \langle [x, y] \rangle,\ \ \mathrm{Z}(H) = \langle [x, y] \rangle \oplus \langle y^2 \rangle. \end{aligned} \tag{4.58}$$

$$\begin{aligned} H &= \langle x, y \mid x^4, y^4, [x, y] = x^2 \rangle, \\ \gamma_2(H) &= \langle x^2 \rangle,\ \ \mathrm{Z}(H) = \langle x^2 \rangle \oplus \langle y^2 \rangle. \end{aligned} \tag{4.59}$$

$$\begin{aligned} H &= \langle x, y \mid x^2, y^8, [x, y] = y^4 \rangle, \\ \gamma_2(H) &= \langle y^4 \rangle,\ \ \mathrm{Z}(H) = \langle y^2 \rangle. \end{aligned} \tag{4.60}$$

$$\begin{aligned} H &= \langle x, y \mid x^8, y^2, [x, y]^{-1} = x^2 \rangle, \\ \gamma_2(H) &= \langle [x, y] \rangle = \mathrm{Z}_2(H),\ \ \mathrm{Z}(H) = \langle [x, y]^2 \rangle = \gamma_3(H). \end{aligned} \tag{4.61}$$

$$\begin{aligned} H &= \langle x, y \mid x^8, y^2, [x, y] = x^2 \rangle, \\ \gamma_2(H) &= \langle [x, y] \rangle = \mathrm{Z}_2(H),\ \ \mathrm{Z}(H) = \langle [x, y]^2 \rangle = \gamma_3(H). \end{aligned} \tag{4.62}$$

$$\begin{aligned} H &= \langle x, y \mid x^8, y^4, [x, y]^{-1} = x^2, [x, y]^2 = y^2 \rangle, \\ \gamma_2(H) &= \langle [x, y] \rangle = \mathrm{Z}_2(H),\ \ \mathrm{Z}(H) = \langle [x, y]^2 \rangle = \gamma_3(H). \end{aligned} \tag{4.63}$$

By suitably modifying the generating sets, the following result is a direct consequence of Theorem 4.52.

Lemma 4.64 *The groups* (4.56), (4.57), (4.59), (4.60), (4.62) *and* (4.63) *are not capable.*

Proposition 4.65 *Let G be a 2-group such that $|G/\mathrm{Z}(G)| = 2^4$. Then $|G|$ divides $|\operatorname{Aut}(G)|$.*

Proof In view of Lemma 4.64, we only need to consider groups (4.55), (4.58) and (4.61) from the preceding list.

Group (4.55): Since $\exp\big(\gamma_2(H)\big) = 2$, it follows from Theorem 1.30 that $\exp\big(\gamma_3(G)\big) = 2$ and

$$\mho_1\big(\gamma_2(G)\big) \le \mathrm{Z}(G).$$

Thus, we have $|G/\mathrm{Z}_2(G)| = 2^2$, $|\gamma_2(G)\,\mathrm{Z}(G)/\mathrm{Z}(G)| = 2$ and the nilpotency class of G is 3. Consequently, $\Phi(G)$ is abelian. By Theorem 1.30(2), we have $\exp\big(\gamma_2(G)\big) \le 2^2$. If $\exp\big(\gamma_2(G)\big) = 2$, then by Theorem 1.27 we get

$$\exp\big(G/\gamma_2(G)\big) \ge \exp\big(\mathrm{Z}(G)\big).$$

And, if $\exp\big(\gamma_2(G)\big) = 2^2$, then by Theorem 1.27, we have $\exp\big(G/\gamma_2(G)\big) \ge \exp\big(\mathrm{Z}(G)\big)/2$.

If either $\mathrm{Z}(G)$ is not cyclic or $\exp\big(G/\gamma_2(G)\big) \ge \exp\big(\mathrm{Z}(G)\big)$, then it follows that $|\,\mathrm{IC}(G)| \ge |G|$. Thus, we assume that $\mathrm{Z}(G)$ is cyclic and $\exp\big(G/\gamma_2(G)\big) < \exp\big(\mathrm{Z}(G)\big)$. Then, by Theorem 1.27, we have $\exp\big(\gamma_2(G)\big) = 2^2$. Since $|G/\mathrm{Z}_2(G)| = 2^2$, we only need to show that $|\gamma_2(G)| = 2^2$. Let

$$G = \langle a, b, c\rangle$$

such that the order of $\mathrm{Z}(G)c$ is 2 and $c \in \mathrm{Z}_2(G)$. Then it follows that $[a, c]$ and $[b, c]$ both lie in $\Omega_1\big(\mathrm{Z}(G)\big)$. Since

$$\gamma_2(G) = \langle [a, b], [a, c], [b, c], \gamma_3(G)\rangle,$$

it follows that $[a, b]$ is of order 2^2. Since $\mho_1\big(\gamma_2(G)\big) \le \mathrm{Z}(G)$, we have $\Omega_1\big(\mathrm{Z}(G)\big) = \langle [a, b]^2\rangle$. Hence, $\gamma_2(G) = \langle [a, b]\rangle$ is cyclic of order 2^2, and the proof in this case is complete.

Group (4.58): Let $G = \langle a, b\rangle$, where $\mathrm{Z}(G)a = x$ and $\mathrm{Z}(G)b = y$. It follows that $\exp\big(\gamma_3(G)\big) = 2$, $\mho_1\big(\gamma_2(G)\big) \le \mathrm{Z}(G)$, $|G/\mathrm{Z}_2(G)| = 2^2$, $|\gamma_2(G)\,\mathrm{Z}(G)/\mathrm{Z}(G)| = 2$, $\Phi(G) = \langle [a, b], b^2, \mathrm{Z}(G)\rangle$ and the nilpotency class of G is 3. Since $b^2 \in \mathrm{Z}_2(G)$, it follows that $\Phi(G)$ is abelian. By Theorem 1.30(2), we obtain $\exp\big(\gamma_2(G)\big) \le 2^2$. An easy exercise shows that

$$\gamma_2(G) = \langle [a, b], [a, b, a], [a, b, b]\rangle,$$

where only $[a, b]$ could possibly have order 2^2. Since the order of a modulo $\mathrm{Z}(G)$ is 2, we have

$$1 = [a^2, b] = [a, b]^2[a, b, a].$$

Thus, $[a, b, a] \in \langle [a, b]\rangle$, and therefore $|\gamma_2(G)| \le 2^3$. We now have two cases: (1) $\mathrm{Z}(G)$ is cyclic; (2) $\mathrm{Z}(G)$ is not cyclic.

Case (1): In this case, since $\gamma_2(G) = \langle [a, b], [a, b, b]\rangle$, we have $|\gamma_2(G)| = 2^2$. Next we claim that $\exp\big(\gamma_2(G)\big) = 2$. If not, then the order of $[a, b]$ is 2^2. If $[a, b, b] \ne 1$, then $[a, b, b] = [a, b]^2$. Further we have

$$[a, b^2] = [a, b]^2[a, b, b] = [a, b]^4 = 1,$$

which implies that $b^2 \in \mathrm{Z}(G)$, which is not true. Hence, $[a, b, b] = 1$. Then $B := \langle [a, b], b, \mathrm{Z}(G)\rangle$ is an abelian normal subgroup of index 2 in G. Thus, $|B| = 2^3|\,\mathrm{Z}(G)|$. On the other hand, by Exercise 1.28, we get

$$|B| = |\gamma_2(G)|\,|B \cap Z(G)| = 2^2\,|Z(G)|,$$

a contradiction. Hence, $\exp\big(\gamma_2(G)\big) = 2$ and consequently $[a, b, a] = 1$.

Since $|\,Z(G)| > 2$ and $Z(G) \leq \mho_1\big(\gamma_2(G)\big)$, it follows that $\exp\big(Z(G)\big) \leq 2^{m-1}$ and $m > 2$. Let $g \in G$ be of maximal order. Since $g^4 \in Z(G)$, we have $g^{2^{m-1}} \in Z(G) \cap \gamma_2(G)$, which is the unique subgroup of $Z(G)$ of order 2. Thus, $\exp\big(G/\gamma_2(G)\big) = 2^{m-1}$. Similarly, $\exp\big(Z(G)\big) = |\,Z(G)| \geq 2^{m-2}$. If $|\,Z(G)| = 2^{m-1}$, then

$$|\,\mathrm{IC}(G)| \geq 2^2\,|G/\gamma_2(G)| = |G|.$$

Assume that $Z(G)$ is cyclic of order 2^{m-2}. Then it follows that $Z(G) \leq \mho_2\big(\gamma_2(G)\big)$. Let $Z(G) = \langle vw^4\rangle$, where $v \in \gamma_2(G)$ and $w \in G$. As $a^2 \in Z(G)$, we have $a^2 = v^i w^{4j}$ for some integers i and j. If $a' := aw^{-2j}$, then $a'^4 = 1$. Since $w^{-2j} \in \Phi(G)$, $G = \langle a', b\rangle$. Therefore, without loss of generality, we can assume that $G = \langle a, b\rangle$ such that the order of a is at most 2^2. Then

$$A := \langle [a, b], a, Z(G)\rangle$$

is an abelian normal subgroup of G such that $G/A = \langle Ab\rangle$ is cyclic of order 2^2. Now it follows from Lemma 4.10 that the map $\phi : G \to G$ defined by

$$\phi(b) = ab \text{ and } \phi(u) = u$$

for all $u \in A$, extends to an automorphism of G centralising A, and the order of ϕ is equal to the order of a. Since $a \notin \gamma_2(G)\,Z(G)$, it follows that ϕ is a non-trivial 2-power automorphism which is not in $\mathrm{IC}(G)$. Hence,

$$|\,\mathrm{Aut}(G)|_p \geq |\langle \phi, \mathrm{IC}(G)\rangle| \geq 2\,|\,\mathrm{IC}(G)| = 2^4\,|\,Z(G)| = |G|,$$

and the proof in complete in this case.

Case (2): In this case, if $\exp\big(G/\gamma_2(G)\big) \geq \exp\big(Z(G)\big)$, then

$$|\,\mathrm{IC}(G)| \geq 2^4\,|\,Z(G)| = |G|.$$

Similarly, if $\exp\big(G/\gamma_2(G)\big) = \exp\big(Z(G)\big)/2$, then

$$|\,\mathrm{IC}(G)| \geq 2^3\,|G/\gamma_2(G)| \geq |G|,$$

and we are done.

Group (4.61): In this case, $G = \langle a, b\rangle$, where the order of $Z(G)a$ is 2^3 and $|G/Z_2(G)| = 2^3$. Then $A := \langle a, Z(G)\rangle$ is an abelian normal subgroup of G with index 2. By Exercise 1.28, we have

$$2^3\,|\,Z(G)| = |A| = |\gamma_2(G)|\,|\,Z(G)|,$$

and hence $|\gamma_2(G)| = 2^3$. If $\exp\big(G/\gamma_2(G)\big) \geq \exp\big(\mathrm{Z}(G)\big)$, then

$$|\operatorname{IC}(G)| \geq 2^4\,|\mathrm{Z}(G)| = |G|.$$

Similarly, if $\exp\big(G/\gamma_2(G)\big) < \exp\big(\mathrm{Z}(G)\big)$, then

$$|\operatorname{IC}(G)| \geq 2^3\,|G/\gamma_2(G)| = |G|.$$

This completes the proof of the proposition. □

Combining Propositions 4.50, 4.51, 4.53, 4.54, 4.65, we have proved the following result of Davitt [20].

Theorem 4.66 *Let G be a non-abelian finite p-group with $|G/\mathrm{Z}(G)| \leq p^4$. Then $|G|$ divides $|\operatorname{Aut}(G)|$.*

As a consequence of the preceding theorem and Theorem 1.32, we readily get

Corollary 4.67 *Let G be a non-cyclic finite p-group such that $p^3 \leq |G| \leq p^6$. Then $|G|$ divides $|\operatorname{Aut}(G)|$.*

Chapter 5
Groups with Divisibility Property-II

This chapter is a continuation of the previous chapter on Divisibility Property. In the first three sections, we deal with groups of order p^7 [41], groups of coclass 2 [35] and 2-groups with a given coclass [26]. Section 5.4 deals with p^2-abelian p-central p-groups [121]. Finally, in Sect. 5.5, results with certain specific conditions on groups are presented [30, 34, 128].

5.1 Groups of Order p^7

In view of Corollary 4.67, to study Divisibility Property, it is enough to consider p-groups of order greater than p^6. That p-groups of order p^7 admit Divisibility Property was established by Gavioli [41], which we present in this section.

We begin with the following result, which is an immediate consequence of [17, Theorem 3.2], whose proof is purely module-theoretic.

Lemma 5.1 *Let $G = \langle a, b\rangle$ be a two-generated metabelian p-group. Then for all $u, v \in \gamma_2(G)$, there exists an automorphism of G mapping a to au and b to bv. In particular, $|\gamma_2(G)|^2$ divides $|\operatorname{Aut}(G)|$.*

For the rest of this section, we assume that G is a p-group of order p^7. In addition, we assume that G satisfies the following hypotheses:

(i) p is an odd prime (For $p = 2$, it is proved in [95] that $|G|$ divides $|\operatorname{Aut}(G)|$, which can also be verified using a direct GAP calculation [38]).

(ii) G is purely non-abelian of nilpotency class greater than 2 such that $\Omega_1\big(\mathrm{Z}(G)\big) \leq \gamma_2(G)$ and $|\mathrm{Z}(G)| = p^2$ (In view of Remarks 4.3 and 4.7, Theorems 4.17 and 4.66).

(iii) If G is 2-generated and metabelian, then $|\gamma_2(G)| \leq p^3$ (By Lemma 5.1).

The main result of this section is the following theorem of Gavioli [41], which is a consequence of the next four results depending on the structure of $\mathrm{Z}(G)$ and the number of generators of G.

I. B. S. Passi et al., *Automorphisms of Finite Groups*, Springer Monographs in Mathematics, https://doi.org/10.1007/978-981-13-2895-4_5

Theorem 5.2 *If G is a non-abelian p-group of order p^7, then $|G|$ divides $|\operatorname{Aut}(G)|$.*

We begin with the case when the center is elementary abelian.

Theorem 5.3 *If G is a non-abelian p-group of order p^7 with $\mathrm{Z}(G) = \mathrm{C}_p \oplus \mathrm{C}_p$, then $|G|$ divides $|\operatorname{Aut}(G)|$.*

Proof If $|\operatorname{Hom}\big(G/\gamma_2(G),\ \mathrm{Z}(G)\big)| \geq |\mathrm{Z}_2(G)|$, then

$$|\operatorname{IC}(G)| = \frac{|\operatorname{Hom}\big(G/\gamma_2(G),\ \mathrm{Z}(G)\big)|\,|G|}{|\mathrm{Z}_2(G)|} \geq |G|,$$

and we are done.

So assume that $|\operatorname{Hom}\big(G/\gamma_2(G),\ \mathrm{Z}(G)\big)| < |\mathrm{Z}_2(G)|$. Observe that G is generated by 2 elements. For, if G is generated by more than 2 elements, then $|\operatorname{Hom}\big(G/\gamma_2(G),\ \mathrm{Z}(G)\big)| \geq p^6$, which implies that $\mathrm{Z}_2(G) = G$, that is, G is nilpotent of class 2, a contradiction. Consequently, we have

$$|\operatorname{Hom}\big(G/\gamma_2(G),\ \mathrm{Z}(G)\big)| = p^4,$$

and hence $|\mathrm{Z}_2(G)| \geq p^5$. By Proposition 1.8(3), $\mathrm{Z}_2(G) \leq \Phi(G)$. Hence, $\mathrm{Z}_2(G) = \Phi(G)$, and consequently $|\mathrm{Z}_2(G)| = p^5$.

Since G is generated by 2 elements and is of nilpotency class 3, by Proposition 1.8(5), it is metabelian. By our assumption on G, $|\gamma_2(G)| \leq p^3$. Since

$$\mathrm{Z}(G) = \Omega_1\big(\mathrm{Z}(G)\big) \leq \gamma_2(G),$$

it follows that $|\gamma_2(G)| = p^3$. Notice that $\exp\big(G/\,\mathrm{Z}(G)\big) = p^2$, and hence

$$G/\gamma_2(G) \cong \mathrm{C}_{p^2} \oplus \mathrm{C}_{p^2}\,.$$

Suppose that $G = \langle x, y\rangle$. Observe that $\mathrm{Z}_2(G)$ is abelian and can be considered as a G-module via conjugation. Also $\gamma_2(G)$ acts trivially on $\mathrm{Z}_2(G)$, and hence $G/\gamma_2(G)$ acts on $\mathrm{Z}_2(G)$. Since the hypothesis of Proposition 2.13 holds, the map $\delta : G/\gamma_2(G) \to \mathrm{Z}_2(G)$ defined on generators by

$$\delta\big(\gamma_2(G)x\big) = y^p$$

and

$$\delta\big(\gamma_2(G)y\big) = 1$$

is a derivation. We lift δ to a derivation $\tilde{\delta} : G \to \mathrm{Z}_2(G)$ by setting

$$\tilde{\delta}(ug) = \delta\big(\gamma_2(G)g\big),$$

where $u \in \gamma_2(G)$ and g is a coset representative of $\gamma_2(G)$ in G. Further, notice that $\tilde{\delta}\big(\mathrm{Z}_2(G)\big) = 1$. Thus, by Proposition 2.14, $\tilde{\delta}$ defines an automorphism of G of p-power order, which is obviously non-inner and non-central. Since $|\operatorname{IC}(G)| = p^6$, we obtain $|\operatorname{Aut}(G)|_p \geq p^7$, and the proof is complete. □

We need the following basic result.

Proposition 5.4 *Let G be a group and A an abelian normal subgroup of G with $\mathrm{Z}(G) \leq A \leq \mathrm{Z}_2(G)$. Then there is an embedding of $A/\mathrm{Z}(G)$ into* $\operatorname{Hom}\big(G/A,\ \mathrm{Z}(G)\big)$.

Proof For $a \in A$, let $\bar{a} = \mathrm{Z}(G)a$. Consider the map

$$\theta : A/\mathrm{Z}(G) \to \operatorname{Hom}\big(G/A,\, \mathrm{Z}(G)\big)$$

by setting

$$\theta(\bar{a}) = \theta_{\bar{a}},$$

where $\theta_{\bar{a}} : G/A \to \mathrm{Z}(G)$ is the homomorphism given by

$$\theta_{\bar{a}}(Ag) = [a, g].$$

It is easy to see that θ is an injective homomorphism. □

Next, we take-up the case when the center is cyclic.

Theorem 5.5 *If G is a 2-generated non-abelian p-group of order p^7 with $\mathrm{Z}(G)$ cyclic, then $|G|$ divides $|\operatorname{Aut}(G)|$.*

Proof Let $G = \langle a, b\rangle$. We have the following five possible cases:

Case (1) $G/\mathrm{Z}_2(G) \cong \mathrm{C}_p \oplus \mathrm{C}_p,\quad \mathrm{Z}_2(G)/\mathrm{Z}(G) \cong \mathrm{C}_{p^2} \oplus \mathrm{C}_p,\quad \mathrm{Z}(G) \cong \mathrm{C}_{p^2}$;

Case (2) $G/\mathrm{Z}_2(G) \cong \mathrm{C}_p \oplus \mathrm{C}_p,\quad \mathrm{Z}_2(G)/\mathrm{Z}(G) \cong \mathrm{C}_p \oplus \mathrm{C}_p \oplus \mathrm{C}_p,\quad \mathrm{Z}(G) \cong \mathrm{C}_{p^2}$;

Case (3) $G/\mathrm{Z}_3(G) \cong \mathrm{C}_p \oplus \mathrm{C}_p,\quad \mathrm{Z}_3(G)/\mathrm{Z}_2(G) \cong \mathrm{C}_p,\quad \mathrm{Z}_2(G)/\mathrm{Z}(G) \cong \mathrm{C}_{p^2},$
$\mathrm{Z}(G) \cong \mathrm{C}_{p^2}$;

Case (4) $G/\mathrm{Z}_3(G) \cong \mathrm{C}_p \oplus \mathrm{C}_p,\quad \mathrm{Z}_3(G)/\mathrm{Z}_2(G) \cong \mathrm{C}_p,\quad \mathrm{Z}_2(G)/\mathrm{Z}(G) \cong \mathrm{C}_p \oplus \mathrm{C}_p,$
$\mathrm{Z}(G) \cong \mathrm{C}_{p^2}$;

Case (5) $G/\mathrm{Z}_4(G) \cong \mathrm{C}_p \oplus \mathrm{C}_p,\quad \mathrm{Z}_4(G)/\mathrm{Z}_3(G) \cong \mathrm{C}_p,\quad \mathrm{Z}_3(G)/\mathrm{Z}_2(G) \cong \mathrm{C}_p,$
$\mathrm{Z}_2(G)/\mathrm{Z}(G) \cong \mathrm{C}_p,\quad \mathrm{Z}(G) \cong \mathrm{C}_{p^2}$.

Cases (1)–(3): Notice that in all these cases $\mathrm{Z}_2(G)$ is abelian. Taking $A = \mathrm{Z}_2(G)$, we see that $A/\mathrm{Z}(G)$ cannot be embedded into $\operatorname{Hom}\big(G/A,\ \mathrm{Z}(G)\big)$, a contradiction to Proposition 5.4. Hence, these cases do not arise.

Case (4): By Proposition 1.8(5), G is metabelian, and therefore by the given condition on G, we have $|\gamma_2(G)| = p^3$. Thus, we obtain

$$G/\gamma_2(G) \cong \mathrm{C}_{p^2} \oplus \mathrm{C}_{p^2} \text{ or } \mathrm{C}_p \oplus \mathrm{C}_{p^3}\,.$$

In the former case, the result holds by considering $\mathrm{IC}(G)$. In the latter case, since $\mathrm{Z}_2(G)\gamma_2(G) = \mathrm{Z}_3(G)$, we have

$$|\,\mathrm{Z}_2(G)/\big(\gamma_2(G) \cap \mathrm{Z}_2(G)\big)| = |\,\mathrm{Z}_3(G)/\gamma_2(G)| = p^2.$$

Hence, we obtain

$$|\gamma_2(G) \cap \mathrm{Z}_2(G)| = p^2.$$

Notice that $[b, a, b]$ and $[b, a, a]$ lie in $\gamma_2(G) \cap \mathrm{Z}_2(G)$. Since

$$\Omega_1\big(\mathrm{Z}(G)\big) = \gamma_2(G) \cap \mathrm{Z}(G) < \gamma_2(G) \cap \mathrm{Z}_2(G),$$

we can choose the generators a, b such that $[b, a, b] \in \Omega_1\big(\mathrm{Z}(G)\big)$. Then, using Hall-Witt identity, we obtain

$$[b, a, a, b] = [b, a, b, a] = 1.$$

Notice that $[b, a, a] \notin \mathrm{Z}(G)$, otherwise $\gamma_3(G) \leq \mathrm{Z}(G)$, which is not possible. Since $\mathrm{Z}_2(G)\gamma_2(G) = \mathrm{Z}_3(G)$, it follows that $[c, a] \notin \mathrm{Z}(G)$ for any $c \in \mathrm{Z}_3(G) \setminus \mathrm{Z}_2(G)$. Consequently, as $[a^p, a] = 1$, we have $a^p \in \mathrm{Z}_2(G)$.

If $a^p \in \gamma_2(G)\,\mathrm{Z}(G)$, then $|\gamma_2(G)b| = p^3$. If $b^p \in \mathrm{Z}_3(G) \setminus \mathrm{Z}_2(G)$, then it follows that $[b, a, b] = 1$. Since $[b, a, a, b] = 1$, we see that $\langle b, \mathrm{Z}_2(G)\rangle$ is abelian and $\mathrm{Z}_2(G)$ centralize b, which is a contradiction. Hence, we obtain

$$b^p \in \mathrm{Z}_2(G) \setminus \mathrm{Z}(G).$$

Since b^p and $[b, a, a]$ are not powers of each other modulo $\gamma_2(G)\,\mathrm{Z}(G)$, they are not so modulo $\mathrm{Z}(G)$. Consequently, $\mathrm{Z}_2(G)$ centralize b, which is again a contradiction. Hence, this situation does not arise, and therefore $a^p \notin \gamma_2(G)\,\mathrm{Z}(G)$.

Since $a^p \in \mathrm{Z}_2(G)$, we have $a^p \in \mathrm{Z}_2(G) \setminus \gamma_2(G)\,\mathrm{Z}(G)$. Choose integers i, j such that the elements $h := a^{pi}$ and $k := [b, a, a]^j$ satisfy $[a, k] = [b, h]$. Using Proposition 2.13, there exists a derivation $\phi : G \to \mathrm{Z}_2(G)$ with

$$\phi(a) = h \text{ and } \phi(b) = k.$$

The automorphism induced by ϕ together with non-inner central automorphisms generate a p-subgroup of $\mathrm{Aut}(G)$ of order greater than or equal to p^2. That $|G|$ divides $|\,\mathrm{Aut}(G)|$ follows by combining this p-subgroup together with $\mathrm{Inn}(G)$.

Case (5): Clearly $p^4 \leq |\gamma_2(G)| \leq p^5$. If $|\gamma_2(G)| = p^4$, then

$$\mathrm{Hom}\,\big(G/\gamma_2(G),\ \ \mathrm{Z}(G)\big) \cong \mathrm{C}_p \oplus \mathrm{C}_{p^2},$$

and therefore $|\,\mathrm{IC}(G)| = p^7$, and we are done.

Now we assume that $|\gamma_2(G)| = p^5$, which yields

$$\gamma_2(G) = \Phi(G) = \mathrm{Z}_4(G).$$

Consequently, we get $\mathrm{Z}_4(G) = \langle [b, a]\rangle \, \mathrm{Z}_3(G)$. Modify generators a, b of G such that $\mathrm{Z}_3(G) = \langle [b, a, a]\rangle \, \mathrm{Z}_2(G)$ and $[b, a, b] \in \mathrm{Z}_2(G)$. Further,

$$[b, a, a, b] \equiv [b, a, b, a] \equiv 1 \mod \Omega_1\big(\mathrm{Z}(G)\big)$$

gives $\mathrm{Z}_2(G) = \langle [b, a, a, a]\rangle \, \mathrm{Z}(G)$.

Let $M = \langle [b, a, a], [b, a, a, a], z^p\rangle$, where $\langle z\rangle = \mathrm{Z}(G)$. Since $[\mathrm{Z}_2(G), \Phi(G)] = 1$, it follows that $\mathrm{Z}_3(G)$ is abelian. Thus, M is an abelian normal subgroup of G. If $a^p \in \mathrm{Z}_k(G) \setminus \mathrm{Z}_{k-1}(G)$ for $k = 3, 4$, then $[a^p, a] = 1$ generates the quotient group $\mathrm{Z}_{k-1}(G)/\mathrm{Z}_{k-2}(G)$, which is absurd. Hence, it follows that $a^p \in \mathrm{Z}_2(G)$. A simple commutator calculation shows that

$$[b, a, a]^p \equiv [b, a, a^p] \equiv 1 \mod \langle [b, a, a, a, a]\rangle$$

and

$$\Omega_1\big(\mathrm{Z}_2(G)\big) = \big\langle [b, a, a, a], z^p\big\rangle.$$

Notice that $[b, a, a, a, a]$ is a central element of order p. Thus, $[b, a, a, a, a] \in \Omega_1\big(\mathrm{Z}(G)\big)$, and consequently $M \cap \mathrm{Z}(G) = \Omega_1\big(\mathrm{Z}(G)\big)$ and $|M| = p^3$.

We claim that $[\mathrm{Z}_4(G), G] \nleq M$. Contrarily, suppose that $[\mathrm{Z}_4(G), G] \leq M$. Since $\mathrm{Z}_4(G) = \gamma_2(G)$ and the nilpotency class of G is 5, it follows that $M = \gamma_3(G)$. Then G/M is a group of order p^4 such that the nilpotency class of G/M is 2 and $|\gamma_2(G/M)| = p^2$, which is not possible. Hence, we must have $[\mathrm{Z}_4(G), G] \nleq M$.

Since $\Omega_1\big(\mathrm{Z}(G)\big) \leq M$ and $\mathrm{Hom}\,\big(G/\mathrm{Z}_3(G),\ \Omega_1\big(\mathrm{Z}(G)\big)\big)$ has a non-inner derivation, it follows that

$$\mathrm{H}^1\,\big(G/\mathrm{Z}_3(G),\ M\big) \neq 1.$$

Since $[\mathrm{Z}_4(G), G] \nleq M$, no inner automorphism can be induced by a representative of a non-trivial element in $\mathrm{H}^1\,\big(G/\mathrm{Z}_3(G),\ M\big)$. If $|\,\mathrm{H}^1\,\big(G/\mathrm{Z}_3(G),\ M\big)| \geq p^2$, then it follows that $\mathrm{H}^1\,\big(G/\mathrm{Z}_3(G),\ M\big)$ embeds in $\mathrm{Out}(G)$ as a p-subgroup, and hence $|G|$ divides $|\,\mathrm{Aut}(G)|$.

Suppose that $|\,\mathrm{H}^1\,\big(G/\mathrm{Z}_3(G),\ M\big)| = p$. By Proposition 2.9, we have the following long exact sequence of cohomology groups

$$0 \to \Omega_1\big(\mathrm{Z}(G)\big) \to \mathrm{Z}(G) \to \mathrm{Z}_3(G)/M \to \mathrm{H}^1\,\big(G/\mathrm{Z}_3(G),\ M\big) \to \mathrm{H}^1\,\big(G/\mathrm{Z}_3(G),\ \mathrm{Z}_3(G)\big)$$

$$\xrightarrow{\sigma} \mathrm{Hom}\,\big(G/\mathrm{Z}_3(G),\ \mathrm{Z}_3(G)/M\big) \xrightarrow{\delta^1} \mathrm{H}^2\,\big(G/\mathrm{Z}_3(G),\ M\big) \to \cdots$$

associated to the short exact sequence

$$1 \to M \to \mathrm{Z}_3(G) \to \mathrm{Z}_3(G)/M \to 1$$

of $G/\mathrm{Z}_3(G)$-modules. We claim that the connecting homomorphism δ^1 is trivial.

First notice that

$$\mathrm{Hom}\big(G/\mathrm{Z}_3(G),\ \mathrm{Z}_3(G)/M\big) \cong \mathrm{Hom}\big(G/\gamma_2(G),\ \mathrm{Z}_3(G)/M\big).$$

Let $f \in \mathrm{Hom}\big(G/\gamma_2(G),\ \mathrm{Z}_3(G)/M\big)$. Then we can factor f through $\mathrm{Z}_3(G)$ via the map

$$\tilde{f}\big(\gamma_2(G)a^ib^j\big) = h\big(\gamma_2(G)a^ib^j\big)z^{li+mj},$$

where $h : G/\gamma_2(G) \to M$ is some map and i, j, l, m are integers such that $0 \le i, j < p$. By the definition of connecting homomorphism, it follows that $\delta^1(f) = \partial^1(h)$ modulo the group of 1-coboundaries of $G/\mathrm{Z}_3(G)$ with coefficients in M, where ∂^1 is the coboundary map of the associated cochain complex. Thus, $\delta^1(f) = 1$ and it follows that

$$|\,\mathrm{H}^1\big(G/\mathrm{Z}_3(G),\ \mathrm{Z}_3(G)\big)| = p^3.$$

Let $K := \mathrm{Z}_3(G)/\mathrm{Z}(G)$ and $L := \mathrm{C}_{\mathrm{Z}_4(G)}\big(\mathrm{Z}_3(G)\big)/\mathrm{Z}(G)$. Then we have

$$L \le G/\mathrm{Z}(G) \cong \mathrm{Inn}(G).$$

Using Proposition 2.45, we get

$$|\,\mathrm{H}^1\big(G/\mathrm{Z}_3(G), \mathrm{Z}_3(G)\big)| = \frac{|\,\mathrm{Aut}^{\mathrm{Z}_3(G), G/\mathrm{Z}_3(G)}(G)|}{|K|}$$

and

$$|\,\mathrm{Aut}^{\mathrm{Z}_3(G), G/\mathrm{Z}_3(G)}(G) \cap \mathrm{Inn}(G)| = |L|.$$

Since $|L/K| \le p$, it follows that

$$|\,\mathrm{Aut}^{\mathrm{Z}_3(G), G/\mathrm{Z}_3(G)}(G)\,\mathrm{Inn}(G)/\,\mathrm{Inn}(G)| = p^i,$$

where $i \ge 2$. Consequently, $|G|$ divides $|\,\mathrm{Aut}(G)|$, and the proof is complete. □

Theorem 5.6 *If G is a 3-generated non-abelian p-group of order p^7 with $\mathrm{Z}(G)$ cyclic, then $|G|$ divides $|\,\mathrm{Aut}(G)|$.*

Proof If $G = \langle a, b, c\rangle$ and $\mathrm{Z}_2(G)/\mathrm{Z}(G)$ is cyclic, then

$$|\,\mathrm{Hom}\big(G/\gamma_2(G),\ \mathrm{Z}(G)\big)| \ge |\,\mathrm{Z}_2(G)|,$$

and we are done. So assume that $\mathrm{Z}_2(G)/\mathrm{Z}(G)$ is not cyclic. Then there are four possible cases, namely:

Case (1) $G/\mathrm{Z}_2(G) \cong \mathrm{C}_p \oplus \mathrm{C}_p, \quad \mathrm{Z}_2(G)/\mathrm{Z}(G) \cong \mathrm{C}_{p^2} \oplus \mathrm{C}_p, \quad \mathrm{Z}(G) \cong \mathrm{C}_{p^2}$;

Case (2) $G/\mathrm{Z}_2(G) \cong \mathrm{C}_p \oplus \mathrm{C}_p, \quad \mathrm{Z}_2(G)/\mathrm{Z}(G) \cong \mathrm{C}_p \oplus \mathrm{C}_p \oplus \mathrm{C}_p, \quad \mathrm{Z}(G) \cong \mathrm{C}_{p^2}$;

Case (3) $G/\mathrm{Z}_2(G) \cong \mathrm{C}_p \oplus \mathrm{C}_p \oplus \mathrm{C}_p, \quad \mathrm{Z}_2(G)/\mathrm{Z}(G) \cong \mathrm{C}_p \oplus \mathrm{C}_p, \quad \mathrm{Z}(G) \cong \mathrm{C}_{p^2}$;

Case (4) $G/\mathrm{Z}_3(G) \cong \mathrm{C}_p \oplus \mathrm{C}_p, \quad \mathrm{Z}_3(G)/\mathrm{Z}_2(G) \cong \mathrm{C}_p, \quad \mathrm{Z}_2(G)/\mathrm{Z}(G) \cong \mathrm{C}_p \oplus \mathrm{C}_p$, $\mathrm{Z}(G) \cong \mathrm{C}_{p^2}$.

Case (1): Let $\mathrm{Z}_2(G) = \langle h, k\rangle\, \mathrm{Z}(G)$ for some $h, k \in G$, where $|\,\mathrm{Z}(G)h| = p^2$ and $|\,\mathrm{Z}(G)k| = p$. If $k \notin \Phi(G)$, then $k \in \mathrm{C}_G\big(\Phi(G)\big)$. Since $\mathrm{Z}_2(G) \cap \Phi(G) = \Phi(G)$ is abelian, it follows that $\mathrm{Z}_2(G)$ is abelian. Taking $A = \mathrm{Z}_2(G)$ contradicts Proposition 5.4. Thus, $k \in \Phi(G)$, and in this case

$$\Phi(G)/\mathrm{Z}(G) \cong \mathrm{C}_p \oplus \mathrm{C}_p\,.$$

Hence, we can assume that $G = \langle a, b, c\rangle$ with $a, b \notin \mathrm{Z}_2(G)$ and $c = h \in \mathrm{Z}_2(G)$. Since c induces a homomorphism of order p^2 from $G/\gamma_2(G)$ onto $\mathrm{Z}(G)$, we get $[b, c] = z$, where $\mathrm{Z}(G) = \langle z\rangle$ and $\mathrm{Z}(G) \le \gamma_2(G)$. Notice that orders of a, b, c modulo $\gamma_2(G)$ are p, p^2, p, respectively. Thus, we can take $k = b^p$, $[b, a] \equiv c^p \bmod \mathrm{Z}(G)$, $[a, c] = [b, c]^{pi}$, where $0 \le i < p$. Replacing a by ab^{-ip}, we can assume that $[a, c] = 1$. It follows that the subgroup $A = \langle a, c\rangle\, \mathrm{Z}(G)$ is abelian and normal. Further, $Q = G/A$ is cyclic of order p^2 and A can be viewed as a Q-module via conjugation.

By Proposition 2.11, we have

$$\mathrm{H}^1(Q,\ A) \cong \mathrm{Ker}(\tau)/I(Q)A$$

and

$$\mathrm{H}^2(Q,\ A) \cong A^Q/\operatorname{Im}(\tau) = \mathrm{Z}(G)/\operatorname{Im}(\tau).$$

Let $\tau : A \to A$ be as in Proposition 2.12. Suppose that $\mathrm{H}^1(Q,\ A) = 1$. Since

$$1 = \mathrm{H}^1(Q,\ A) \cong \mathrm{Ker}(\tau)/I(Q)A$$

and $I(Q)A = \gamma_2(G)$, it follows that $\mathrm{Ker}(\tau) = \gamma_2(G)$. Consequently, we get

$$\operatorname{Im}(\tau) \cong A/\mathrm{Ker}(\tau) \cong A/\gamma_2(G) \cong \mathrm{C}_p \oplus \mathrm{C}_p\,.$$

By Theorem 2.10, we obtain

$$1 = \mathrm{H}^2(Q,\ A) \cong \mathrm{Z}(G)/\operatorname{Im}(\tau),$$

which implies that

$$\operatorname{Im}(\tau) = \mathrm{Z}(G) \cong \mathrm{C}_{p^2},$$

a contradiction. Hence, we must have $\mathrm{H}^1(Q,\ A) \neq 1$. Since $\mathrm{H}^1(Q,\ A) = \mathrm{Ker}(\tau)/\gamma_2(G)$, it follows that there exists an element $x \in A \setminus \gamma_2(G)$ such that $\tau(x) = 1$. By Proposition 2.12, there exists a non-inner derivation of G, which, by Proposition 2.14 induces a non-central automorphism of G. Since the nilpotency class of G is greater than 2, G also admits a non-inner central automorphism. As $\mathrm{Autcent}(G)$ is a normal subgroup of $\mathrm{Aut}(G)$, the two automorphisms are in the same Sylow p-subgroup of $\mathrm{Aut}(G)$, and the result follows.

Case (2): Notice that, in this case $\mathrm{Z}_2(G)$ is abelian. Using Proposition 5.4 with $A = \mathrm{Z}_2(G)$, we get a contradiction. Hence, this case does not arise.

Case (3): If $\gamma_2(G) \neq \Phi(G)$, then

$$|\,\mathrm{Hom}\big(G/\gamma_2(G),\ \mathrm{Z}(G)\big)| \geq |\,\mathrm{Z}_2(G)|,$$

and we are done. So assume that $\gamma_2(G) = \Phi(G)$. It follows that $\mathrm{Z}_2(G) = \langle h, k\rangle\, \mathrm{Z}(G)$ for some $h, k \in G$. In fact, we can take $h = [a, b]$ and $k = [a, c]$. This implies $\langle h, k\rangle\, \Omega_1\big(\mathrm{Z}(G)\big)$ is an abelian normal subgroup of G of order p^3. Further, $\gamma_2(G) = \Phi(G)$ implies that $[b, c] \notin \langle h, k\rangle\, \Omega_1\big(\mathrm{Z}(G)\big)$ and $[b, c] = h^s k^t z$, where $\langle z\rangle = \mathrm{Z}(G)$. Replacing b by ba^{-t} and c by ca^{-s}, we can take $\langle [b, c]\rangle = \mathrm{Z}(G)$. Since

$$[b, c]^p = [b^p, c] = [b, c^p] \neq 1,$$

it follows that both b^p and c^p gives non-trivial elements in $\mathrm{Z}_2(G)/\,\mathrm{Z}(G)$. Since

$$[b, c^p] \neq 1 \neq [b^p, c],$$

it follows that b^p and c^p do not have the same centralizer. Therefore, we have $\mathrm{Z}_2(G)/\,\mathrm{Z}(G) = \langle b^p, c^p\rangle$. Thus, $\Phi(G) = \mho_1(\langle b, c\rangle)$ and

$$\mathrm{C}_{\langle b,c\rangle}\,\big(\Phi(G)\big) = \mathrm{Z}_2(G) = \mho_1\big(\,\langle b, c\rangle\,\big).$$

Since $\mathrm{C}_{G/\Phi(G)}\,\big(\Phi(G)\big) \neq 1$, without loss of generality, we can assume that a centralizes $\Phi(G)$.

Set $A = \langle a\rangle\, \mathrm{Z}_2(G)$. Then A is normal in G and $\mathrm{C}_G(A) = A$. Since $a^p, b^p \in A$, it follows that the extension

$$1 \to A \to G \to G/A \to 1$$

does not split. Hence, $\mathrm{H}^2(G/A,\ A) \neq 1$, and therefore $\mathrm{H}^1(G/A,\ A) \neq 1$ by Theorem 2.10. Since $\mathrm{C}_G(A) = A$, by Proposition 2.45, it follows that

$$\begin{aligned}\mathrm{H}^1(G/A,\ A) &\cong \mathrm{Aut}^{A,G/A}(G)/\big(\,\mathrm{Aut}^{A,G/A}(G) \cap \mathrm{Inn}(G)\big)\\ &\cong \mathrm{Aut}^{A,G/A}(G)\,\mathrm{Inn}(G)/\,\mathrm{Inn}(G).\end{aligned}$$

Since $|\,\mathrm{H}^1(G/A,\ A)| \geq p$, there exists a non-inner automorphism ζ with $|\zeta| \geq p$.

Define $\psi : G/\mathrm{Z}_2(G) \to \mathrm{Z}(G)$ by setting

$$\psi(a) = z^p,\ \psi(b) = 1,\ \psi(c) = 1.$$

Then $\psi \in \mathrm{Hom}\big(G/\mathrm{Z}_2(G),\ \mathrm{Z}(G)\big)$. Since $\gamma_2(G) = \mathrm{Z}_2(G)$, in view of Theorem 3.72, ψ corresponds to an automorphism, say, $\gamma \in \mathrm{Autcent}(G)$. We claim that $\gamma \notin \mathrm{Inn}(G)\,\mathrm{Aut}^{A,G/A}(G)$. Suppose that $\gamma = \alpha\beta$, where $\alpha \in \mathrm{Inn}(G)$ and $\beta \in \mathrm{Aut}^{A,G/A}(G)$. Then

$$\gamma(a) = \alpha\big(\beta(a)\big) = \alpha(a) = [g, a]a$$

for some $g \in G$. This implies $[g, a] = z^p \in \mathrm{Z}(G)$. Since $[a, \mathrm{Z}_2(G)] = 1$, it follows that $g \in G \setminus A$. Hence, $gA = b^l c^m A$ for some integers l, m such that $lm \not\equiv 0 \mod p$. This yields

$$[g, a] \equiv [b, a]^l [c, a]^m \not\equiv 0 \mod \mathrm{Z}(G),$$

a contradiction. Hence, $\gamma \notin \mathrm{Inn}(G)\,\mathrm{Aut}^{A,G/A}(G)$. Therefore, $\langle\zeta, \gamma\rangle\,\mathrm{Inn}(G)$ is a subgroup of $\mathrm{Aut}(G)$ with $|\,\langle\zeta, \gamma\rangle\,\mathrm{Inn}(G)| \geq p^7$, and the result follows.

Case (4): Since $\mathrm{Z}_2(G)$ is abelian and centralizes $\Phi(G)$, it follows that G is metabelian. We claim that $\gamma_2(G) < \Phi(G)$. Contrarily, suppose that $\gamma_2(G) = \Phi(G)$. Then we can choose the generators a, b, c such that $c \in \mathrm{Z}_2(G)$ and $[b, a, b] \in \mathrm{Z}(G)$. It follows that $[b, a, a, b] = 1$, and neither $a^p\,\mathrm{Z}_2(G)$ generates $\mathrm{Z}_3(G)/\mathrm{Z}_2(G)$ nor $a^p\,\mathrm{Z}(G)$ generates $\big(\mathrm{Z}_2(G) \cap \langle a, b\rangle\,\mathrm{Z}(G)\big)/\mathrm{Z}(G)$. Hence, $a^p \in \mathrm{Z}(G)$ and we obtain

$$1 \equiv [a^p, b] \equiv [a, b]^p \mod \gamma_3(G)$$

and $[c, G] \leq \gamma_3(G)$. Thus, $\mathrm{Z}(G) \nleq \langle[a, b]\rangle\,\gamma_3(G) = \gamma_2(G)$, a contradiction to the fact that $\gamma_2(G) = \Phi(G)$. Hence, the claim follows, and $|\gamma_2(G)| \leq p^3$. Consequently, we get

$$|\,\mathrm{Hom}\big(G/\gamma_2(G),\ \mathrm{Z}(G)\big)| \geq |\,\mathrm{Z}_2(G)|,$$

and the proof is complete. □

Theorem 5.7 *If G is a 4-generated non-abelian p-group of order p^7 with $\mathrm{Z}(G)$ cyclic, then $|G|$ divides $|\,\mathrm{Aut}(G)|$.*

Proof In this case, we can assume that $\mathrm{Z}_2(G)/\mathrm{Z}(G)$ is elementary abelian of order p^3. Thus, we have

$$G/\mathrm{Z}_2(G) \cong \mathrm{C}_p \oplus \mathrm{C}_p,$$

$$\mathrm{Z}_2(G)/\mathrm{Z}(G) \cong \mathrm{C}_p \oplus \mathrm{C}_p \oplus \mathrm{C}_p$$

and

$$\mathrm{Z}(G) \cong \mathrm{C}_{p^2}.$$

It now follows that $\gamma_2(G) = \langle [a, b] \rangle \, \Omega_1\big(\mathrm{Z}(G)\big)$, where cosets of a and b form a basis for $G/\mathrm{Z}_2(G)$. Since $|\operatorname{Hom}\big(G/\gamma_2(G),\ \mathrm{Z}(G)\big)| = p^5$, it follows that

$$|\operatorname{IC}(G)| = p^7 = |G|,$$

and the proof is complete. □

5.2 Groups of Coclass 2

Recall that, for a p-group of order p^n and nilpotency class c, the number $n - c$ is called its *coclass*. We begin by noticing that if G is a finite non-abelian p-group of coclass 1 (maximal nilpotency class), then $|\mathrm{Z}(G)| = p$, and hence $|G|$ divides $|\operatorname{Aut}(G)|$ by Theorem 1.32. The aim of this section is to prove the same assertion for finite non-abelian p-groups of coclass 2, where p is an odd prime. Notice that for such groups G, we have $|\gamma_2(G)| = p^{n-2}$ or p^{n-3}.

We begin with the following result of Blackburn [66, III.14.14 Hilfssatz].

Lemma 5.8 *Let G be a p-group of maximal nilpotency class and of order p^n such that $5 \le n \le p + 1$. Then $G/\gamma_{n-1}(G)$ and $\gamma_2(G)$ are of exponent p.*

Lemma 5.9 *Let G be a p-group of order p^n with coclass 2, where p is an odd prime. If $|\mathrm{Z}(G)| = p^2$, then the following statements hold:*

(1) $\exp\big(G/\mathrm{Z}_{n-4}(G)\big) = p$ *for* $n \ge 6$*;*

(2) $|\mathrm{Z}_i(G)| = p^{i+1}$ *for* $1 \le i \le n - 3$.

Proof Set $G_1 = G/Z(G)$ and $G_2 = G_1/\gamma_4(G_1)$. Then both G_1 and G_2 are of maximal nilpotency class having order, respectively, p^{n-2} and p^4. Since $p + 1 \ge 4$, by Lemma 5.8, it follows that $\exp\big(G_2/\gamma_3(G_2)\big) = p$. Since $\gamma_3(G_2) = \gamma_3(G_1)/\gamma_4(G_1)$, we have

$$G/\mathrm{Z}_{n-4}(G) \cong \big(G/\mathrm{Z}(G)\big)/\big(\mathrm{Z}_{n-4}(G)/\mathrm{Z}(G)\big) = G_1/\gamma_3(G_1) \cong G_2/\gamma_3(G_2).$$

This completes the proof of assertion (1).

Since $|\mathrm{Z}_2(G)/\mathrm{Z}(G)| = |\mathrm{Z}\left(G/\mathrm{Z}(G)\right)| = p$, we have $|\mathrm{Z}_2(G)| = p^3$. Assertion (2) now follows by induction on i. □

We now present the following result of Fouladi-Jamali-Orfi [35].

Theorem 5.10 *Let G be a p-group of order p^n and coclass 2, where p is an odd prime. Then $|G|$ divides $|\operatorname{Aut}(G)|$.*

Proof We first suppose that either $\mathrm{Z}(G)$ is elementary abelian or $|\gamma_2(G)| = p^{n-3}$. If $|\mathrm{Z}(G)| = p$, then the assertion follows by Theorem 1.32. So assume that $\mathrm{Z}(G)$ is elementary abelian of order p^2. Since $G/\gamma_2(G)$ is non-cyclic, we have

$$|\operatorname{Autcent}(G)| = |\operatorname{Hom}\big(G/\gamma_2(G),\ \mathrm{Z}(G)\big)| \geq p^4.$$

Further, as $G/\mathrm{Z}(G)$ is of maximal nilpotency class, we get $|\mathrm{Z}_2(G)/\mathrm{Z}(G)| = p$, and hence

$$|\operatorname{Aut}(G)|_p \geq |\operatorname{IC}(G)| \geq p^{n+1}.$$

If $|\gamma_2(G)| = p^{n-3}$, then we can assume that $\mathrm{Z}(G)$ is cyclic of order p^2. It follows that $|\operatorname{Autcent}(G)| \geq p^3$, and hence

$$|\operatorname{Aut}(G)|_p \geq |\operatorname{IC}(G)| \geq p^n.$$

We now take up the remaining case, that is, $\mathrm{Z}(G)$ is cyclic of order p^2 and $|\gamma_2(G)| = p^{n-2}$. Further, by Corollary 4.67, we can take $n \geq 7$. Since $|\mathrm{Z}_2(G)/\mathrm{Z}(G)| = p$, it follows that

$$|\operatorname{IC}(G)| = p^{n-1}.$$

So, to complete the proof, it suffices to construct a non-central and non-inner automorphism of G of p-power order. Since $|\mathrm{Z}_2(G)| = p^3$ and $\mathrm{Z}(G)$ is of order p^2, it follows that $\mathrm{Z}_2(G)$ is abelian. By Proposition 1.8(6), $\mathrm{Z}_2(G)$ is non-cyclic, and therefore we can write

$$\mathrm{Z}_2(G) = \langle z\rangle \oplus \langle x\rangle\,,$$

where z is a generator of $\mathrm{Z}(G)$ and $x \in \mathrm{Z}_2(G) \setminus \mathrm{Z}(G)$. It is not difficult to show that $\mathrm{C}_G(x)$ properly contains $\gamma_2(G)$. Since $x \notin \mathrm{Z}(G)$, it follows that $\mathrm{C}_G\big(\mathrm{Z}_2(G)\big)$ is a maximal subgroup of G.

Set $H = \mathrm{C}_G\big(\mathrm{Z}_2(G)\big)$ and choose elements $s \in G \setminus H$ and $t \in H \setminus \gamma_2(G)$. Then we have $G = \langle s, t\rangle$. Obviously $\mathrm{Z}_2(G) \leq \mathrm{Z}(H)$, and the element $z_1 := [s^{-1}, x]$ lies in $\mathrm{Z}(G)$. Since x is of order p, it follows that z_1 is also of order p. Set $s_2 = [t, s]$. Since $G = \langle s, t\rangle$, it follows that $s_2 \in \gamma_2(G) \setminus \mathrm{Z}_{n-4}(G)$ and

$$H = \langle \mathrm{Z}_{n-4}(G), s_2, t\rangle\,.$$

We construct an automorphism of H, which extends to an automorphism of G of order p. By Lemma 5.9, $H/\mathrm{Z}_{n-4}(G)$ is elementary abelian, and hence can be written as

$$H/\mathrm{Z}_{n-4}(G) = \langle \mathrm{Z}_{n-4}(G)s_2\rangle \oplus \langle \mathrm{Z}_{n-4}(G)t\rangle\,.$$

Consider the homomorphism

$$\psi : H/\mathrm{Z}_{n-4}(G) \to \mathrm{Z}(H)$$

defined by setting $\psi\big(\mathrm{Z}_{n-4}(G)s_2\big) = z_1$ and $\psi\big(\mathrm{Z}_{n-4}(G)t\big) = x$. Let

$$\pi : H \to H/\mathrm{Z}_{n-4}(G)$$

be the natural projection. Then the map

$$h \mapsto h\psi\big(\pi(h)\big)$$

defines a homomorphism

$$\alpha : H \to H$$

such that $\alpha(t) = tx$, $\alpha(s_2) = s_2z_1$ and $\alpha(y) = y$ for all $y \in \mathrm{Z}_{n-4}(G)$. Notice that α^p is identity on H, and hence it follows that α is an automorphism of H of order p.

We extend α to an automorphism of G. Since H is a maximal subgroup, each element of G can be uniquely written in the form hs^i for some $h \in H$ and some i with $1 \leq i \leq p - 1$. Define

$$\hat{\alpha} : G \to G$$

by setting

$$\hat{\alpha}(hs^i) = \alpha(h)s^i.$$

Let $\iota_s : H \to H$ be the restriction of the inner automorphism of G induced by s. Since $H = \langle \mathrm{Z}_{n-4}(G), s_2, t\rangle$ and $\gamma_3(G) \leq \mathrm{Z}_{n-4}(G)$, it is straightforward to show that $\alpha\iota_s = \iota_s\alpha$. Consequently, $\hat{\alpha}$ is an endomorphism of G. Since $\hat{\alpha}^p$ is identity on G, it follows that it is an automorphism of G of order p. Further, $\hat{\alpha}$ is a non-central automorphism of G, since $t^{-1}\hat{\alpha}(t) = x \notin \mathrm{Z}(G)$.

Notice that $G = \langle ts, t\rangle$. The same way as in the preceding paragraph, we can also extend α to a non-central automorphism

$$\tilde{\alpha} : G \to G$$

by defining

$$\tilde{\alpha}(ts) = ts \text{ and } \tilde{\alpha}(t) = tx.$$

Consequently, we have $\tilde{\alpha}(s) = x^{-1}s$. Our final claim is that both $\hat{\alpha}$ and $\tilde{\alpha}$ cannot be inner automorphisms. Contrarily, assume that $\hat{\alpha}$ and $\tilde{\alpha}$ are inner automorphisms induced by the elements u_1 and u_2 of G, respectively. Then the automorphisms induced by $\hat{\alpha}$ and $\tilde{\alpha}$ on $G/\mathrm{Z}(G)$ agree with the inner automorphisms induced by the elements $u_1\mathrm{Z}(G)$ and $u_2\mathrm{Z}(G)$, respectively, which are also central as $x \in \mathrm{Z}_2(G)$. So it follows that $u_1\mathrm{Z}(G)$ and $u_2\mathrm{Z}(G)$ lie in $\mathrm{Z}_2\big(G/\mathrm{Z}(G)\big)$, and therefore u_1 and u_2 belong to $\mathrm{Z}_3(G) \setminus \mathrm{Z}_2(G)$. Thus,

$$u_2 \equiv u_1^l \mod \mathrm{Z}_2(G)$$

for some integer l with $1 \leq l \leq p - 1$. Since $s = \hat{\alpha}(s) = u_1su_1^{-1}$, we get $[u_1, s] = 1$. Notice that

$$x^{-1}s = \tilde{\alpha}(s) = u_2su_2^{-1}.$$

Consequently,

$$x^{-1} = [u_2, s] = [u_1^l x^j, s] = [x, s]^j \in \mathrm{Z}(G),$$

where $0 \leq j \leq p - 1$, which is a contraction. The proof of the theorem is now complete. □

The following problem remains open.

Problem 5.11 Do all 2-groups of coclass 2 satisfy Divisibility Property?

For each coclass it is known that all but finitely many 2-groups have Divisibility Property; we discuss this result of Eick [26] in the following section.

5.3 2-Groups of Fixed Coclass

In this section, we present a result of Eick [26] which asserts that there can possibly be only finitely many groups without Divisibility Property among the 2-groups of a fixed coclass. The tools include coclass theory, pro-p-groups and the fundamental exact sequence of Wells.

Notice that, in view of Corollary 4.67, non-abelian 2-groups of order at most 2^6 have Divisibility Property. Further, in [95, 97], using computational methods, it is proved that non-abelian 2-groups of order 2^7 and 2^8, respectively, also have Divisibility Property.

In what follows, we recall a bit of extension theory from Chap. 2 for abelian extensions. Let

$$\mathcal{E} : 1 \to N \to G \to H \to 1$$

be an abelian extension of groups inducing the coupling $\alpha : H \to \mathrm{Aut}(N)$. Recall from Sect. 2.4 of Chap. 2 that a pair $(\phi, \theta) \in \mathrm{Aut}(H) \times \mathrm{Aut}(N)$ is α-compatible if

$$\theta\alpha(x)\theta^{-1} = \alpha\big(\phi(x)\big)$$

for all $x \in H$. The group of all α-compatible pairs is denoted by $\mathrm{C}_\alpha(H, N)$. We suppress α from the notation when the action is clear from the context.

We use Wells fundamental exact sequence (2.53)

$$1 \to \mathrm{Z}^1(H, N) \longrightarrow \mathrm{Aut}_N(G) \xrightarrow{\rho(\mathcal{E})} \mathrm{C}(H, N) \xrightarrow{\omega(\mathcal{E})} \mathrm{H}^2(H, N),$$

where $\omega(\mathcal{E})$ is Wells map defined as follows.

Recall that $\mathrm{C}(H, N)$ acts on the set $\mathrm{Ext}_\alpha(H, N)$ in a natural way. Let $[\mathcal{E}]$ denote the equivalence class of $\mathcal{E}$ in $\mathrm{Ext}_\alpha(H, N)$ and $c \in \mathrm{C}(H, N)$. Then ${}^c[\mathcal{E}] \in \mathrm{Ext}_\alpha(H, N)$. Since $\mathrm{H}^2(H, N)$ acts freely and transitively on $\mathrm{Ext}_\alpha(H, N)$, there exists a unique element $h \in \mathrm{H}^2(H, N)$ such that

$$^{h}\big(^{c}[\mathcal{E}]\big) = [\mathcal{E}].$$

Then $\omega(\mathcal{E})$ is defined as

$$\omega(\mathcal{E})(c) = h.$$

Now, by exactness of the preceding sequence at $\mathrm{C}(H,\ N)$, we have

$$\begin{aligned}\operatorname{Im}\big(\rho(\mathcal{E})\big) &= \operatorname{Ker}\big(\omega(\mathcal{E})\big)\\ &= \big\{c \in \mathrm{C}(H,\ N) \mid {}^{c}[\mathcal{E}] = [\mathcal{E}]\big\}\\ &= \mathrm{C}(H,\ N)_{[\mathcal{E}]},\ \text{the stabilizer subgroup at } [\mathcal{E}].\end{aligned}$$

In view of the preceding observation, we obtain the following short exact sequence

$$1 \to \mathrm{Z}^1(H,\ N) \longrightarrow \operatorname{Aut}_N(G) \longrightarrow \mathrm{C}(H,\ N)_{[\mathcal{E}]} \to 1.$$

Consequently, if G is finite, then

$$|\operatorname{Aut}_N(G)| = |\mathrm{Z}^1(H,\ N)|\ |\mathrm{C}(H,\ N)_{[\mathcal{E}]}|. \tag{5.12}$$

Let H and N be finite p-groups such that H acts on N. We say that the action is *uniserial* if $\big\langle(^{h}k)k^{-1} \mid k \in K, h \in H\big\rangle$ is an index p subgroup of K for each H-invariant normal subgroup K of N. We refer the reader to [82, Chapter 4] for extensive investigation of uniseriality.

Let L be an infinite pro-2-group of coclass r. Then, by Theorem 1.42, L has an open normal subgroup $T \cong (\mathbb{Z}_2)^d$ for $d = 2^s$ for some integer $s \le r+1$. Further, the quotient group $P = L/T$ is a 2-group of order $2^{r+(r+1)2^{r+1}}$ and coclass r. Setting $T_0 = T$ and $T_{i+1} = [T_i, L]$, we have the following result.

Lemma 5.13 $|\mathrm{Z}^1(P,\ T/T_{j+d})| = 2^d\ |\mathrm{Z}^1(P,\ T/T_j)|$ *for sufficiently large positive integer j.*

Proof First we show that the group of 1-coboundaries $\mathrm{B}^1(P,\ T/T_j)$ has order 2^{j-1} for each positive integer j. By definition, if $\lambda \in \mathrm{B}^1(P,\ T/T_j)$, then there exists $m \in T/T_j$ such that

$$\lambda(g) = \partial^0(m)(g) = {}^{g}m\, m^{-1}$$

for all $g \in P$. Recall that $\partial^0 : C^0(P,\ T/T_j) \to C^1(P,\ T/T_j)$ is the coboundary operator (see (2.1)). Notice that P acts uniserially on T/T_j for each j [82, Chapter 7, Section 4]. Thus, $\operatorname{Ker}(\partial^0) = (T/T_j)^P$, the fixed-point set under the action of P, has size 2, and therefore

$$|\mathrm{B}^1(P,\ T/T_j)| = |(T/T_j)/\operatorname{Ker}(\partial^0)| = 2^{j-1} \tag{5.14}$$

for each j.

Now consider the exact sequence

$$\mathrm{H}^1(P,\ T) \xrightarrow{\alpha} \mathrm{H}^1(P,\ T/T_j) \xrightarrow{\beta_j} \mathrm{H}^2(P,\ T_j)$$

obtained from the long exact sequence corresponding to the short exact sequence

$$1 \to T_j \to T \to T/T_j \to 1$$

of P-modules (see Theorem 2.9). Let $\exp\big(\mathrm{H}^1(P,\ T)\big) = 2^e$. Then it follows that

$$\mathrm{Z}^1(P,\ T_{de}) = \mathrm{Z}^1(P,\ 2^e T) \leq \big(\mathrm{Z}^1(P,\ T)\big)^{2^e} \leq \mathrm{B}^1(P,\ T).$$

Thus, if $j \geq de$, then α is injective. Set $k \equiv j \mod d$. Then $T_j \cong T_k$ as P-modules and $\mathrm{H}^2(P,\ T_j) \cong \mathrm{H}^2(P,\ T_k)$. Thus, $\mathrm{Im}(\beta_j) \cong I_j$, where I_j is a subgroup of $\mathrm{H}^2(P,\ T_k)$. It can be seen that

$$I_k \leq I_{k+d} \leq \cdots .$$

Since $\mathrm{H}^2(P,\ T_k)$ is finite, there exits a positive integer l such that

$$I_l = I_{l+d} = \cdots .$$

If we choose $j \geq \max\{l, de\}$, then

$$|\,\mathrm{H}^1(P,\ T/T_j)| = |\,\mathrm{H}^1(P,\ T)|\ |I_l| = |\,\mathrm{H}^1(P,\ T/T_{j+d})|. \tag{5.15}$$

Using (5.14) and (5.15), we obtain

$$\begin{aligned} |\,\mathrm{Z}^1(P,\ T/T_{j+d})| &= |\,\mathrm{H}^1(P,\ T/T_{j+d})|\ |\,\mathrm{B}^1(P,\ T/T_{j+d})| \\ &= |\,\mathrm{H}^1(P,\ T/T_j)|\ 2^{j+d-1} \\ &= 2^d\ |\,\mathrm{H}^1(P,\ T/T_j)|\ |\,\mathrm{B}^1(P,\ T/T_j)| \\ &= 2^d\ |\,\mathrm{Z}^1(P,\ T/T_j)|, \end{aligned}$$

which completes the proof. □

Let k be a positive integer and $j \geq k$. Then

$$T/T_k \cong (T/T_j)/(T_k/T_j)$$

as P-modules. This implies that the natural projections

$$T/T_j \to T/T_k$$

and

$$T \to T/T_k$$

are homomorphisms of P-modules.

Set $l = \dim\big(\mathrm{End}_P(T)\big)$ for the rest of this section.

Lemma 5.16 *For each positive integer k and each $j \geq k$, the above natural projections induce the following homomorphisms between groups of compatible pairs:*

$$\pi_{j,k} : \mathrm{C}(P,\ T/T_j) \to \mathrm{C}(P,\ T/T_k)$$

and

$$\pi_k : \mathrm{C}(P,\ T) \to \mathrm{C}(P,\ T/T_k)$$

defined by $\pi_{j,k}(\phi, \theta) = (\phi, \bar{\theta})$ and $\pi_k(\phi, \theta) = (\phi, \bar{\theta})$ respectively, where $\bar{\theta}$ denotes the induced automorphism on the corresponding quotient. Furthermore,

$$\pi_{k,l}\pi_{j,k} = \pi_{j,l} \text{ and } \pi_{k,l}\pi_k = \pi_l$$

for $j \geq k \geq l$.

Proof It is sufficient to prove that the maps are well-defined. More precisely, we prove that if $(\phi, \theta) \in \mathrm{C}(P,\ T/T_j)$, then $\theta(T_k/T_j) = T_k/T_j$, and similarly if $(\phi, \theta) \in \mathrm{C}(P,\ T)$, then $\theta(T_k) = T_k$. Let $(\phi, \theta) \in \mathrm{C}(P,\ T/T_j)$ and K be a P-invariant subgroup of T/T_j. If $x \in K$, then for each $g \in P$, we have

$$\alpha\big(\phi(g)\big)\theta(x) = \theta\big(\alpha(g)(x)\big) \in \theta(K),$$

since K is P-invariant. Thus, θ maps P-invariant subgroups of T/T_j to P-invariant subgroups. Since P acts uniserially on T/T_j with unique maximal P-invariant series

$$T/T_j > T_1/T_j > \cdots > T_j/T_j = 1,$$

it follows that T_k/T_j are θ-invariant. Compatibility of $(\phi, \bar{\theta})$ follows from that of (ϕ, θ). The proof for π_k follows along similar lines, and left to the reader.

The last assertion follows simply by observing that $T/T_l \cong (T/T_k)/(T_l/T_k)$, $T/T_k \cong (T/T_j)/(T_k/T_j)$ and $T_l/T_k \cong (T_l/T_j)/(T_k/T_j)$. □

If $(\phi, \theta) \in \mathrm{Ker}(\pi_{j,k})$, then $\phi = 1$ and $\theta : T/T_j \to T/T_j$ looks like $\theta(x) = x\lambda(x)$ for some $\lambda(x) \in T_k/T_j$, where $x \in T/T_j$. This defines a function

$$\lambda : T/T_j \to T_k/T_j.$$

It is not difficult to check that λ is indeed a group homomorphism. Further, the fact $(1, \theta)$ is a compatible pair implies that λ is a homomorphism of P-modules. We now have the following result.

Lemma 5.17 *For each positive integer k and each $j \geq k$, the following statements hold:*

(1) The map $(1, \theta) \mapsto \lambda$ defines a bijection $\mathrm{Ker}(\pi_{j,k}) \to \mathrm{Hom}_P(T/T_j,\ T_k/T_j)$. Furthermore, if $j \leq 2k$, then this is an isomorphism of groups.

(2) The map $(1, \theta) \mapsto \lambda$ defines a bijection $\mathrm{Ker}(\pi_k) \to \mathrm{Hom}_P(T,\ T_k)$.

Proof First we prove that the map in assertion (1) is well-defined. Since $\theta \in Aut(T/T_j)$, it follows that $\lambda \in \mathrm{Hom}(T/T_j,\ T_k/T_j)$. As $(1, \theta) \in C(P,\ T/T_j)$, we see that $\lambda(gxg^{-1}) = g\lambda(x)g^{-1}$ for all $g \in P$ and $x \in T/T_j$. Thus, λ is compatible with the action of P, and hence the map $(1, \theta) \mapsto \lambda$ is well-defined. The injectivity and surjectivity follows by similar arguments.

Suppose that $j \leq 2k$. Notice that the map $(1, \theta) \mapsto \lambda$ is a homomorphism if and only if $T_k/T_j \leq \mathrm{Ker}(\theta)$ for all $\theta \in \mathrm{Ker}(\pi_{j,k})$. Since $\theta(T_i/T_j) \subseteq T_{k+i}/T_j$ for all i, we have the desired result.

The assertion (2) follows by similar arguments as in (1). □

Now assume that $j \geq d$. We set

$$A(T/T_j) = \left\{\theta \in \mathrm{Aut}(T/T_j) \mid (1, \theta) \in \mathrm{Ker}(\pi_{k,d})\right\} \tag{5.18}$$

and

$$A(T) = \left\{\theta \in \mathrm{Aut}(T) \mid (1, \theta) \in \mathrm{Ker}(\pi_d)\right\}. \tag{5.19}$$

Observe that $A(T/T_j) \cong \mathrm{Ker}(\pi_{j,d})$ and $A(T) \cong \mathrm{Ker}(\pi_d)$. With this set-up, we have the following result.

Theorem 5.20 *If j is a sufficiently large positive integer, then*

$$|A(T/T_{j+d})| = 2^l\ |A(T/T_j)|.$$

Proof In view of the final assertion of Lemma 5.16, we have the following commutative diagram

$$\begin{tikzcd}
\cdots \arrow[r, "\mathrm{id}"] & A(T) \arrow[r, "\mathrm{id}"] \arrow[d, "\hat{\pi}_{j+d}"] & A(T) \arrow[r, "\mathrm{id}"] \arrow[d, "\hat{\pi}_{j}"] & \cdots \\
\cdots \arrow[r, "\hat{\pi}_{j+2d,j+d}"] & A(T/T_{j+d}) \arrow[r, "\hat{\pi}_{j+d,j}"] & A(T/T_j) \arrow[r, "\hat{\pi}_{j,j-d}"] & \cdots ,
\end{tikzcd}$$

where $\hat{\pi}_{j,k}$ and $\hat{\pi}_k$ denote restrictions of $\pi_{j,k}$ and π_k on $A(T/T_j)$ and $A(T)$, respectively. Lemma 5.17 yields the following commutative diagram

$$\begin{tikzcd}
\cdots \arrow[r, "\mathrm{id}"] & \mathrm{Hom}_P(T,\ T) \arrow[r, "\mathrm{id}"] \arrow[d, "\tilde{\pi}_{j+d}"] & \mathrm{Hom}_P(T,\ T) \arrow[r, "\mathrm{id}"] \arrow[d, "\tilde{\pi}_{j}"] & \cdots \\
\cdots \arrow[r, "\tilde{\pi}_{j+2d,j+d}"] & \mathrm{Hom}_P(T/T_{j+d},\ T_d/T_{j+d}) \arrow[r, "\tilde{\pi}_{j+d,j}"] & \mathrm{Hom}_P(T/T_j,\ T_d/T_j) \arrow[r, "\tilde{\pi}_{j,j-d}"] & \cdots ,
\end{tikzcd}$$

where $\tilde{\pi}_{j,k}$ and $\tilde{\pi}_k$ are the corresponding maps. Since

$$\mathrm{Hom}_P(T/T_{j+d},\ T_d/T_{j+d}) \cong \mathrm{Hom}_P(T/T_j,\ T/T_j) = \mathrm{End}_P(T/T_j)$$

for all j, it follows that the preceding commutative diagram is equivalent to the following commutative diagram

$$\begin{tikzcd}
\cdots \arrow[r, "\mathrm{id}"] & \mathrm{End}_P(T) \arrow[r, "\mathrm{id}"] \arrow[d, "\tilde{\pi}_{j+d}"] & \mathrm{End}_P(T) \arrow[r, "\mathrm{id}"] \arrow[d, "\tilde{\pi}_j"] & \cdots \\
\cdots \arrow[r, "\tilde{\pi}_{j+2d,j+d}"] & \mathrm{End}_P(T/Tj) \arrow[r, "\tilde{\pi}_{j+d,j}"] & \mathrm{End}_P(T/T_{j-d}) \arrow[r, "\tilde{\pi}_{j,j-d}"] & \cdots ,
\end{tikzcd}$$

where the maps are natural projections. Since $T \cong \mathbb{Z}_2^d$, we have

$$\mathrm{End}(T) \cong T \otimes T \cong \mathbb{Z}_2^{d^2}.$$

The given action of P on T induces an action on $\mathrm{End}(T)$ as follows: For $x \in P$ and $f \in \mathrm{End}(T)$, define ${}^x f$ to be the conjugation of f by the automorphism of T induced by x.

Let $P \to \mathrm{GL}(d^2,\ \mathbb{Z}_2)$ be the action of P on $\mathrm{End}(T)$ given by $g \mapsto M_g$. Then $\mathrm{End}_P(T) = \mathrm{End}(T)^P$, the fixed-point subgroup under the action of P, can be determined as the kernel of the $md^2 \times d^2$ matrix

$$M = \begin{pmatrix} M_{g_1} - I \\ \vdots \\ M_{g_m} - I \end{pmatrix}$$

with entries in $\mathbb{Z}$, where $P = \{g_1, \ldots, g_m\}$. Along similar lines, we see that the group $\mathrm{End}_P(T/T_j)$ corresponds to the kernel of M in T/T_j. Write $M = ADB$ for some diagonal matrix D and invertible matrices A and B. Then for $v \in \mathrm{End}(T)$, we have

$$\begin{aligned}
T_j \otimes T_j + v \in \mathrm{End}_P(T/T_j) &\Leftrightarrow M(v) \equiv 0 \mod T_j \otimes T_j \\
&\Leftrightarrow ADB(v) = w \in T_j \otimes T_j \\
&\Leftrightarrow DB(v) = A^{-1}(w) \in A^{-1}(T_j \otimes T_j) \\
&\Leftrightarrow D(v') \equiv 0 \mod A^{-1}(T_j \otimes T_j),
\end{aligned}$$

where $B(v) = v'$. Similarly, $v \in \mathrm{End}_P(T)$ if and only if $M(v) = 0$, which holds if and only if $D(v') = 0$. Now, let $d_1, \ldots, d_s, e_1, \ldots, e_l$ be the elementary divisors of D such that $d_i > 0$ for all i, $e_j = 0$ for all j, and $l = \dim\big(\mathrm{End}_P(T)\big)$. Choose j sufficiently large such that $\exp(T/T_j) \geq d_i$ for all i. Then we obtain

$$\mathrm{End}_P(T/T_j) \cong \mathrm{C}_{d_1} \oplus \cdots \oplus \mathrm{C}_{d_s} \oplus \mathrm{Im}(\tilde{\pi}_{j+d}).$$

Since $T_{j+d} = 2T_j$, we obtain $A^{-1}(T_j \otimes T_j) = 2\,P^{-1}(T_{j-d} \otimes T_{j-d})$. Consequently,

$$|\operatorname{Im}(\tilde{\pi}_{j+d})| = 2^l\ |\operatorname{Im}(\tilde{\pi}_j)|,$$

and hence

$$|\operatorname{End}_P(T/T_j)| = 2^l\ |\operatorname{End}_P(T/T_{j-d})|,$$

completing the proof. □

Combining the preceding results, we prove the following

Theorem 5.21 *If j is a sufficiently large positive integer, then*

$$|\,\mathrm{C}(P,\ T/T_{j+d})| = 2^l\ |\,\mathrm{C}(P,\ T/T_j)|.$$

Proof By the last assertion of Lemma 5.16, we obtain the chain

$$\cdots \geq \operatorname{Im}(\pi_{j-d,d}) \geq \operatorname{Im}(\pi_{j,d}) \geq \operatorname{Im}(\pi_{j+d,d}) \geq \cdots$$

of subgroups of $\mathrm{C}(P,\ T/T_d)$. Since $\mathrm{C}(P,\ T/T_d)$ is a finite group, the chain must stabilise at some point. Hence, there exists a positive integer k such that

$$\operatorname{Im}(\pi_{j,d}) = \operatorname{Im}(\pi_{j+d,d})$$

for all $j \geq k$. Recall that $A(T/T_j) \cong \operatorname{Ker}(\pi_{j,d})$ and $A(T) \cong \operatorname{Ker}(\pi_d)$. Now, using Theorem 5.20, we obtain

$$\begin{aligned}|\,\mathrm{C}(P,\ T/T_{j+d})| &= |\operatorname{Im}(\pi_{j+d,d})|\ |A(T/T_{j+d})|\\ &= 2^l\ |\operatorname{Im}(\pi_{j,d})|\ |A(T/T_j)| \text{ for sufficiently large } j\\ &= 2^l\ |\,\mathrm{C}(P,\ T/T_j)|,\end{aligned}$$

and the proof is complete. □

Let L be an infinite pro-2-group of coclass r with lower central series

$$L = \gamma_1(L) > \gamma_2(L) > \cdots .$$

Let t be the minimal positive integer such that $L/\gamma_t(L)$ has coclass r and $L/\gamma_t(L)$ does not arise as a quotient of an infinite pro-2-group of coclass r not isomorphic to L. Then the full subtree $\mathcal{T}(L)$ of $\mathcal{G}(2, r)$ consisting of all descendants of $L/\gamma_t(L)$ is a maximal coclass tree in the coclass graph $\mathcal{G}(2, r)$.

The sequence of groups $\{G_i\}_{i\geq 0}$ with $G_i = L/\gamma_{t+i}(L)$ contains every infinite path of $\mathcal{T}(L)$. For each integer $i \geq 0$, let $\mathcal{T}(L)_i$ be the subgraph of $\mathcal{T}(L)$ consisting of all descendants of G_i which are not descendants of G_{i+1}. Then, by Theorem 1.45, there exists a positive integer m such that for each $j \geq m$, there is a graph isomorphism

$$\tau_j : \mathcal{T}(L)_j \to \mathcal{T}(L)_{j+d}.$$

With this set-up, we are now in a position to present the following result leading to the main theorem of this section.

Theorem 5.22 *Let L be an infinite pro-2-group of coclass r which is an extension of T by P, and $\mathcal{T}(L)$ the corresponding maximal coclass tree in $\mathcal{G}(2, r)$ of rank d and periodicity root G_m. Then for each sufficiently large $j \geq m$ and $G \in \mathcal{T}(L)_j$,*

$$|\operatorname{Aut}\big(\tau_j(G)\big)| = 2^{d+l}\ |\operatorname{Aut}(G)|,$$

where $l = \dim\big(\operatorname{End}_P(T)\big)$.

Proof Let $j \geq m$ and $G \in \mathcal{T}(L)_i$. Then, by Theorem 1.46, we have extensions

$$\mathcal{E} : 1 \to T/T_j \to G \to P \to 1$$

and

$$\mathcal{E}' : 1 \to T/T_{j+d} \to \tau_j(G) \to P \to 1.$$

We know from Sect. 2.4 of Chap. 2 that $\mathrm{C}(P,\ T/T_j)$ and $\mathrm{C}(P,\ T/T_{j+d})$ act on the extension classes $[\mathcal{E}]$ and $[\mathcal{E}']$, respectively. It follows from [27, Section 6] that the orbits of $[\mathcal{E}]$ and $[\mathcal{E}']$ have the same size. Hence, by the orbit-stabilizer theorem, we obtain

$$\frac{|\mathrm{C}(P,\ T/T_j)|}{|\mathrm{C}(P,\ T/T_j)_{[\mathcal{E}]}|} = \frac{|\mathrm{C}(P,\ T/T_{j+d})|}{|\mathrm{C}(P, T/T_{j+d})_{[\mathcal{E}']}|}.$$

Now, by Theorem 5.21, for sufficiently large j, we get

$$|\mathrm{C}(P,\ T/T_{j+d})_{[\mathcal{E}']}| = 2^l\ |\mathrm{C}(P,\ T/T_j)_{[\mathcal{E}]}|.$$

Notice that $\operatorname{Aut}\big(\tau_j(G)\big) = \operatorname{Aut}_{T/T_{j+d}}\big(\tau_j(G)\big)$ and $\operatorname{Aut}(G) = \operatorname{Aut}_{T/T_j}(G)$, since T/T_{j+d} and T/T_j are characteristic subgroups of $\tau_j(G)$ and G, respectively. Finally, by (5.12), we have

$$\begin{aligned}
|\operatorname{Aut}\big(\tau_j(G)\big)| &= |\mathrm{Z}^1(P,\ T/T_{j+d})|\ |\mathrm{C}(P,\ T/T_{j+d})_{[\mathcal{E}']}| \\
&= 2^d\ |\mathrm{Z}^1(P,\ T/T_j)|\ |\mathrm{C}(P,\ T/T_{j+d})_{[\mathcal{E}']}|, \text{ by Lemma 5.13} \\
&= 2^d\ |\mathrm{Z}^1(P,\ T/T_j)|\ 2^l\ |\mathrm{C}(P,\ T/T_j)_{[\mathcal{E}]}|, \text{ by Theorem 5.21} \\
&= 2^{d+l}\ |\operatorname{Aut}(G)|.
\end{aligned}$$

The proof of the theorem is complete. □

As an immediate consequence of the preceding theorem and Theorem 1.45, we have

$$\frac{|\operatorname{Aut}\big(\tau_j(G)\big)|}{|\tau_j(G)|} = \frac{2^{d+l}\ |\operatorname{Aut}(G)|}{2^d\ |G|} = \frac{2^l\ |\operatorname{Aut}(G)|}{|G|}$$

for all sufficiently large j. Notice that $l = \dim\big(\mathrm{End}_P(T)\big)$ is positive, and hence $|\operatorname{Aut}\big(\tau_{j+i}(G)\big)|$ grows faster than $|\tau_{j+i}(G)|$ with consecutive applications of τ_{j+i} for $i = 0, d, 2d, \ldots$. Indeed, for instance

$$\frac{|\operatorname{Aut}\big(\tau_{j+d}\ \tau_j(G)\big)|}{|\tau_{j+d}\ \tau_j(G)|} = \frac{2^{d+l}\ |\operatorname{Aut}\big(\tau_j(G)\big)|}{2^d\ |\tau_j(G)|} = \frac{2^{2l}\ |\operatorname{Aut}(G)|}{|G|}.$$

Therefore,

$$\frac{|\operatorname{Aut}\big(\tau_{j+i}(G)\big)|}{|\tau_{j+i}(G)|} \in \mathbb{N}$$

for some i. Using Corollary 1.44, the preceding discussion leads to the following theorem.

Theorem 5.23 *Let r be a fixed positive integer. Then there exists a function $f_r : \mathbb{N} \to \mathbb{N}$ such that $2^s|G|$ divides $|\operatorname{Aut}(G)|$ for each 2-group G of coclass r and order at least $2^{f_r(s)}$.*

Corollary 5.24 *Given a fixed positive integer r, all but finitely many 2-groups of coclass r have Divisibility Property.*

5.4 p^2-Abelian p-Central Groups

In this section, we present a result of Thillaisundaram [121, Theorem 1.1] showing that p^2-abelian p-central p-groups have Divisibility Property.

A p-group G is said to be *p-central* if $x^p \in \mathrm{Z}(G)$ for all $x \in G$. For example, extra-special p-groups are p-central. Recall that a finite abelian p-group A can be decomposed as

$$A \cong \mathrm{C}_{p^{m_1}} \oplus \cdots \oplus \mathrm{C}_{p^{m_r}},$$

where $1 \le m_1 \le \cdots \le m_r$. Suppose that, for each $1 \le t \le r$, $\mathrm{C}_{p^{m_t}} = \langle z_t \rangle$, and set

$$d_t = \max\{s \mid m_s = m_t\}$$

and

$$c_t = \min\{s \mid m_s = m_t\}.$$

Let k be the number of factors of distinct orders in the decomosition of A. Suppose that for each $1 \le l \le k$, A has r_l generators of order p^{n_l}, where $n_1 < \cdots < n_k$. Then, we can write

$$A \cong \underbrace{\mathrm{C}_{p^{n_1}} \oplus \cdots \oplus \mathrm{C}_{p^{n_1}}}_{r_1} \oplus \cdots \oplus \underbrace{\mathrm{C}_{p^{n_l}} \oplus \cdots \oplus \mathrm{C}_{p^{n_l}}}_{r_l} \oplus \cdots \oplus \underbrace{\mathrm{C}_{p^{n_k}} \oplus \cdots \oplus \mathrm{C}_{p^{n_k}}}_{r_k}.$$

Notice that $\sum_{l=1}^{k} r_l = r$. For each $1 \le l \le k$, define

$$D_l = \sum_{i=1}^{l} r_i \text{ and } C_l = \sum_{i=1}^{l-1} r_i + 1.$$

For convenience, we set $C_{k+1} = r + 1$.

Define the following set

$$R_p = \left\{(a_{ij}) \in \mathrm{M}(r, \mathbb{Z}) \mid a_{ij} \equiv 0 \mod p^{m_i - m_j} \text{ for } 1 \le j \le i \le r\right\}.$$

It is easy to check that R_p is a subring of $\mathrm{M}(r, \mathbb{Z})$, the ring of $r \times r$ matrices with entries in $\mathbb{Z}$. For each $1 \le i \le r$, let

$$\pi_i : \mathbb{Z} \to \mathbb{Z}/p^{m_i}\mathbb{Z}$$

be the natural projection. Define the group homomorphism

$$\pi : \mathbb{Z}^r \to A$$

by setting

$$\pi(x_1, \ldots, x_r) = \left(z_1^{\pi_1(x_1)}, \ldots, z_r^{\pi_r(x_r)}\right).$$

Let $\mathrm{End}(A)$ be the ring of endomorphisms of the abelian group A. In this setting, we have the following result due to Hillar-Rhea [57, Theorem 3.3]. Since the proof is elementary, we leave it to the reader. We denote the transpose of a matrix M by M^t.

Theorem 5.25 *The map $\psi : R_p \to \mathrm{End}(A)$ given by*

$$\psi(M)\left(z_1^{\pi_1(x_1)}, \ldots, z_r^{\pi_r(x_r)}\right) = \pi\Big(\big(M(x_1, \ldots, x_r)^t\big)^t\Big)$$

is a surjective ring homomorphism with

$$\mathrm{Ker}(\psi) = \left\{(a_{ij}) \mid a_{ij} \equiv 0 \mod p^{m_i} \textit{ for all } i, j\right\}.$$

Throughout this section, we take $A = \mathrm{Z}(G)$ for a given finite p-group G and use the above setting.

Proposition 5.26 *Let G be a finite non-abelian p^2-abelian p-central p-group with*

$$\mathrm{Z}(G) \cong C_{p^{m_1}} \oplus \cdots \oplus C_{p^{m_r}},$$

where $2 \le m_1 \le \cdots \le m_r$. Let $\theta \in \mathrm{Aut}\big(\mathrm{Z}(G)\big)$ and $M \in R_p$ with $\psi(M) = \theta$ satisfying the following conditions:

(1) $M \equiv I \mod p$;
(2) $a_{ij} \equiv 0 \mod p^{m_i - m_j + 2}$ *for* $i \neq j$ *with* $m_i \geq m_j$, *and* $a_{ii} \equiv 1 \mod p^2$.

Then θ *extends to an automorphism* $\tilde{\theta} \in \mathrm{Autcent}(G)$.

Proof Taking $N = \mathrm{Z}(G)$ and $\phi = 1$ in Proposition 2.51, we see that θ can be extended to a central automorphism of G if and only if there exists a function

$$\chi : G/\mathrm{Z}(G) \to \mathrm{Z}(G)$$

such that

$$\mu(x, y)\theta\big(\mu(x, y)\big)^{-1} = \chi(x)\chi(y)\chi(xy)^{-1}. \tag{5.27}$$

Here $\mu : G/\mathrm{Z}(G) \times G/\mathrm{Z}(G) \to \mathrm{Z}(G)$ is the 2-cocycle corresponding to a transversal $t : G/\mathrm{Z}(G) \to G$ of the central extension

$$1 \to \mathrm{Z}(G) \to G \to G/\mathrm{Z}(G) \to 1.$$

Let $\theta = \psi(M)$ be an automorphism of $\mathrm{Z}(G)$ satisfying the given conditions (1) and (2). Then we can write M in the following form

$$M = \begin{pmatrix} 1 + s_1 p^2 & a_{12} & \cdots & a_{1r} \\ a_{21} & 1 + s_2 p^2 & \cdots & a_{2r} \\ \vdots & \vdots & \vdots & \vdots \\ a_{r1} & a_{r2} & \cdots & 1 + s_r p^2 \end{pmatrix},$$

where $0 \leq s_i < p^{m_i - 2}$. Given $x, y \in G/\mathrm{Z}(G)$, we have

$$\mu(x, y) = z_1^{\alpha_1} \cdots z_r^{\alpha_r}$$

for some $0 \leq \alpha_i < p^{m_i}$ for each i. The left hand side of (5.27) equals

$$\prod_{j=1}^{r} z_j^{-\alpha_j s_j p^2} \prod_{j=1}^{r} z_j^{-\sum_{i \neq j} a_{ji}\alpha_i}.$$

We now proceed to define the desired χ. Notice that, since G is p-central, $t(g)^p \in \mathrm{Z}(G)$ for all $g \in G$. Therefore, we can write

$$t(x)^p = z_1^{\beta_1} \cdots z_r^{\beta_r} \text{ for some } 0 \leq \beta_i < p^{m_i},$$

$$t(y)^p = z_1^{\gamma_1} \cdots z_r^{\gamma_r} \text{ for some } 0 \leq \gamma_i < p^{m_i}$$

and

$$t(xy)^p = z_1^{\delta_1} \cdots z_r^{\delta_r} \text{ for some } 0 \leq \delta_i < p^{m_i}.$$

Since G is also p^2-abelian, we have

$$\mu(x, y)^{p^2} = t(x)^{p^2} t(y)^{p^2} t(xy)^{-p^2}.$$

Putting values in this equation yields

$$z_1^{\alpha_1 p^2} \cdots z_r^{\alpha_r p^2} = z_1^{(\beta_1+\gamma_1-\delta_1)p} \cdots z_r^{(\beta_r+\gamma_r-\delta_r)p}.$$

Now comparing the powers, we get

$$\alpha_i p^2 \equiv (\beta_i + \gamma_i - \delta_i)p \mod p^{m_i}.$$

Define the maps $\chi_1 : G/\mathrm{Z}(G) \to \mathrm{Z}(G)$ and $\chi_2 : \mathrm{Z}(G) \to \mathrm{Z}(G)$ given by

$$\chi_1(x) = t(x)^p = z_1^{\beta_1} \cdots z_r^{\beta_r}$$

and

$$\chi_2(z_1^{\beta_1} \cdots z_r^{\beta_r}) = \prod_{j=1}^{r} z_j^{-\beta_j s_j p} \prod_{j=1}^{r} z_j^{-\sum_{i\neq j} \frac{a_{ji}\beta_i}{p}}.$$

Taking $\chi = \chi_2\chi_1$ and using the conditions (1)–(2), it is not difficult to see that χ satisfies equation (5.27). □

For notational convenience, a matrix $M \in R_p$ is said to be of type (H) if it satisfies the conditions (1)–(2) of Proposition 5.26. Set

$$S = \left\{\tilde{\theta} \in \mathrm{Autcent}(G) \mid \tilde{\theta}|_{\mathrm{Z}(G)} = \theta = \psi(M),\ \text{where } M \text{ is of type (H)}\right\}. \tag{5.28}$$

Continuing with the preceding set-up, we have the following

Proposition 5.29 *Let G be a finite purely non-abelian p^2-abelian p-central p-group with $2 \le n_1 < \cdots < n_k$. Then S is a p-subgroup of* Autcent(G) *and*

$$|S| \ge \frac{|\mathrm{Z}(G)|}{p^{2r}} \prod_{i=1}^{k} p^{(n_i-1)(r-C_{i+1}+1)(C_{i+1}-C_i)} \prod_{i=1}^{k} p^{(n_i-2)(r-C_i)(C_{i+1}-C_i)}.$$

Proof Since G is a purely non-abelian p-group, Autcent(G) is a p-group. Hence, for the first assertion, it suffices to prove that S is a subgroup of Autcent(G). If $\tilde{\theta}_i \in \mathrm{Autcent}(G)$ with $\psi(M_i) = \theta_i$ for $i = 1, 2$, then $\psi(M_1M_2) = \theta_1\theta_2$. Thus, it only remains to show that M_1M_2 is of type (H), which we leave as an exercise for the reader.

If $\tilde{\theta} \in S$, then there exists a matrix M of type (H) and of the form

$$M = \begin{pmatrix}
a_{11} & \cdots & a_{1D_1} & & & & & & & \\
\vdots & & \vdots & & & & & & & \\
a_{D_11} & \cdots & a_{D_1D_1} & & & & & & & \\
& & & a_{C_2C_2} & \cdots & a_{C_2D_2} & & * & & \\
& & & \vdots & & \vdots & & & & \\
& & & a_{D_2C_2} & \cdots & a_{D_2D_2} & & & & \\
& & & & & & \ddots & & & \\
& & * & & & & & a_{C_kC_k} & \cdots & a_{k_kD_k} \\
& & & & & & & \vdots & & \vdots \\
& & & & & & & a_{D_kC_k} & \cdots & a_{D_kD_k}
\end{pmatrix}.$$

In view of Theorem 5.25, we count the choices for a_{ij} modulo p^{m_i} for $1 \leq i, j \leq r$. Further, since each $a_{ii} \equiv 1 \mod p^2$, the number of choices for a_{ii} is p^{m_i-2}. Thus, the total number of choices for the diagonal of M is

$$\prod_{i=1}^{r} p^{m_i-2} = \frac{|\mathrm{Z}(G)|}{p^{2r}}.$$

For each $1 \leq i \leq r$, the number of choices for the ith block modulo the diagonal is

$$p^{(n_i-2)(C_{i+1}-C_i-1)(C_{i+1}-C_i)}.$$

The number of choices for the entries a_{ij} of M with $n_i < n_j$ is

$$\prod_{i=1}^{k} p^{(n_i-1)(r-C_{i+1}+1)(C_{i+1}-C_i)}.$$

Finally, the number of choices for the entries of M with $n_i > n_j$ is at least

$$\prod_{j=1}^{k} p^{(n_j-2)(r-C_{j+1}+1)(C_{j+1}-C_j)}.$$

Since the matrices M are counted modulo $\mathrm{Ker}(\psi)$, it follows that distinct matrices give rise to distinct automorphisms of $\mathrm{Z}(G)$, and hence distinct elements of S. It is now clear from the above counting that the order of S is as desired. □

We now present the main result of this section [121, Theorem 1.1].

Theorem 5.30 *Let G be a finite purely non-abelian p^2-abelian p-central p-group with*

$$\mathrm{Z}(G) \cong \mathrm{C}_{p^{m_1}} \oplus \cdots \oplus \mathrm{C}_{p^{m_r}},$$

where $r \geq 3$ and $3 \leq m_1 \leq \cdots \leq m_r$. Then $|G|$ divides $|\operatorname{Aut}(G)|$.

Proof Recall the definition of S from (5.28). Notice that $S \cap \operatorname{Inn}(G) = 1$. It is sufficient to prove that $|S| \geq |\mathrm{Z}(G)|$. Since $n_i \geq 3$, by Proposition 5.29, we have

$$\begin{aligned}
|S| &\geq \frac{|\mathrm{Z}(G)|}{p^{2r}} \prod_{i=1}^{k} p^{2(r-C_{i+1}+1)(C_{i+1}-C_i)} \prod_{i=1}^{k} p^{(r-C_i)(C_{i+1}-C_i)} \\
&\geq \frac{|\mathrm{Z}(G)|}{p^{2r}} \prod_{i=1}^{k} p^{(r-C_{i+1}+1)(C_{i+1}-C_i)} \prod_{i=1}^{k} p^{(r-C_i)(C_{i+1}-C_i)} \\
&= \frac{|\mathrm{Z}(G)|}{p^{2r}} \prod_{i=1}^{k} p^{\left(2r+1-(C_{i+1}+C_i)\right)(C_{i+1}-C_i)} \\
&= \frac{|\mathrm{Z}(G)|}{p^{2r}} \prod_{i=1}^{k} p^{(2r+1)(C_{i+1}-C_i)-(C_{i+1}^2-C_i^2)} \\
&= \frac{|\mathrm{Z}(G)|}{p^{2r}} p^{(2r+1)(C_{k+1}-C_1)-(C_{k+1}^2-C_1^2)} \\
&= |\mathrm{Z}(G)| p^{r^2-3r}.
\end{aligned}$$

Since $r \geq 3$, the result follows. □

Remark 5.31 The preceding theorem does not imply that all p^2-abelian p-central p-groups have Divisibility Property. The cases $1 \leq r \leq 2$ and $1 \leq m_1 \leq 2$, except $r = m_1 = 1$, still remain open.

Remark 5.32 Recall that, it was proved by Davitt (Theorem 4.49) that all p-abelian p-groups have Divisibility Property. Notice that every p-abelian p-group is obviously p^2-abelian. Further, it is p-central by Theorem 1.26. Thus, Theorem 5.30 gives an alternate proof of Theorem 4.49, except in the cases as stated in Remark 5.31.

5.5 Further Results

In this section, we present additional results on Divisibility Property which are not covered in the previous sections.

We begin with groups of unitriangular matrices over finite fields. Let $\mathbb{F}_q$ be a finite field, where $q = p^n$ for a prime p. For an integer $m \geq 2$, an $m \times m$ matrix $A = (a_{ij})$ over $\mathbb{F}_q$ is said to be upper *unitriangular* if

$$a_{ij} = 0 \text{ for all } i > j$$

and

$$a_{ii} = 1 \text{ for all } i.$$

Let $\mathrm{UT}(m, \mathbb{F}_q)$ be the group of all $m \times m$ upper unitriangular matrices over $\mathbb{F}_q$. It is well-known that $\mathrm{UT}(m, \mathbb{F}_q)$ is a Sylow p-subgroup of the general linear group $\mathrm{GL}(m, \mathbb{F}_q)$ of order $p^{\frac{nm(m-1)}{2}}$ and nilpotency class $m - 1$. We need the following result [66, III.16.4 Satz].

Lemma 5.33 *The upper and the lower central series of* $\mathrm{UT}(m, \mathbb{F}_q)$ *coincide.*

The stucture of the automorphism group of $\mathrm{UT}(m, \mathbb{F}_q)$ has been investigated by Weir [125] for odd primes p, and by Maginnis [86] for $\mathbb{F}_2$. Concerning Divisibility Property, we have the following result.

Theorem 5.34 *For each* $3 \leq i \leq m$*, the group*

$$G_i := \mathrm{UT}(m, \mathbb{F}_q)/\gamma_i\big(\mathrm{UT}(m, \mathbb{F}_q)\big)$$

satisfies Divisibility Property.

Proof By Lemma 5.33, $\mathrm{Z}(G_i) = \gamma_{i-1}(G_i)$ and $\mathrm{Z}_2(G_i) = \gamma_{i-2}(G_i)$. Since G_i is purely non-abelian, by Theorem 3.72, we obtain

$$\begin{aligned} |\operatorname{Aut}(G_i)|_p &\geq |\mathrm{IC}(G_i)| \\ &= \frac{|\operatorname{Hom}\big(G_i/\gamma_2(G_i), \mathrm{Z}(G_i)\big)|\,|G|}{|\mathrm{Z}_2(G_i)|} \\ &= \frac{q^{2m-i}\,|G|}{q^{2m-2i+3}} \\ &= q^{i-3}\,|G| \\ &\geq |G|, \end{aligned}$$

and the proof is complete. □

Let n and m be positive integers such that $n \geq m \geq 3$. A group G is said to be of type $ECF(m, n, p)$ if G is a p-group of order p^n and nilpotency class $m - 1$, $G/\gamma_2(G)$ is elementary abelian, and $|\gamma_i(G)/\gamma_{i+1}(G)| = p$ for $2 \leq i \leq m - 1$. This special class of groups was introduced by Blackburn [13]. The following result is due of Otto [98, Theorem 2].

Theorem 5.35 *Let n and m be positive integers such that* $n \geq m \geq 3$*. If G is a purely non-abelian group of type* $ECF(m, n, p)$*, then* $|G|$ *divides* $|\operatorname{Aut}(G)|$.

Proof Notice that, if $m = 3$, then the group G is of nilpotency class 2, and therefore the result follows by Theorem 4.17. Therefore, we assume that $m > 3$. Since $|\gamma_i(G)/\gamma_{i+1}(G)| = p$ for $2 \leq i \leq m-1$ and $|G| = p^n$, it follows that $G/\gamma_2(G)$ is elementary abelian of order p^{n-m+2}. Let $\mathrm{Z}(G)$ be of order p^r and minimally generated by t elements. Then, by Theorem 3.72, we have

$$|\operatorname{Autcent}(G)| = p^{(n-m+2)t}.$$

Since $t \geq 1$, it follows that $|\operatorname{Autcent}(G)| \geq p^{n-m+2}$. Further, since $|G/\mathrm{Z}_{m-2}(G)| \geq p^2$ and $|\mathrm{Z}_i(G)/\mathrm{Z}_{i-1}(G)| \geq p$ for $1 \leq i \leq m-2$, we have

$$|\mathrm{Z}_2(G)/\mathrm{Z}(G)| \leq p^{n-(r+m-2)}.$$

Clubbing these all together with $|G/\mathrm{Z}(G)| = p^{n-r}$, we get

$$|\mathrm{IC}(G)| = \frac{|G/\mathrm{Z}(G)|\,|\operatorname{Autcent}(G)|}{|\mathrm{Z}_2(G)/\mathrm{Z}(G)|} \geq \frac{p^{n-r}\ p^{n-m+2}}{p^{n-(r+m-2)}} = p^n,$$

which proves that $|G|$ divides $|\operatorname{Aut}(G)|$. □

As a consequence of the preceding theorem, taking $n = m$, we get the following result, which also follows from Theorem 1.32.

Corollary 5.36 *Let G be a finite p-group of maximal nilpotency class with order greater than p^2. Then $|G|$ divides $|\operatorname{Aut}(G)|$.*

We now present some results from [30] on p-groups with Divisibility Property.

Theorem 5.37 *Let G be a purely non-abelian p-group of nilpotency class c such that $\gamma_i(G)/\gamma_{i+1}(G)$ is cyclic of order p^r for some $r \geq 1$ and for all $2 \leq i \leq c$. If $|G/\mathrm{Z}_{c-1}(G)| \geq p^{2r}$ and $\exp\big(G/\gamma_2(G)\big) \leq |\mathrm{Z}(G)|$, then $|G|$ divides $|\operatorname{Aut}(G)|$.*

Proof Let $|G| = p^n$ and $|G/\gamma_2(G)| = p^m$. Since $|\gamma_i(G)/\gamma_{i+1}(G)| = p^r$ for all $2 \leq i \leq c$, we have $n = m + (c-1)r$. By Proposition 1.6, we get

$$\mathrm{Z}_i(G) \cap \gamma_{c-i}(G) = \gamma_{c-i+1}(G)$$

for all $0 \leq i \leq c-2$. It follows that

$$\frac{|\mathrm{Z}_{i+1}(G)|}{|\mathrm{Z}_i(G)|} \geq \frac{|\mathrm{Z}_i(G)\gamma_{c-i}(G)|}{|\mathrm{Z}_i(G)|} = \frac{|\gamma_{c-i}(G)|}{|\mathrm{Z}_i(G) \cap \gamma_{c-i}(G)|} = \frac{|\gamma_{c-i}(G)|}{|\gamma_{c-i+1}(G)|} = p^r.$$

Further, $|G/\mathrm{Z}_{c-1}(G)| \geq p^{2r}$ by the hypothesis. Let $|\mathrm{Z}(G)| = p^k$ and $|\mathrm{Z}_2(G)/\mathrm{Z}(G)| = p^u$. Then we have $n \geq 2r + (c-3)r + u + k$. Consequently, $m + (c-1)r \geq 2r + (c-3)r + u + k$, and hence $m \geq k + u$. By Corollary 3.75(2),

$$|\operatorname{Autcent}(G)| \geq p^m \geq p^{k+u},$$

and hence

$$|\operatorname{Aut}(G)|_p \geq |\operatorname{IC}(G)| \geq p^n,$$

and the proof is complete. □

The following result is the case $p = 2$ of [118, Theorem 4.1].

Theorem 5.38 *Let G be a non-abelian 2-group of order 2^n and M a maximal cyclic subgroup of G. Then G is isomorphic to one of the following groups:*

(1) The dihedral group of order 2^n for $n \geq 3$.

(2) The generalised quaternion group of order 2^n for $n \geq 3$.

(3) $\left\langle x, y \mid x^{2^{n-1}} = y^2 = 1, yxy^{-1} = x^{1+2^{n-2}} \right\rangle$ for $n \geq 4$.

(4) $\left\langle x, y \mid x^{2^{n-1}} = y^2 = 1, yxy^{-1} = x^{-1+2^{n-2}} \right\rangle$ for $n \geq 4$.

Theorem 5.39 *If G is a non-abelian finite p-group such that the Frattini subgroup $\Phi(G)$ is cyclic, then $|G|$ divides $|\operatorname{Aut}(G)|$.*

Proof Suppose that p is an odd prime. Since $\gamma_2(G) \leq \Phi(G)$, it follows that $\gamma_2(G)$ is also cyclic. Then, by Lemma 1.13, G is regular. It follows that

$$|\Omega_1\big(G/\Omega_1(G)\big)| = |\Omega_2(G)/\Omega_1(G)| = |\mho_1(G)/\mho_2(G)|.$$

Since $\mho_1(G) \leq \Phi(G)$, $\mho_1(G)$ is cyclic and $|\mho_1(G)/\mho_2(G)| \leq p$. Hence, $|\Omega_1\big(G/\Omega_1(G)\big)| \leq p$ and $G/\Omega_1(G)$ has at most one subgroup of order p. Thus, $G/\Omega_1(G)$ is cyclic and $\gamma_2(G) \leq \Omega_1(G)$. Since G is regular, we have $\exp\big(\Omega_1(G)\big) = p$. Consequently, $\exp\big(\gamma_2(G)\big) = p$, and hence $|\gamma_2(G)| = p$. Thus, G has nilpotency class 2, and the result follows from Theorem 4.17.

Now assume that $p = 2$. In this case $\mho_1(G) = \Phi(G)$. Thus, there exists an element $a \in G$ such that $\Phi(G) = \langle a^2 \rangle$. Let

$$\mathcal{C} = \big\{H \mid H \leq G, a \in H \text{ and } |H/\langle a\rangle| = 2\big\}.$$

Since for each $x \in G$, we have $x^2 \in \Phi(G)$, it follows that

$$G = \langle H \mid H \in \mathcal{C}\rangle.$$

Notice that, each $H \in \mathcal{C}$ has a maximal cyclic subgroup. Therefore, by Theorem 5.38, H satisfies one of the following conditions:

(1) H is abelian;
(2) H is of nilpotency class 2 with $H/\mathrm{Z}(H)$ elementary abelian of order 4;
(3) H is of maximal nilpotency class.

If there is no group of maximal nilpotency class in $\mathcal{C}$, then $a^2 \in \mathrm{Z}(H)$ for all $H \in \mathcal{C}$. Consequently, $\Phi(G) = \langle a^2 \rangle \leq \mathrm{Z}(G)$ and G has nilpotency class 2. The result again follows from Theorem 4.17.

If $H \in \mathcal{C}$ is of maximal nilpotency class, then $|H/\gamma_2(H)| = 4 = |H/\Phi(G)|$, and hence $\gamma_2(G) = \Phi(G)$. Therefore, $\exp\big(G/\gamma_2(G)\big) = 2$ and $\gamma_i(G)/\gamma_{i+1}(G)$ is cyclic of order 2 for all $2 \leq i \leq c$. The result now follows from Theorem 5.37. □

Next we investigate Divisibility Property for finite p-groups admitting a normal subgroup of maximal nilpotency class [30, Theorem 2].

Theorem 5.40 *Let G be a purely non-abelian finite p-group and M a normal subgroup of G of maximal nilpotency class. If G/M is elementary abelian or $|G/M| = p^2$, then $|G|$ divides $|\operatorname{Aut}(G)|$.*

Proof Let G be of nilpotency class c with $|G| = p^n$, $|G/\gamma_2(G)| = p^m$ and $|G/M| = p^a$. Then M is of nilpotency class $c' = n - a - 1$ with $c \geq c'$. In view of Theorem 4.17, we can assume that $c > 2$. By Theorem 1.32, we can further assume that $|\mathrm{Z}(G)| \geq p^2$.

Suppose that G/M is elementary abelian. Then $\Phi(G) \leq M$. Since $\Phi(G)$ cannot be of maximal nilpotency class, it follows that $\Phi(G) < M$, and therefore $\gamma_2(G) < M$. This implies that $m \geq a + 1$. Further, nilpotency class of G being c implies that $|\gamma_2(G)| \geq p^{c-1}$. This together with the fact that $c \geq c'$ implies that $m \leq a + 2$, and hence $m = a + 1$ or $a + 2$. Consequently, $|\Phi(G)/\gamma_2(G)| \leq p$, which along with the fact that $\exp\big(G/\Phi(G)\big) = p$ yields

$$\exp\big(G/\gamma_2(G)\big) \leq p^2 \leq |\mathrm{Z}(G)|.$$

Thus, by Corollary 3.75(2),

$$|\operatorname{Autcent}(G)|_p \geq p^m.$$

Since $c > 2$, it follows that $|G/\mathrm{Z}_2(G)| \geq p^{c-1}$. Consequently, we get

$$|\operatorname{Aut}(G)|_p \geq |\mathrm{IC}(G)|_p = |G/\mathrm{Z}_2(G)|\,|\operatorname{Autcent}(G)| \geq p^{m+c-1}.$$

Thus, it suffices to prove that $m + c - 1 \geq n$.

Notice that, since $c \geq c'$, for $m = a + 2$, we have $m + c - 1 \geq n$. So, we assume that $m = a + 1$. Consequently, we get $|\gamma_2(G)/\gamma_2(M)| = p$. We claim that $\gamma_{i+1}(G) = \gamma_i(M)$ for all i. First notice that, $\gamma_2(M)$ being a normal subgroup of G, $\gamma_2(G)/\gamma_2(M) \leq \mathrm{Z}\big(G/\gamma_2(M)\big)$, which further yields

$$\gamma_3(G) = [\gamma_2(G), G] \leq \gamma_2(M).$$

Since $M/\gamma_2(G)$ is cyclic, we get $\gamma_2(M) = [M, \gamma_2(G)]$. Consequently,

$$\gamma_2(M) = [\gamma_2(G), M] \leq [\gamma_2(G), G] = \gamma_3(G),$$

which yields $\gamma_3(G) = \gamma_2(M)$. Assuming that $\gamma_{i+1}(G) = \gamma_i(M)$ for some $2 \le i \le c - 1$, we obtain

$$\gamma_i(M) = \gamma_{i+1}(G) > \gamma_{i+2}(G) = [\gamma_{i+1}(G), G] \ge [\gamma_i(M), M] = \gamma_{i+1}(M).$$

Since M is of maximal nilpotency class, we have $|\gamma_i(M)/\gamma_{i+1}(M)| = p$. Hence, $\gamma_{i+2}(G) = \gamma_{i+1}(M)$, which proves our claim. In particular, we have $\gamma_{c'+2}(G) = \gamma_{c'+1}(M) = 1$ and $\gamma_{c'+1}(G) = \gamma_{c'}(M) \neq 1$. Therefore, G has nilpotency class $c = c' + 1 = n - a$, and hence $m + c - 1 = n$. This completes the proof when G/M is elementary abelian.

We remark that $|G/\mathrm{Z}_2(G)| \ge p^{c-1}$. Next, suppose that $|G/M| = p^2$. We only need to consider the case when G/M is cyclic of order p^2 and $c \ge c' = n - 3$. Since $G/\gamma_2(G)$ is not cyclic, we must have $\gamma_2(G) < M$, and hence $m \ge 3$. Further, $|\gamma_2(G)| \ge p^{c-1}$ yields $m \le 4$, which implies that $m = 3$ or 4.

If $m = 3$, then proceeding as in the case when G/M is elementary abelian, we obtain $c = c' + 1 = n - 2$. Since $\exp\big(G/\gamma_2(G)\big) \le p^2 \le |\,\mathrm{Z}(G)|$, by Corollary 3.75(2), we have $|\,\mathrm{Autcent}(G)|_p \ge p^3$, which in turn gives $|\,\mathrm{Aut}(G)|_p \ge p^{c+2} = p^n$.

If $m = 4$, then $|\gamma_i(G)/\gamma_{i+1}(G)| = p$ for all $i \ge 1$ and $c = n - 3$. Moreover,

$$|G/\gamma_2(G)| = p^4 = |G/M|\,|M/\gamma_2(M)| = |G/\gamma_2(M)|$$

implies that $\gamma_2(G) = \gamma_2(M)$. Suppose that G is generated by two elements. Since $M < G$, there exists a maximal subgroup N of G such that $M \le N$. Consequently, we have $\Phi(G) \le N$. Since G is generated by two elements, there exists an element $x \in G$ such that $N = \langle x, \Phi(G)\rangle$. By Proposition 1.7, we get

$$\gamma_2(N) = \gamma_2(\langle x\rangle\, \Phi(G)) < \gamma_2(G),$$

which implies that $\gamma_2(M) < \gamma_2(G)$, a contradiction. Hence, G cannot be generated by two elements. Thus, $G/\gamma_2(G)$ has more than two invariants and $\exp\big(G/\gamma_2(G)\big) \le p^2 \le |\,\mathrm{Z}(G)|$. By Corollary 3.75(2), we obtain

$$|\,\mathrm{Aut}(G)|_p \ge |\,\mathrm{IC}(G)| \ge p^4\, p^{c-1} = p^n,$$

and the proof is complete. □

Divisibility Property for p-groups admitting certain quotient of maximal nilpotency class is considered in the following result [30, Theorem 3].

Theorem 5.41 *Let G be a finite p-group and M a maximal subgroup of G. If M contains a normal subgroup H of order p such that M/H is of maximal nilpotency class, then $|G|$ divides $|\,\mathrm{Aut}(G)|$.*

Proof Suppose that $|G| = p^n$. By Theorem 1.32, we can assume that $|\,\mathrm{Z}(G)| \ge p^2$. Since $|M/H| = p^{n-2}$, it follows that M/H has nilpotency class $n - 3$, and hence M

has nilpotency class $c' \geq n-3$. If $c' = n-2$, then the results follows from Theorem 5.40.

Assume that $c' = n-3$. As H is normal in M and $|H| = p$, it follows that $H \leq \mathrm{Z}(M)$ and $|\,\mathrm{Z}(M)| = p^2$. We claim that $\mathrm{Z}(M)$ is elementary abelian. Suppose that $\mathrm{Z}(M)$ is cyclic. Since $|M| = p^{n-1}$, we have

$$p^2 \leq |M/\gamma_2(M)| \leq p^3.$$

Consequently, $M/\gamma_2(M)$ is one of the following groups:

$$\mathrm{C}_p \oplus \mathrm{C}_p,\ \mathrm{C}_p \oplus \mathrm{C}_{p^2},\ \mathrm{C}_p \oplus \mathrm{C}_p \oplus \mathrm{C}_p\,.$$

In each of these cases, $\exp\big(\gamma_{c'}(M)\big) = p$. Further, $\gamma_{c'}(M) \leq \mathrm{Z}(M)$ and $\mathrm{Z}(M)$ being cyclic implies that $\gamma_{c'}(M)$ is cyclic of order p. Since $\mathrm{Z}(M)$ has only one subgroup H of order p, we have $H = \gamma_{c'}(M)$, and hence $\gamma_{c'}(M/H) = 1$, a contradiction. Therefore, $\mathrm{Z}(M)$ is elementary abelian of order p^2, and hence

$$|\,\mathrm{Aut}(M)|_p \geq |\,\mathrm{IC}(G)| \geq p^{c'+3} = p^n.$$

If $\mathrm{Z}(G) \not\leq M$, then $G = \mathrm{Z}(G)M$, and the result follows from Theorem 4.4. And, if $\mathrm{Z}(G) \leq M$, then $\mathrm{Z}(G) \leq \mathrm{Z}(M)$. Since $|\,\mathrm{Z}(G)| \geq p^2$, it must be elementary abelian of order p^2, and we again obtain

$$|\,\mathrm{Aut}(G)|_p \geq |\,\mathrm{IC}(G)| \geq p^{c'+3} = p^n,$$

completing the proof. □

Let G be a finite p-group and N a non-trivial proper normal subgroup of G. Recall that (G, N) is called a *Camina pair* if

$$Nx \ \subseteq\ {}^{G}x$$

for all $x \in G \setminus N$.

Let (G, N) be a Camina pair and H a normal subgroup of G such that $H < N$. Then it easily follows that $\big(G/H, N/H\big)$ is also a Camina pair. We begin with the following observation.

Lemma 5.42 *Let G be a finite p-group and M a maximal subgroup of G. If* $\mathrm{Z}(M) \leq \mathrm{Z}(G)$*, then* $\mathrm{Aut}^M(G) \cap \mathrm{Inn}(G) = 1$.

Proof Each element $\phi \in \mathrm{Aut}^M(G) \cap \mathrm{Inn}(G)$ is conjugation by some element $g \in G$ such that g centralizes M. If $g \notin M$, then $G = M\,\langle g\rangle$. Thus, g centralizes G, and therefore lies in $\mathrm{Z}(G)$. If $g \in M$, then $g \in \mathrm{Z}(M) \leq \mathrm{Z}(G)$. Hence, $g \in \mathrm{Z}(G)$, and ϕ is trivial. □

The following result is from [34, Lemma 3.2].

Proposition 5.43 *Let G be a finite p-group such that $\mathrm{Z}(G)$ is elementary abelian and $\mathrm{Z}(G) = \mathrm{Z}(M)$ for some maximal subgroup M of G. Then $|G|$ divides $|\operatorname{Aut}(G)|$.*

Proof Under the given hypothesis, by Proposition 2.45, we have

$$|\operatorname{Aut}^{M,G/M}(G)| = |\operatorname{Der}\big(G/M,\ \mathrm{Z}(M)\big)| = |\operatorname{Hom}\big(G/M,\ \mathrm{Z}(M)\big)| = |\mathrm{Z}(G)|.$$

By Lemma 5.42, $\operatorname{Aut}^{M,G/M}(G) \cap \operatorname{Inn}(G) = 1$. Thus,

$$|\operatorname{Out}(G)|_p \geq |\operatorname{Aut}^{M,G/M}(G)| = |\mathrm{Z}(G)|,$$

and the proof is complete. □

The next result is from [128, Theorem A].

Theorem 5.44 *Let G be a finite p-group such that $\big(G, \mathrm{Z}(G)\big)$ is a Camina pair. Then $|G|$ divides $|\operatorname{Aut}(G)|$.*

Proof If $|\mathrm{Z}(G)| = p$, then the result follows from Theorem 1.32. So, we assume that $|\mathrm{Z}(G)| \geq p^2$.

Since $\big(G, \mathrm{Z}(G)\big)$ is a Camina pair, $\mathrm{Z}(G)$ is elementary abelian by Proposition 1.11(2). Further, by Theorem 1.12, either G has a maximal subgroup M with $\mathrm{Z}(M) = \mathrm{Z}(G)$ or $|\mathrm{Z}_2(G)/\mathrm{Z}(G)| = |G/\Phi(G)|$. First assume that G has a maximal subgroup M such that $\mathrm{Z}(M) = \mathrm{Z}(G)$. By Proposition 2.45, we get

$$\operatorname{Aut}^{M,G/M}(G) \cong \mathrm{Z}^1\big(G/M,\ \mathrm{Z}(M)\big).$$

Since $\mathrm{Z}(M) = \mathrm{Z}(G)$, we have $\mathrm{Z}^1\big(G/M,\ \mathrm{Z}(M)\big) = \operatorname{Hom}\big(G/M,\ \mathrm{Z}(G)\big)$. It follows from Lemma 5.42 that

$$\operatorname{Aut}^{M,G/M}(G) \cap \operatorname{Inn}(G) = 1.$$

Since $|G/M| = p$, we get $|\operatorname{Hom}\big(G/M,\ \mathrm{Z}(G)\big)| = |\mathrm{Z}(G)|$. Thus,

$$|\operatorname{Aut}(G)| \geq |\operatorname{Aut}^{M,G/M}(G)|\,|\operatorname{Inn}(G)| = |\mathrm{Z}(G)|\,|G/\mathrm{Z}(G)| = |G|.$$

Now assume the second case. Since $\big(G, \mathrm{Z}(G)\big)$ is a Camina pair, we have $\mathrm{Z}(G) \leq \gamma_2(G)$, and therefore G is purely non-abelian. Let $|G/\Phi(G)| = p^d$ and $|\mathrm{Z}(G)| = p^r$. By the given hypothesis,

$$|\mathrm{Z}_2(G)/\mathrm{Z}(G)| = |G/\Phi(G)| = p^d,$$

and hence $|\mathrm{Z}_2(G)| = p^{r+d}$. Also, we have $|\operatorname{Hom}\big(G/\Phi(G),\ \mathrm{Z}(G)\big)| = p^{rd}$. Since both r and d are greater than 1, we get

$$|\mathrm{Z}_2(G)| = p^{r+d} \leq p^{rd} = |\operatorname{Hom}\big(G/\Phi(G),\ \mathrm{Z}(G)\big)|.$$

By Theorem 3.72, we obtain $|\operatorname{Autcent}(G)| = |\operatorname{Hom}\big(G/\Phi(G),\ \mathrm{Z}(G)\big)|$, and hence

$$|\operatorname{Aut}(G)|_p \geq |\operatorname{IC}(G)| \geq |G|.$$

This completes the proof of the theorem. □

Before proceeding further, we recall some notations from Sect. 1.4 of Chap. 1. Let G be a finite p-group, and M be a maximal subgroup of G. Let $g \in G$ be such that $G/M = \langle Mg \rangle$. Define endomorphisms τ and γ of $\mathrm{Z}(M)$ as follows:

$$\tau(m) = m\ {}^{g}m \cdots {}^{g^{p-1}}m$$

and

$$\gamma(m) = [m, g],$$

for all $m \in \mathrm{Z}(M)$.

Below is one of the main results of [34, Theorem 2.4].

Theorem 5.45 *Let G be a finite non-cyclic p-group of order greater than p^2 admitting an abelian maximal subgroup. Then $|G|$ divides $|\operatorname{Aut}(G)|$.*

Proof In view of Remark 4.7, we can assume that G is purely non-abelian. Let M be an abelian maximal subgroup of G. Let $g \in G$ be such that $G/M = \langle Mg \rangle$. Then we have

$$\gamma_2(G) = \big\{[m, g] \mid m \in M\big\} = [M, g].$$

Further, by Exercise 1.28, we get $|\gamma_2(G)| = |M/\big(M \cap \mathrm{Z}(G)\big)|$. Since $\mathrm{Z}(G) \leq M$, it follows that $|\gamma_2(G)| = |M/\mathrm{Z}(G)|$, and hence

$$|G/\gamma_2(G)| = p\,|\mathrm{Z}(G)|.$$

Notice that $M/\mathrm{Z}(G)$ is an abelian maximal subgroup of $G/\mathrm{Z}(G)$. So, as above, we obtain

$$|\big(G/\mathrm{Z}(G)\big)/\gamma_2\big(G/\mathrm{Z}(G)\big)| = p\,|\mathrm{Z}\left(G/\mathrm{Z}(G)\right)|.$$

This yields

$$|G/\big(\gamma_2(G)\,\mathrm{Z}(G)\big)| = p\,|\mathrm{Z}_2(G)/\mathrm{Z}(G)|,$$

which further implies that

$$|\mathrm{Z}_2(G)| = \frac{|G/\gamma_2(G)|\,|\gamma_2(G) \cap \mathrm{Z}(G)|}{p} = |\mathrm{Z}(G)|\,|\gamma_2(G) \cap \mathrm{Z}(G)|. \tag{5.46}$$

We claim that $\exp\big(\gamma_2(G) \cap \mathrm{Z}(G)\big) = p$. Since $M = \mathrm{Z}(M)$, γ and τ, as defined above, are endomorphisms of M. We know that $\operatorname{Im}(\gamma) \leq \operatorname{Ker}(\tau)$. Since $\operatorname{Im}(\gamma) = [M, g] = \gamma_2(G)$, we have

$$[m,g]\,{}^{g}[m,g]\cdots{}^{g^{p-1}}[m,g]=1$$

for all $m\in M$. But, if $[m,g]\in \mathrm{Z}(G)$, then this yields $[m,g]^p=1$. Thus, for any $[m,g]\in\gamma_2(G)\cap\mathrm{Z}(G)$, $[m,g]^p=1$, and our claim follows.

Notice that $d(G)\geq 2$. If $\exp\big(G/\gamma_2(G)\big)\geq\exp\big(\mathrm{Z}(G)\big)$, then the preceding claim together with (5.46) implies that

$$|\operatorname{Hom}\big(G/\gamma_2(G),\ \mathrm{Z}(G)\big)|\geq|\mathrm{Z}(G)|\,|\Omega_1\big(\mathrm{Z}(G)\big)|\geq|\mathrm{Z}(G)|\,|\gamma_2(G)\cap\mathrm{Z}(G)|=|\mathrm{Z}_2(G)|.$$

If $\exp\big(G/\gamma_2(G)\big)<\exp\big(\mathrm{Z}(G)\big)$, then again by (5.46), we get

$$\begin{aligned}|\operatorname{Hom}\big(G/\gamma_2(G),\ \mathrm{Z}(G)\big)|&\geq\frac{|G/\gamma_2(G)|\,|\Omega_1\big(\mathrm{Z}(G)\big)|}{p}\\&\geq\frac{|G/\gamma_2(G)|\,|\gamma_2(G)\cap\mathrm{Z}(G)|}{p}\\&=|\mathrm{Z}_2(G)|.\end{aligned}$$

Since G is purely non-abelian, by Theorem 3.72, we have

$$|\operatorname{Aut}(G)|_p\geq|\mathrm{IC}(G)|=\frac{|\operatorname{Hom}\big(G/\gamma_2(G),\ \mathrm{Z}(G)\big)|\,|G|}{|\mathrm{Z}_2(G)|}\geq|G|,$$

and the proof is now complete. □

We need the following result of Müller [91, Lemma 2.2].

Lemma 5.47 *Let G be a finite p-group such that $\mathrm{Z}(G)<\mathrm{Z}(M)$ for all maximal subgroups M of G and $\mathrm{C}_G\big(\mathrm{Z}(\Phi(G))\big)\neq\Phi(G)$. Then $G=RS$ is a central product of subgroups R and S with $R/\mathrm{Z}(R)$ elementary abelian of order p^2.*

Proof We claim that there exists a maximal subgroup M of G such that $\mathrm{Z}(M)\nleq\Phi(G)$. Suppose $\mathrm{Z}(M)\leq\Phi(G)$ for each maximal subgroup M of G. It follows that

$$\cup_{M\text{ maximal}}\mathrm{Z}(M)\leq\mathrm{Z}\big(\Phi(G)\big).$$

Since $\mathrm{C}_G\big(\mathrm{Z}(M)\big)=M$ for all maximal subgroups M of G, we have

$$\mathrm{C}_G\big(\cup_{M\text{ maximal}}\mathrm{Z}(M)\big)\leq\Phi(G).$$

Hence, $\mathrm{C}_G\big(\mathrm{Z}(\Phi(G))\big)=\Phi(G)$, a contradiction to our hypothesis.

With M as above, choose a maximal subgroup N such that $G=\mathrm{Z}(M)N$. Next, we claim that $\mathrm{Z}(M)\cap N=\mathrm{Z}(G)$. If $\mathrm{Z}(M)\cap N\neq\mathrm{Z}(G)$, then

$$M=\mathrm{C}_G\big(\mathrm{Z}(M)\cap N\big)\geq\mathrm{C}_G(N)=\mathrm{Z}(N),$$

which implies that $\mathrm{Z}(M) = \mathrm{C}_G(M) \leq \mathrm{C}_G\big(\mathrm{Z}(N)\big) = N$, a contradiction. Similarly, we can prove that $M \cap \mathrm{Z}(N) = \mathrm{Z}(G)$.

Set $R = \mathrm{Z}(M)\,\mathrm{Z}(N)$ and $S = M \cap N$. Notice that

$$\mathrm{Z}(M)/\mathrm{Z}(G) = \mathrm{Z}(M)/\big(\mathrm{Z}(M) \cap N\big) \cong \mathrm{Z}(M)N/N = G/N.$$

Thus, $|\mathrm{Z}(M)/\mathrm{Z}(G)| = p$, and similarly $|\mathrm{Z}(N)/\mathrm{Z}(G)| = p$. It follows that R is non-abelian with $|R/\mathrm{Z}(R)| = p^2$ and $S = \mathrm{C}_G(R)$. Further, it is easy to see that

$$\mathrm{Z}(R) = \mathrm{Z}(G) = \mathrm{Z}(S) = R \cap S,$$

and hence $G = RS$ is a central product. □

Finally, we present [34, Proposition 3.4].

Theorem 5.48 *Let G be a finite p-group with elementary abelian center such that $\mathrm{C}_G(\mathrm{Z}(\Phi(G))) \neq \Phi(G)$ and $\mathrm{Z}(G) < \mathrm{Z}(M)$ for all maximal subgroups M of G. Then $|G|$ divides $|\mathrm{Aut}(G)|$.*

Proof If $|\mathrm{Z}(G)| = p$, then the result follows from Theorem 1.32. So assume that $|\mathrm{Z}(G)| \geq p^2$. By the proof of Lemma 5.47, there exist maximal subgroups M and N such that $G = \mathrm{Z}(M)N$ and $\mathrm{Z}(G) = \mathrm{Z}(M) \cap N$. Thus, we have

$$\mathrm{Z}(M)/\mathrm{Z}(G) = \mathrm{Z}(M)/\big(\mathrm{Z}(M) \cap N\big) \cong \big(\mathrm{Z}(M)N\big)/N = G/N.$$

Write $G/M = \langle Mg \rangle$ for some $g \in G$. Let τ and γ be as in the discussion preceding Theorem 5.45. Since $\mathrm{Z}(G) \leq \mathrm{Ker}(\tau)$, it follows that $|\operatorname{Im}(\tau)| \leq p$. For simplicity of notation, we set

$$\mathrm{Out}^{M,G/M}(G) = \mathrm{Aut}^{M,G/M}(G)\,\mathrm{Inn}(G)/\,\mathrm{Inn}(G).$$

By Corollary 1.37, we obtain

$$|\,\mathrm{Out}^{M,G/M}(G)| = |\,\mathrm{Ker}(\gamma)/\operatorname{Im}(\tau)|.$$

If $\operatorname{Im}(\tau) = 1$, then $|\,\mathrm{Out}^{M,G/M}(G)| = |\mathrm{Z}(G)|$, and we are done. Hence, we assume that $\operatorname{Im}(\tau) \cong \mathrm{C}_p$. In this case, we have

$$|\,\mathrm{Out}^{M,G/M}(G)| = |\mathrm{Z}(G)|/p.$$

By Lemma 5.47, G is a central product of subgroups R and S with

$$R/\mathrm{Z}(R) \cong \mathrm{C}_p \oplus \mathrm{C}_p$$

and

$$\mathrm{Z}(R) = \mathrm{Z}(G) = \mathrm{Z}(S) = R \cap S.$$

Furthermore, $R = \mathrm{Z}(M)\,\mathrm{Z}(N)$ and $S = M \cap N = \mathrm{C}_G(R)$. By Theorem 1.33, there exists a non-inner automorphism $\beta \in \mathrm{Aut}^{\mathrm{Z}(S)}(S)$ of p-power order. Since

$$\mathrm{Z}(G) = \mathrm{Z}(S) = R \cap S,$$

the automorphism β uniquely extends to a non-inner automorphism $\tilde{\beta} \in \mathrm{Aut}^{\mathrm{Z}(G),R}(G)$.

Certainly, $\tilde{\beta}$ does not act trivially on $M \cap N = S$, and hence $\tilde{\beta} \notin \mathrm{Aut}^{M}(G)$. We show that $\mathrm{Inn}(G)\tilde{\beta} \notin \mathrm{Out}^{M,G/M}(G)$. Contrarily suppose that $\tilde{\beta} = \iota_x \rho$ for some $\iota_x \in \mathrm{Inn}(G)$ and $\rho \in \mathrm{Aut}^{M,G/M}(G)$, where $x \in G$. As $S \leq M$, we have

$$\beta(s) = \tilde{\beta}(s) = \iota_x\big(\rho(s)\big) = \iota_x(s)$$

for all $s \in S$. Write $x = rs'$ for some $r \in R$ and $s' \in S$. Since $S = \mathrm{C}_G(R)$, we obtain $\beta(s) = \iota_{s'}(s)$. This implies that $\beta \in \mathrm{Inn}(S)$, a contradiction. Hence, $\mathrm{Inn}(G)\tilde{\beta} \notin \mathrm{Out}^{M,G/M}(G)$, and we obtain

$$|\,\mathrm{Out}(G)|_p \geq |\langle \mathrm{Inn}(G)\tilde{\beta}, \mathrm{Out}^{M,G/M}(G)\rangle| \geq |\,\mathrm{Z}(G)|,$$

which was desired. □

Remark 5.49 It would be interesting to explore whether finite p-groups G with $\mathrm{Z}(G)$ elementary abelian, $\mathrm{Z}(G) < \mathrm{Z}(M)$ for all maximal subgroups M of G and $\mathrm{C}_G\left(\mathrm{Z}(\Phi(G))\right) = \Phi(G)$ satisfy Divisibility Property.

Chapter 6
Groups Without Divisibility Property

We conclude the monograph by showing the existence of finite p-groups without Divisibility Property. This is a recent work of González-Sánchez and Jaikin-Zapirain [46]. Uniform pro-p-groups, uniform $\mathbb{Z}_p$-Lie algebras, continuous cohomology, and existence of a 41-dimensional $\mathbb{Q}$-Lie algebra with one dimensional center and admitting only inner derivations, are the main tools in this work.

6.1 Lie Algebras and Uniform Pro-p-Groups

In this section we recall some basics from the theory of Lie algebras and uniform pro-p-groups which are needed in the proof of the main result of [46].

Let R be a commutative ring. An R-Lie algebra is an R-module L with a binary operation

$$[-,-] : L \times L \to L,$$

called the *Lie bracket*, that is R-bilinear and satisfies the following conditions:

(1) $[x, x] = 0$ for all $x \in L$;
(2) $[[x, y], z] + [[y, z], x] + [[z, x], y] = 0$ for all $x, y, z \in L$ (Jacobi identity).

Expanding the Lie bracket $[x + y, x + y]$ and using bilinearity together with condition (1) yields

(3) $[x, y] = -[y, x]$ for all $x, y \in L$.

Further, if 2 is invertible in R, then condition (3) implies condition (1). Throughout this chapter, the notation $[-,-]$ stands for the Lie bracket, and it does not conflict with the group commutator notation as the latter is not used in this chapter. Given elements $x_1, \ldots, x_n \in L$, we set

$$[x_1, \ldots, x_n] = [\ldots[[x_1, x_2], x_3], \ldots, x_n],$$

I. B. S. Passi et al., *Automorphisms of Finite Groups*, Springer Monographs in Mathematics, https://doi.org/10.1007/978-981-13-2895-4_6

called the *left-normed Lie bracket* of $x_1, \ldots, x_n$. If L_1 and L_2 are two R-Lie algebras, then an R-module homomorphism $f : L_1 \to L_2$ satisfying

$$f\big([x, y]\big) = \big[f(x), f(y)\big]$$

for all $x, y \in L_1$, is called a *Lie algebra homomorphism.*

For example, any associative algebra A over a commutative ring R can be turned into an R-Lie algebra by defining the Lie bracket on A as

$$[a, b] = ab - ba$$

for $a, b \in A$. In particular, if M is an R-module, then the set $\mathrm{End}_R(M)$ of all R-module endomorphisms of M is an associative R-algebra in the usual way. And thus, $\mathrm{End}_R(M)$ can be viewed as an R-Lie algebra.

Let L be an R-Lie algebra and M an R-module. An *L-module* structure on M is a Lie algebra homomorphism

$$L \to \mathrm{End}_R(M).$$

For each $x \in L$, let $ad_x : L \to L$ be the map defined by

$$ad_x(y) = [x, y]$$

for $y \in L$. Taking $M = L$ as the R-module, we see that $ad_x \in \mathrm{End}_R(L)$ for each $x \in L$. Notice that the Jacobi identity is equivalent to saying that the map

$$ad : L \to \mathrm{End}_R(L)$$

given by $x \mapsto ad_x$ is a Lie algebra homomorphism, also referred to as the *adjoint representation* of the Lie algebra L.

Let L be an R-Lie algebra. Then an R-linear map $d : L \to L$ is called a *derivation* of L if

$$d\big([x, y]\big) = \big[d(x), y\big] + \big[x, d(y)\big]$$

for $x, y \in L$. The set of all derivations of L, denoted $\mathrm{Der}(L)$, forms a Lie subalgebra of $\mathrm{End}_R(L)$ and called the *derivation algebra* of L. Further, each ad_x is also a derivation of L called an *inner derivation.* The set of all inner derivations, denoted $\mathrm{InnDer}(A)$, is a Lie subalgebra of $\mathrm{Der}(L)$.

We now recall the definition of Lie algebra cohomology. In contrast to rest of the monograph, *the cohomology groups dealt with in this section are written additively so that they can be viewed as modules over some appropriate rings.*

Let R be a field, L an R-Lie algebra and M an L-module. Set $\Lambda^0(L) = R$. For each integer $k \geq 1$, let $\Lambda^k L$ denote the kth exterior power of L and set

$$C^k(L, M) := \mathrm{Hom}_R\left(\Lambda^k L, M\right).$$

Define $\partial^k : C^k(L,\ M) \to C^{k+1}(L,\ M)$ by setting

$$\partial^k(\nu)(x_0, \ldots, x_k) = \sum_{i=0}^{k}(-1)^i\ x_i\ \nu\big(x_0, \ldots, x_{i-1}, x_{i+1}, \ldots, x_k\big)$$
$$+ \sum_{0\le i<j\le k} (-1)^{i+j}\ \nu\big([x_i, x_j], x_0, \ldots, x_{i-1}, x_{i+1}, \ldots, x_{j-1}, x_{j+1}, \ldots, x_k\big)$$

for $\nu \in C^k(L,\ M)$. It is easy to verify, using the Jacobi identity and the L-module structure on M, that $\partial^k\partial^{k-1}$ is the trivial homomorphism, and hence $\{C^*(L,\ M), \partial^*\}$ is a cochain complex. The cohomology groups $\mathrm{H}^*_{Lie}(L,\ M)$ of this cochain complex are called the *Lie algebra cohomology groups* of L with coefficients in M.

If we take $M = L$ with the adjoint representation $ad : L \to \mathrm{End}_R(L)$, then the cohomology groups $\mathrm{H}^*_{Lie}(L,\ L)$ contain structural information about L. In particular, it follows that

$$\mathrm{H}^1_{Lie}(L,\ L) = \mathrm{Der}(L)/\,\mathrm{InnDer}(L).$$

Let p be a prime. Let $\mathbb{Z}_p$ and $\mathbb{Q}_p$ be the ring of p-adic integers and the field of p-adic numbers, respectively. A $\mathbb{Z}_p$-Lie algebra L is said to be *uniform* if $L \cong \mathbb{Z}_p^k$ as a $\mathbb{Z}_p$-module for some integer k and $[L, L] \subseteq 2pL$.

Similarly, a pro-p-group G is said to be *uniform* if it is finitely generated, has no non-trivial element of finite order and $\gamma_2(G) \le G^{2p}$, where $G^{2p} = \overline{\langle g^{2p} \mid g \in G\rangle}$, the topological closure of the subgroup generated by $2p$th powers of elements of G. We refer the reader to [24] and the seminal paper [79] of Lazard for detailed account of uniform pro-p-groups and $\mathbb{Z}_p$-Lie algebras.

Let $\mathcal{L}$ be the category of uniform $\mathbb{Z}_p$-Lie algebras, and $\mathcal{G}$ the category of uniform pro-p-groups. Then there are functors

$$\mathbf{Exp} : \mathcal{L} \to \mathcal{G}$$

and

$$\mathbf{Log} : \mathcal{G} \to \mathcal{L}$$

described as follows.

Let G be a pro-p-group, $a \in G$ and $\lambda \in \mathbb{Z}_p$. Then define

$$\lambda a = \lim_{n\to\infty} a^{a_n}, \tag{6.1}$$

where (a_n) is a sequence of integers converging to λ. By [24, Lemma 1.24], the limit exists and the definition does not depend on the choice of the sequence (a_n).

If U is a uniform pro-p-group, then $\mathbf{Log}(U)$ is the $\mathbb{Z}_p$-Lie algebra with underlying set U and the scalar multiplication, the addition and the Lie bracket defined as follows [24, Theorem 4.30]: For $\lambda \in \mathbb{Z}_p$ and $a, b \in U$, λa is given by (6.1),

$$a + b = \lim_{n\to\infty} (a^{p^n} b^{p^n})^{1/p^n} \tag{6.2}$$

and

$$[a, b] = \lim_{n\to\infty} \left(a^{p^n} b^{p^n} a^{-p^n} b^{-p^n}\right)^{1/p^{2n}}. \tag{6.3}$$

If $f : U \to V$ is a group homomorphism between two uniform pro-p-groups, then $\mathbf{Log}(f) = f$ is a homomorphism of corresponding $\mathbb{Z}_p$-Lie algebras. In particular, conjugation in U gives a U-module structure on $\mathbf{Log}(U)$.

On the other hand, the passage from Lie algebra to the group structure is described in terms of the classical Baker–Campbell–Hausdorff formula. Let $\mathbb{Q}[[X, Y]]$ be the ring of formal power series over $\mathbb{Q}$ in two non-commuting variables X and Y. Then $\mathbb{Q}[[X, Y]]$ is an associative algebra and so can be viewed as a $\mathbb{Q}$-Lie algebra. Consider the power series

$$\sum_{n=0}^{\infty} \frac{X^n}{n!} \text{ and } \sum_{n=0}^{\infty} \frac{Y^n}{n!}$$

in $\mathbb{Q}[[X, Y]]$. Then their formal product can be written as $1 + p(X, Y)$, where $p(X, Y)$ is a power series with zero constant term. The essence of the Baker–Campbell–Hausdorff formula is that the nth term of the power series

$$\sum_{n=1}^{\infty} \frac{(-1)^{n+1}\ p(X, Y)^n}{n}$$

can be written as a Lie polynomial of degree n, that is, it is a linear combination of commutators of length n involving X and Y. More precisely, the nth term of the power series is $u_n(X, Y)$ as described below.

Let L be a $\mathbb{Q}_p$-Lie algebra. Let $x, y \in L$ and $e = (e_1, \ldots, e_k)$ be a vector of positive integers. Set

$$[x, y]_e = [x, \underbrace{y, \ldots, y}_{e_1}, \underbrace{x, \ldots, x}_{e_2}, \ldots],$$

the left-normed Lie bracket of total length $|e| + 1$, where

$$|e| = e_1 + \cdots + e_k.$$

Then the Baker–Campbell–Hausdorff series of L with respect to $x, y \in L$ is the series

$$\sum_{n=1}^{\infty} u_n(x, y),$$

where

$$u_1(x, y) = x + y,$$

$$u_2(x, y) = \frac{1}{2}[x, y]$$

and

$$u_n(x, y) = \sum_e q_e[x, y]_e \text{ for } n \geq 3. \tag{6.4}$$

Notice here that the summation in (6.4) is over all vectors e of positive integers satisfying $|e| = n - 1$, and the coefficients q_e are certain rational numbers satisfying the convergence condition

$$\lim_{|e|\to\infty} |p^{|e|}q_e| = 0.$$

Since each $u_n(x, y)$ is a finite sum, it can be evaluated in any $\mathbb{Q}_p$-Lie algebra. By [24, Corollary 6.38], if L is a uniform $\mathbb{Z}_p$-Lie algebra, then, in fact, each $u_n(x, y)$ can be evaluated in L, and furthermore, the series

$$\sum_{n=1}^{\infty} u_n(x, y)$$

converges in L. Therefore, given a uniform $\mathbb{Z}_p$-Lie algebra L, we can define the uniform pro-p-group $\mathbf{Exp}(L)$ as the set L with the group operation given by

$$xy := \sum_{n=1}^{\infty} u_n(x, y)$$

for $x, y \in L$. Then, by [24, Theorem 9.8], $\mathbf{Exp}(L)$ is a uniform pro-p-group. If $f : L \to M$ is a Lie algebra homomorphism between two uniform $\mathbb{Z}_p$-Lie algebras, then $\mathbf{Exp}(f) = f$ is a homomorphism of the corresponding uniform pro-p-groups.

The two functors **Exp** and **Log** are related as follows [24, Theorem 9.10]. Also, see [45, Theorem A] and [79].

Theorem 6.5 *The functor* ***Exp*** $: \mathcal{L} \to \mathcal{G}$ *is an isomorphism of categories with the functor* ***Log*** $: \mathcal{G} \to \mathcal{L}$ *as its inverse.*

Let U be a uniform pro-p-group. Then, for $i \leq j$, U acts on $\mho_i(U)/\mho_j(U)$ by conjugation. More precisely,

$${}^{u}\big(\mho_j(U)v\big) := \mho_j(U)uvu^{-1}$$

for $u \in U$ and $\mho_j(U)v \in \mho_i(U)/\mho_j(U)$. A consequence of the definition of addition in (6.2) is the following result.

Lemma 6.6 *Let U be a uniform pro-p-group. Let $i, j \in \mathbb{N}$ be such that $i \leq j \leq 2i+1$. Then $\mho_i(U)/\mho_j(U)$ is abelian and*

$$\mho_i(U)/\mho_j(U) \cong \boldsymbol{Log}(U)/p^{j-i}\,\boldsymbol{Log}(U)$$

as U-modules.

We recall the notion of a p-adic analytic profinite group. For an integer $r \geq 1$, let $\mathbb{Q}_p[[X_1, X_2, \ldots, X_r]]$ be the ring of formal power series over $\mathbb{Q}_p$ in commuting variables $X_1, X_2, \ldots, X_r$. For $x = (x_1, \ldots, x_r) \in \mathbb{Z}_p^r$ and $h \in \mathbb{N}$, we set

$$B(x, p^{-h}) = \left\{x + p^h y \mid y \in \mathbb{Z}_p^r\right\}.$$

It is easy to see that $B(x, p^{-h})$ is open in $\mathbb{Z}_p^r$, where $\mathbb{Z}_p^r$ is equipped with the product topology.

Let V be a non-empty open subset of $\mathbb{Z}_p^r$ and $f = (f_1, \ldots, f_s)$ a function from V to $\mathbb{Z}_p^s$. Then, for $x \in V$, we say that f is *analytic* at x if there exist $h \in \mathbb{N}$ with $B(x, p^{-h}) \subseteq V$ and formal power series $F_i(X) \in \mathbb{Q}_p[[X_1, X_2, \ldots, X_r]]$ $(i = 1, \ldots, s)$ such that

$$f_i(x + p^h y) = F_i(y)$$

for all $y \in \mathbb{Z}_p^r$. Further, f is analytic on V if it is analytic at each point of V.

For example, the function $f(z) = 1/z$ is analytic on the group of units $\mathbb{Z}_p^\times$ of $\mathbb{Z}_p$. It is not difficult to see that the composition of analytic functions is again analytic.

Let X be a topological space and U a non-empty open subset of X. A triple (U, ϕ, n) is called a *p-adic chart* on X if ϕ is a homeomorphism from U onto an open subset of $\mathbb{Z}_p^n$. Further, two p-adic charts (U, ϕ, n) and (V, ψ, m) on X are *compatible* if the maps $\psi\phi^{-1}|_{\phi(U\cap V)}$ and $\phi\psi^{-1}|_{\psi(U\cap V)}$ are analytic functions on $\phi(U \cap V)$ and $\psi(U \cap V)$, respectively. A *p-adic atlas* $\mathcal{A}_X$ on X is a set of pairwise compatible p-adic charts that covers the topological space X.

A *p-adic analytic manifold* structure on a topological space X is an equivalence class of compatible p-adic atlases on X. If such a structure exists, then X is called a p-adic analytic manifold. Any atlas belonging to the given equivalence class is called an atlas of X; and any chart belonging to such an atlas is called a chart of X.

For example, any discrete topological space X is a p-adic analytic manifold with the structure determined by the atlas $\left\{(\{x\}, \phi_x, 0) \mid x \in X\right\}$, where $\phi_x : x \to 0$. The topological spaces $\mathbb{Q}_p^n$ and $\mathrm{GL}(n, \mathbb{Z}_p)$ are p-adic analytic manifolds. Also, by [24, Theorem 4.9], uniform pro-p-groups are p-adic analytic manifolds.

Let X and Y be p-adic analytic manifolds and $f : X \to Y$ a function. We say that f is analytic if there exist p-adic atlases $\mathcal{A}_X$ on X and $\mathcal{A}_Y$ on Y such that for each pair of p-adic charts $(U, \phi, n) \in \mathcal{A}_X$ and $(V, \psi, m) \in \mathcal{A}_Y$, the set $f^{-1}(V)$ is open in X and the composition

$$\psi f \phi^{-1}|_{\phi\left(U\cap f^{-1}(V)\right)} : \phi\big(U \cap f^{-1}(V)\big) \to \mathbb{Z}_p^m$$

is an analytic function. The composition of analytic functions between p-adic analytic manifolds is analytic.

A topological group G is a *p-adic analytic group* if G has the structure of a p-adic analytic manifold such that the function

$$G \times G \to G$$

given by

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

for $x, y \in G$, is analytic.

For example, discrete groups, the additive group $\mathbb{Q}_p^n$ and the multiplicative group $\mathrm{GL}(n, \mathbb{Z}_p)$ are p-adic analytic groups. Also, by [24, Theorem 8.18], uniform pro-p-groups are p-adic analytic groups.

The following result guarantees the existence of a uniform pro-p-subgroup in a p-adic analytic profinite group. See [24, Theorem 8.29 and Theorem 8.31] or [79] for the original source.

Theorem 6.7 *Let G be a p-adic analytic profinite group. Then G contains an open uniform pro-p-subgroup U.*

For a p-adic analytic profinite group G, define its Lie algebra $\mathbf{L}(G)$ as the $\mathbb{Q}_p$-Lie algebra

$$\mathbf{L}(G) = \mathbf{Log}(U) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p.$$

Notice that the definition of $\mathbf{L}(G)$ does not depend on the choice of U. Further, the dimension of G is defined as

$$\dim(G) = \dim_{\mathbb{Q}_p} \big(\mathbf{L}(G)\big).$$

For a p-adic analytic pro-p-group G, the dimension $\dim(G)$ and $|G/\mho_i(G)|$ are related as follows ([24, Lemma 4.10], [79, Proposition III.3.1.8]).

Theorem 6.8 *Let G be a p-adic analytic pro-p-group. Then there exist positive constants c_1 and c_2 such that*

$$c_1\ p^{i \dim(G)} \leq |G/\mho_i(G)| \leq c_2\ p^{i \dim(G)}$$

for each i. Moreover, if G is uniform, then $|G/\mho_i(G)| = p^{i \dim(G)}$.

Finally, we recall the definition of continuous cohomology of topological groups for the convenience of the reader. Let G be a pro-p-group. An abelian Hausdorff topological group A is said to be a topological G-module if it is a left G-module such that the action $G \times A \to A$ is continuous. Set $C^{-1}(G, N) = 0$, and $C^0(G, N) = N$ viewed as maps from the trivial group to the group N. For each $n \geq 1$, the set

$$C^n_{cts}(G,\ A) := \big\{\mu : G^n \to A \mid\ \mu \text{ is a continuous function}\big\}$$

is an abelian group with

$$(\mu + \nu)(g_1,\ \dots,\ g_n) := \mu(g_1,\ \dots,\ g_n)\, \nu(g_1,\ \dots,\ g_n)$$

for $\mu, \nu \in C^n_{cts}(G,\ A)$. The coboundary operator

$$\partial^n : C^n_{cts}(G,\ A) \to C^{n+1}_{cts}(G,\ A)$$

is the same as in (2.1) given by

$$\begin{aligned} &\partial^n(\mu)(g_1,\ \dots,\ g_{n+1}) \\ &= {}^{g_1}\mu(g_2,\ \dots,\ g_{n+1}) \prod_{k=1}^{n} \mu(g_1,\ \dots,\ g_k g_{k+1},\ \dots,\ g_{n+1})^{(-1)^k}\, \mu(g_1,\ \dots,\ g_n)^{(-1)^{n+1}} \end{aligned} \tag{6.9}$$

for all $\mu \in C^n_{cts}(G,\ A)$ and $(g_1,\ \dots,\ g_{n+1}) \in G^{n+1}$. Then the cohomology groups $\mathrm{H}^*_{cts}(G,\ A)$ of the cochain complex $\{C^*_{cts}(G,\ A),\ \partial^*\}$ are called the *continuous cohomology* groups of G with coefficients in A. If A is a finite p-group, then

$$\mathrm{H}^n_{cts}(G,\ A) = \mathrm{H}^n(G,\ A),$$

the usual cohomology of G with coefficients in A. The reader is referred to [93, 119] for more details on continuous cohomology of p-adic analytic groups.

Let $\beta : A \to B$ be a continuous homomorphism of topological G-modules. Then, as in Corollary 2.3, for each $n \geq 0$, there is a homomorphism of cohomology groups

$$\beta^n : \mathrm{H}^n_{cts}(G,\ A) \to \mathrm{H}^n_{cts}(G,\ B)$$

given by

$$\beta^n\big([\mu]\big) = [\beta\mu].$$

Let G be a pro-p-group and $H < K$ open normal subgroups of G. Then the natural map $G/H \to G/K$ induces an epimorphism between the group algebras

$$\mathbb{Z}_p[G/H] \to \mathbb{Z}_p[G/K].$$

Thus, we obtain an inverse system of $\mathbb{Z}_p$-algebras whose inverse limit, denoted by $\mathbb{Z}_p[[G]]$, is called the *completed group algebra* of G. More precisely,

$$\mathbb{Z}_p[[G]] := \varprojlim \mathbb{Z}_p[G/U],$$

where U ranges over the inverse system of open normal subgroups of G (see [24, Section 7.4] for details). Then the following result holds [93, Lemma 2.7.2] (compare with Proposition 2.9).

Lemma 6.10 *Let G be a pro-p-group and*

$$0 \to A \overset{\alpha}{\to} B \overset{\beta}{\to} C \to 0$$

a short exact sequence of $\mathbb{Z}_p[[G]]$-modules with C finite. Then there exists an exact sequence

$$\mathrm{H}^1_{cts}(G,\ A) \overset{\alpha^1}{\to} \mathrm{H}^1_{cts}(G,\ B) \overset{\beta^1}{\to} \mathrm{H}^1_{cts}(G,\ C) \overset{\delta^1}{\to} \mathrm{H}^2_{cts}(G,\ A) \overset{\alpha^2}{\to} \mathrm{H}^2_{cts}(G,\ B),$$

where $\delta^1 : \mathrm{H}^1_{cts}(G,\ C) \to \mathrm{H}^2_{cts}(G,\ A)$ is the connecting homomorphism.

We need the following result [119, Proposition 4.2.2].

Theorem 6.11 *If G is a p-adic analytic pro-p-group and A is a topological G-module which is finitely generated as a $\mathbb{Z}_p$-module, then $\mathrm{H}^n_{cts}(G,\ A)$ is finitely generated as a $\mathbb{Z}_p$-module for each $n \geq 0$.*

6.2 Existence of Groups Without Divisibility Property

We begin the final section by proving finiteness of first cohomology of a uniform pro-p-group U for which all derivations of $\mathbf{L}(U)$ are inner.

Proposition 6.12 *Let U be a uniform pro-p-group such that the Lie algebra $\mathbf{L}(U)$ has only inner derivations. Then $\mathrm{H}^1_{cts}\big(U,\ \mathbf{Log}(U)\big)$ is finite.*

Proof Since U is a finitely generated pro-p-group and $\mathbf{Log}(U)$ is finitely generated as a $\mathbb{Z}_p$-module, by Theorem 6.11, it follows that $\mathrm{H}^1_{cts}\big(U,\ \mathbf{Log}(U)\big)$ is also finitely generated as a $\mathbb{Z}_p$-module. Thus, it is enough to show that $\mathrm{H}^1_{cts}\big(U,\ \mathbf{Log}(U)\big)$ is a torsion module, equivalently,

$$\mathrm{H}^1_{cts}\big(U,\ \mathbf{Log}(U)\big) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p = 0.$$

By [119, Theorem 3.8.2], we have

$$\mathrm{H}^1_{cts}\big(U,\ \mathbf{Log}(U)\big) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \cong \mathrm{H}^1_{cts}\big(U,\ \mathbf{L}(U)\big),$$

and, by [119, Theorem 5.2.4], we get

$$\mathrm{H}^1_{cts}\big(U,\ \mathbf{L}(U)\big) \cong \mathrm{H}^1_{Lie}\big(\mathbf{L}(U),\ \mathbf{L}(U)\big).$$

But,

$$\mathrm{H}^1_{Lie}\big(\mathbf{L}(U),\ \mathbf{L}(U)\big) = \mathrm{Der}\big(\mathbf{L}(U)\big)/\,\mathrm{InnDer}\big(\mathbf{L}(U)\big) = 0,$$

and the proof is complete. □

Next, we derive a bound for $|\,\mathrm{H}^1_{cts}\big(U,\ \mathbf{Log}(U)/p^i\mathbf{Log}(U)\big)|$ which is uniform for all i.

Proposition 6.13 *Let U be a uniform pro-p-group such that the Lie algebra $\mathbf{L}(U)$ has only inner derivations. Then there exists a constant C such that*

$$|\,\mathrm{H}^1_{cts}\big(U,\ \boldsymbol{Log}(U)/p^i\boldsymbol{Log}(U)\big)| \le C$$

for all i.

Proof Let $\alpha : \mathbf{Log}(U) \to \mathbf{Log}(U)$ be the multiplication by p^i. Then the induced map

$$\alpha^2 : \mathrm{H}^2_{cts}\big(U,\ \mathbf{Log}(U)\big) \to \mathrm{H}^2_{cts}\big(U,\ \mathbf{Log}(U)\big)$$

is also the multiplication by p^i, and hence $\mathrm{Ker}(\alpha^2) \le T$, where T is the torsion subgroup of $\mathrm{H}^2_{cts}\big(U,\ \mathbf{Log}(U)\big)$. Since U is a finitely generated pro-p-group and $\mathbf{Log}(U)$ is finitely generated as a $\mathbb{Z}_p$-module, by Theorem 6.11, it follows that $\mathrm{H}^2_{cts}\big(U,\ \mathbf{Log}(U)\big)$ is also finitely generated as a $\mathbb{Z}_p$-module. Consequently, T must be finite. Applying Lemma 6.10 for the short exact sequence

$$0 \to \mathbf{Log}(U) \xrightarrow{p^i} \mathbf{Log}(U) \to \mathbf{Log}(U)/p^i\mathbf{Log}(U) \to 0$$

of U-modules, we obtain

$$|\,\mathrm{H}^1_{cts}\big(U,\ \mathbf{Log}(U)/p^i\,\mathbf{Log}(U)\big)| \le |\,\mathrm{H}^1_{cts}\big(U,\ \mathbf{Log}(U)\big)|\ |T|.$$

Finally, the result follows by Proposition 6.12. □

The following result of Satô [110, Section 4], showing the existence of a $\mathbb{Q}$-Lie algebra M with its derivation algebra $\mathrm{Der}(M)$ consisting of only inner derivations, is the key to the main result of this section.

Proposition 6.14 *There exists a $\mathbb{Q}$-Lie algebra M such that* $\dim_{\mathbb{Q}}(M) = 41$, $\dim_{\mathbb{Q}}\big(\mathrm{Z}(M)\big) = 1$, *and the derived algebra* $\mathrm{Der}(M)$ *consists only of inner derivations.*

The Lie algebra M as in the preceding proposition allows construction of a uniform pro-p-group U such that $\mathbf{L}(U)$ admits only inner derivations. The algebra M has a sub-algebra M_0 such that $M = M_0 \otimes_{\mathbb{Z}} \mathbb{Q}$. Setting

$$L = p^2(M_0 \otimes_{\mathbb{Z}} \mathbb{Z}_p),$$

we see that L is a uniform $\mathbb{Z}_p$-Lie algebra. For the rest of this section, set

$$U = \mathbf{Exp}(L) \text{ and } U_i = U/\mho_i(U) \tag{6.15}$$

for each i. Then we have $L = \mathbf{Log}(U)$ and

$$\mathbf{L}(U) = L \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \cong M \otimes_{\mathbb{Q}} \mathbb{Q}_p.$$

Consequently, for the $\mathbb{Q}_p$-Lie algebra $\mathbf{L}(U)$, we have

$$\dim_{\mathbb{Q}_p}\big(\mathbf{L}(U)\big) = 41, \tag{6.16}$$

$$\dim_{\mathbb{Q}_p}\big(\mathrm{Z}(\mathbf{L}(U))\big) = 1 \tag{6.17}$$

and

$$\mathrm{Der}\big(\mathbf{L}(U)\big) = \mathrm{InnDer}\big(\mathbf{L}(U)\big). \tag{6.18}$$

For $i \geq j$, let

$$\pi_{i,j} : U_i \to U_j$$

be the natural projection and

$$\rho_{i,j} : \mathrm{Aut}(U_i) \to \mathrm{Aut}(U_j)$$

the map given by

$$\rho_{i,j}(\phi)\big(\mho_j(U)u\big) = \pi_{i,j}\big(\phi(\mho_i(U)u)\big)$$

for $\phi \in \mathrm{Aut}(U_i)$ and $u \in U$.

The next result is the final step towards the main theorem.

Proposition 6.19 *Let U and U_i be as in the preceding discussion. Then there exists a constant D such that*

$$|\,\mathrm{Aut}(U_i)/\,\mathrm{Inn}(U_i)| \leq D$$

for all i.

Proof By (6.18), the hypothesis of Proposition 6.13 holds, and hence there exists an integer k such that

$$p^k\,\mathrm{H}^1_{cts}\left(U,\ \mathbf{Log}(U)/p^i\,\mathbf{Log}(U)\right) = 0$$

for all i. Further, by Lemma 6.6, $\mho_{i-k}(U)/\mho_{i+1}(U)$ is abelian, and, further, it is isomorphic to $\mathbf{Log}(U)/p^{k+1}\mathbf{Log}(U)$ as an U-module. Consequently, we have

$$p^k\,\mathrm{H}^1_{cts}\left(U,\ \mho_{i-k}(U)/\mho_{i+1}(U)\right) = 0$$

for all i.

We now claim that

$$\operatorname{Ker}(\rho_{i,k}) \leq \operatorname{Inn}(U_i)\operatorname{Ker}(\rho_{i,i-k})$$

for all $i \geq 2k$. We proceed by induction on i. For $i = 2k$, the claim is obvious. Assume that the claim holds for $i \geq 2k$. Let $\phi \in \operatorname{Ker}(\rho_{i+1,k})$. Since $\rho_{i+1,i}(\phi) \in \operatorname{Ker}(\rho_{i,k})$, the induction hypothesis implies that $\phi \in \operatorname{Inn}(U_{i+1})\operatorname{Ker}(\rho_{i+1,i-k})$. Therefore, without loss of generality, we can assume that $\phi \in \operatorname{Ker}(\rho_{i+1,i-k})$.

Since $\phi \in \operatorname{Ker}(\rho_{i+1,i-k})$, we have $\phi\big(\mho_{i+1}(U)u\big)\big(\mho_{i+1}(U)u\big)^{-1} \in \mho_{i-k}(U)/\mho_{i+1}(U)$ for each $u \in U$. Thus, we can consider the map

$$c : U \to \mho_{i-k}(U)/\mho_{i+1}(U)$$

defined by

$$c(u) = \phi\big(\mho_{i+1}(U)u\big)\big(\mho_{i+1}(U)u\big)^{-1}$$

for $u \in U$. Further, for $u_1, u_2 \in U$, we have

$$c(u_1u_2) = \phi\big(\mho_{i+1}(U)u_1u_2\big)\big(\mho_{i+1}(U)u_1u_2\big)^{-1} = c(u_1)\,{}^{u_1}c(u_2),$$

and hence $c \in \mathrm{Z}^1\left(U,\ \mho_{i-k}(U)/\mho_{i+1}(U)\right)$.

Consider the following short exact sequence of U-modules

$$1 \to \mho_{i-k+1}(U)/\mho_{i+1}(U) \xrightarrow{\alpha} \mho_{i-k}(U)/\mho_{i+1}(U) \xrightarrow{\beta} \mho_{i}(U)/\mho_{i+1}(U) \to 1,$$

where α is the inclusion map and β is the p^kth power map. Then the induced homomorphism β^1 is multiplication by p^k. Hence, by Lemma 6.10, we have

$$\operatorname{Im}(\alpha^1) = \operatorname{Ker}(\beta^1) = \mathrm{H}^1_{cts}\left(U,\ \mho_{i-k}(U)/\mho_{i+1}(U)\right).$$

Therefore, there exist $c' \in \mathrm{Z}^1\left(U,\ \mho_{i-k+1}(U)/\mho_{i+1}(U)\right)$, and $v \in \mho_{i-k}(U)$ such that

$$c(u) = c'(u)\,\partial^0\big(\mho_{i+1}(U)v\big)(u) = c'(u)\,{}^{u}\big(\mho_{i+1}(U)v\big)\,\big(\mho_{i+1}(U)v\big)^{-1}$$

for each $u \in U$. Thus, for each $u \in U$, we obtain

$$\begin{aligned}
\phi\big(\mho_{i+1}(U)u\big) &= c(u)\,\big(\mho_{i+1}(U)u\big)\\
&= c'(u)\,{}^{u}\big(\mho_{i+1}(U)v\big)\,\big(\mho_{i+1}(U)v\big)^{-1}\,\big(\mho_{i+1}(U)u\big)\\
&= c'(u)\,\big(\mho_{i+1}(U)v\big)^{-1}\,{}^{u}\big(\mho_{i+1}(U)v\big)\,\big(\mho_{i+1}(U)u\big)\\
&= c'(u)\,\big(\mho_{i+1}(U)v\big)^{-1}\,\big(\mho_{i+1}(U)u\big)\,\big(\mho_{i+1}(U)v\big),
\end{aligned}$$

since $\mho_{i-k}(U)/\mho_{i+1}(U)$ is abelian. Since $c'(u) \in \mho_{i-k+1}(U)/\mho_{i+1}(U)$, we have $\phi \in \operatorname{Ker}(\rho_{i+1,i-k+1}) \operatorname{Inn}(U_{i+1})$, and the claim follows.

In view of the preceding discussion, we obtain

$$\begin{aligned} |\operatorname{Aut}(U_i)/\operatorname{Inn}(U_i)| &= |\operatorname{Aut}(U_i)/\operatorname{Inn}(U_i)\operatorname{Ker}(\rho_{i,i-k})|\,|\operatorname{Inn}(U_i)\operatorname{Ker}(\rho_{i,i-k})/\operatorname{Inn}(U_i)| \\ &\le |\operatorname{Aut}(U_i)/\operatorname{Ker}(\rho_{i,k})|\,|\operatorname{Ker}(\rho_{i,i-k})| \\ &\le |\operatorname{Aut}(U_k)|\,|\operatorname{Ker}(\rho_{i,i-k})|. \end{aligned}$$

Since U_i has 41 generators and $|\mho_{i-k}(U)/\mho_i(U)| = p^{41k}$, we obtain

$$|\operatorname{Ker}(\rho_{i,i-k})| \le p^{(41)^2 k},$$

and the proof is complete. □

Finally, we present the main result of González-Sánchez and Jaikin-Zapirain [46, Theorem 1.1] establishing the existence of finite p-groups without Divisibility Property.

Theorem 6.20 *For each prime p, the family of finite p-groups $\{U_i\}$ given by (6.15) satisfy*

$$\lim_{i\to\infty} |U_i| = \infty$$

and

$$\limsup_{i\to\infty} \frac{|\operatorname{Aut}(U_i)|}{|U_i|^{\frac{40}{41}}} < \infty.$$

In particular, for each prime p, there exists a non-abelian finite p-group G such that $|\operatorname{Aut}(G)| < |G|$.

Proof Notice that, by Theorem 6.8, we have

$$|U_i| = p^{41i}.$$

By (6.16) and (6.17), we have $\dim(U) = 41$ and $\dim\big(\operatorname{Z}(U)\big) = 1$, respectively, and therefore $\dim\big(U/\operatorname{Z}(U)\big) = 40$. Consequently,

$$|\operatorname{Inn}(U_i)| \le |U/\big(\mho_i(U)\operatorname{Z}(U)\big)| = p^{40i}$$

and $|\operatorname{Inn}(U_i)| \le |U_i|^{\frac{40}{41}}$. The result now follows from Proposition 6.19. □

Remark 6.21 In [14], Buckley asked whether converse of Theorem 4.6 is true. More precisely, if $G = A \times N$ is a finite p-group with A abelian and N purely non-abelian such that $|\operatorname{Aut}(G)|_p \ge |G|$, then $|\operatorname{Aut}(N)|_p \ge |N|$. Unfortunately, it is not true in general. For, by Theorem 6.20, there exists a finite p-group N such that $|N| = p^r\ |\operatorname{Aut}(N)|_p$ for some integer $r \ge 1$. Let A be an elementary abelian

p-group of rank d such that $d(d-3) \geq 2r$. Taking $G = A \times N$, we see that $|\operatorname{Aut}(G)|_p \geq |G|$.

We conclude the chapter with the following problem.

Problem 6.22 Construct explicit examples of finite p-groups without Divisibility Property. More precisely, construct such an example of the smallest order.

References

1. A. Ádem, R.J. Milgram, *Cohomology of Finite Groups*. Grundlehren der Mathematischen Wissenschaften, vol. 309, 2nd edn. (Springer, Berlin, 2004), viii+324 pp
2. A. Ádem, Automorphisms and cohomology of discrete groups. J. Algebra **182**(3), 721–737 (1996)
3. J.E. Adney, T. Yen, Automorphisms of p-groups. Ill. J. Math. **9**, 137–143 (1965)
4. J.L. Alperin, Groups with finitely many automorphisms. Pac. J. Math. **12**, 1–5 (1962)
5. T.M. Apostol, *Introduction to Analytic Number Theory*. Undergraduate Texts in Mathematics (Springer, New York, 1976), xii+338 pp
6. R. Baer, Erweiterungen von Gruppen und ihren Isomorphismen. Math. Z. **38**, 375–416 (1934)
7. R. Baer, Groups with preassigned central and central quotient group. Trans. Am. Math. Soc. **44**(3), 387–412 (1938)
8. R. Baer, Finite extensions of abelian groups with minimum condition. Trans. Am. Math. Soc. **79**, 521–540 (1955)
9. Y. Berkovich, Z. Janko, *Groups of Prime Power Order*. De Gruyter Expositions in Mathematics 47, vol. 2 (Walter de Gruyter GmbH & Co. KG, Berlin, 2008), xvi+596 pp
10. F.R. Beyl, J. Tappe, *Group Extensions, Representations, and the Schur Multiplicator*. Lecture Notes in Mathematics, vol. 958 (Springer, Berlin, 1982), iv+278 pp
11. K.S. Brown, *Cohomology of Groups*. Graduate Texts in Mathematics, vol. 87 (Springer, New York, 1982), x+306 pp
12. G. Birkhoff, P. Hall, On the order of groups of automorphisms. Trans. Am. Math. Soc. **39**, 496–499 (1936)
13. N. Blackburn, On a special class of p-groups. Acta Math. **100**, 45–92 (1958)
14. J. Buckley, Automorphism groups of isoclinic p-groups. J. Lond. Math. Soc. **12**, 37–44 (1975/76)
15. M.V.D. Burmester, T.G. Exarchakos, The function $g(h)$ for which $|A(G)|_p \geq p^h$ whenever $|G| \geq p^{g(h)}$, G a finite p-group. Bull. Soc. Math. Grèce (N.S.) **29**, 27–44 (1988)
16. W. Burnside, *Theory of Groups of Finite Order*, 2nd edn. (Dover Publications, Inc., New York, 1955), xxiv+512 pp
17. A. Caranti, C.M. Scoppola, Endomorphisms of two-generated metabelian groups that induce the identity modulo the derived subgroup. Arch. Math. **56**, 218–227 (1991)
18. R.M. Davitt, The automorphism group of a finite metacyclic p-group. Proc. Am. Math. Soc. **25**, 876–879 (1970)
19. R.M. Davitt, The automorphism group of finite p-abelian p-groups. Ill. J. Math. **16**, 76–85 (1972)

I. B. S. Passi et al., *Automorphisms of Finite Groups*, Springer Monographs
in Mathematics, https://doi.org/10.1007/978-981-13-2895-4

20. R.M. Davitt, On the automorphism group of a finite p-group with a small central quotient. Can. J. Math. **32**, 1168–1176 (1980)
21. R.M. Davitt, A.D. Otto, On the automorphism group of a finite p-group with the central quotient metacyclic. Proc. Am. Math. Soc. **30**, 467–472 (1971)
22. R.M. Davitt, A.D. Otto, On the automorphism group of a finite modular p-group. Proc. Am. Math. Soc. **35**, 399–404 (1972)
23. J. Dietz, Resurrecting wells exact sequence and Buckley's group action, in *Groups St Andrews 2013*. London Mathematical Society Lecture Note Series, vol. 422 (Cambridge University Press, Cambridge, 2015), pp. 209–224
24. J.D. Dixon, M.P.F. Du Sautoy, A. Mann, D. Segal, *Analytic Pro-p Groups*. Cambridge Studies in Advanced Mathematics, vol. 61, 2nd edn. (Cambridge University Press, Cambridge, 1999), xviii+368 pp
25. B. Eckmann, Cohomology of groups and transfer. Ann. Math. **58**(2), 481–493 (1953)
26. B. Eick, Automorphism groups of 2-groups. J. Algebra **300**, 91–101 (2006)
27. B. Eick, C. Leedham-Green, On the classification of prime-power groups by coclass. Bull. Lond. Math. Soc. **40**, 274–288 (2008)
28. G. Ellis, J. Wiegold, A bound on the Schur multiplier of a prime power group. Bull. Aust. Math. Soc. **60**, 191–196 (1999)
29. T.G. Exarchakos, On the number of automorphisms of a finite p-group. Can. J. Math. **32**, 1448–1458 (1980)
30. T.G. Exarchakos, LA-groups. J. Math. Soc. Jpn. **33**, 185–190 (1981)
31. T.G. Exarchakos, G.M. Dimakos, G.E. Baralis, Finite p-groups and their automorphisms. Far East J. Math. Sci. **47**, 167–184 (2010)
32. T.G. Exarchakos, G.M. Dimakos, G.E. Baralis, The function $g(h)$ for which $|Aut(G)|_p \geq p^h$ whenever $|G|_p \geq p^{g(h)}$, G a finite p-group II. Far East J. Math. Sci. **62**, 161–175 (2012)
33. R. Faudree, A note on the automorphism group of a p-group. Proc. Am. Math. Soc. **19**, 1379–1382 (1968)
34. G.A. Fernández-Alcober, A. Thillaisundaram, A note on automorphisms of finite p-groups. Glas. Mat. Ser. III **51**(71), 117–123 (2016)
35. S. Fouladi, A.R. Jamali, R. Orfi, Automorphism groups of finite p-groups of coclass 2. J. Group Theory **10**, 437–440 (2007)
36. G. Frobenius, Über auflösbare Gruppen II. Sitz. Wiss. Akad. Berlin **2**, 1027–1044 (1895)
37. J.A. Gallian, Finite p-groups with homocyclic central factors. Can. J. Math. **26**, 636–643 (1974)
38. The GAP Group, GAP: Groups, Algorithms, and Programming, Version 4.8.8 (2017), http://www.gap-system.org
39. W. Gaschütz, Kohomogische Trivialitäten und äussere Automorphismen von p-gruppen. Math. Z. **88**, 432–433 (1965)
40. W. Gaschütz, Nichtabelsche p-Gruppen besitzen äussere p-Automorphismen. J. Algebra **4**, 1–2 (1966)
41. N. Gavioli, The number of automorphisms of groups of order p^7. Proc. R. Ir. Acad. Sect. A **93**, 177–184 (1993)
42. N. Gavioli, V. Pannone, Frobenius partitions in extraspecial groups. Geom. Dedicata **74**, 313–323 (1999)
43. F.Q. Gouvêa, *p-adic Numbers. An Introduction*. Universitext, 2nd edn. (Springer, Berlin, 1997), vi+298 pp
44. J. González-Sánchez, A.P. Nicolas, A bound for the exponent of the Schur multiplier of a finite p-group. J. Algebra **324**, 2564–2567 (2010)
45. J. González-Sánchez, A.P. Nicolas, Uniform groups and Lie algebras. J. Algebra **334**, 54–73 (2011)
46. J. González-Sánchez, A. Jaikin-Zapirain, Finite p-groups with small automorphism group. Forum Math. Sigma **3**, e7, 11 pp. (2015)
47. G. Grätzer, *Lattice Theory: Foundation* (Birkhäuser/Springer Basel AG, Basel, 2011), xxx+613 pp

48. J.C. Harris, N.J. Kuhn, Stable decompositions of classifying spaces of finite abelian p-groups. Math. Proc. Camb. Philos. Soc. **103**(3), 427–449 (1988)
49. J.A. Green, On the number of automorphisms of a finite group. Proc. R. Soc. Lond. Ser. A. **237**, 574–581 (1956)
50. K.W. Gruenberg, *Cohomological Topics in Group Theory*. Lecture Notes in Mathematics, vol. 143 (Springer, Berlin, 1970), xiv+275 pp
51. M. Hall Jr., *The Theory of Groups* (The Macmillan Co., New York, 1959), xiii+434 pp
52. P. Hall, A contribution to the theory of groups of prime-power orders. Proc. Lond. Math. Soc. **36**, 29–95 (1934)
53. P. Hall, The classification of prime power groups. J. Reine Angew. Math. **40**, 130–141 (1940)
54. P. Hall, J.K. Senior, *The Groups of Order* 2^n *(*$n \leq 6$*)* (The Macmillan Co., New York; Collier-Macmillan, Ltd, London 1964), 225 pp
55. I.N. Herstein, J.E. Adney, A note on the automorphism group of a finite group. Am. Math. Mon. **59**, 309–310 (1952)
56. P. Hill, Remarks on a paper of Hobby and Wright. Proc. Am. Math. Soc. **13**, 80–81 (1962)
57. C.J. Hillar, D.L. Rhea, Automorphisms of finite abelian groups. Am. Math. Mon. **114**, 917–923 (2007)
58. H. Hilton, On the order of the group of automorphisms of an abelian group. Messenger Math. **38**, 132–134 (1909)
59. P.J. Hilton, U. Stammbach, *A Course in Homological Algebra*. Graduate Texts in Mathematics, vol. 4 (Springer, New York, 1971), ix+338 pp
60. C. Hobby, A characteristic subgroup of p-group. Pac. J. Math. **10**, 853–858 (1960)
61. C. Hobby, C.R.B. Wright, A generalization of a theorem of N. Itô on p-groups. Proc. Am. Math. Soc. **11**, 707–709 (1960)
62. H. Hopf, Fundamentalgruppe und zweite Bettische Gruppe. Comment. Math. Helv. **14**, 257–309 (1942)
63. J.C. Howarth, On the power of a prime dividing the order of the automorphism group of a finite group. Proc. Glas. Math. Assoc. **4**, 163–170 (1960)
64. N.J.S. Hughes, The structure and order of the group of central automorphisms of a finite group. Proc. Lond. Math. Soc. **52**, 377–385 (1951)
65. K.G. Hummel, The order of the automorphism group of a central product. Proc. Am. Math. Soc. **47**, 37–40 (1975)
66. B. Huppert, *Endliche Gruppen I*, Die Grundlehren der Mathematischen Wissenschaften, Band 134 (Springer, Berlin, 1967), xii+793 pp
67. O.J. Huval, A note on the outer automorphisms of finite nilpotent groups. Am. Math. Mon. **73**, 174–175 (1966)
68. K.H. Hyde, On the order of the Sylow subgroups of the automorphism group of a finite group. Glas. Math. J. **11**, 88–96 (1970)
69. K. Iwasawa, Über die endlichen Gruppen und die Verbände ihrer Untergruppen (German). J. Fac. Sci. Imp. Univ. Tokyo Sect. **I**(4), 171–199 (1941)
70. N. Itô, On a theorem of L. Rédei and J. Szép concerning p-groups. Acta Sci. Math. Szeged **14**, 186–187 (1952)
71. S. Jackowski, Z. Marciniak, Group automorphisms inducing the identity map on cohomology. Proceedings of the Northwestern conference on cohomology of groups (Evanston, Ill., 1985). J. Pure Appl. Algebra **44**(1–3), 241–250 (1987)
72. E. Jespers, A. Zimmermann, *Group Automorphism Action on Group Cohomology*, http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.618.1258&rep=rep1&type=pdf
73. P. Jin, Automorphisms of groups. J. Algebra **312**, 562–569 (2007)
74. P. Jin, H. Liu, The Wells exact sequence for the automorphism group of a group extension. J. Algebra **324**, 1219–1228 (2010)
75. M.R. Jones, Multiplicators of p-groups. Math. Z. **127**, 165–166 (1972)
76. G. Karpilovsky, *The Schur Multiplier*. London Mathematical Society Monographs. New Series, vol. 2 (The Clarendon Press, Oxford University Press, New York, 1987), x+302 pp
77. L.G. Kovacs, A non-extendable abstract kernel. Ill. J. Math. **47**, 327–328 (2003)

78. N.J. Kuhn, The nilpotent filtration and the action of automorphisms on the cohomology of finite p-groups. Math. Proc. Camb. Philos. Soc. **144**(3), 575–602 (2008)
79. M. Lazard, Groupes analytiques p-adiques. Inst. Hautes Études Sci. Publ. Math. **26**, 389–603 (1965)
80. W. Ledermann, B.H. Neumann, On the order of the automorphism group of a finite group. I. Proc. R. Soc. Lond. Ser. A. **233**, 494–506 (1956)
81. W. Ledermann, B.H. Neumann, On the order of the automorphism group of a finite group. II. Proc. R. Soc. Lond. Ser. A. **235**, 235–246 (1956)
82. C.R. Leedham-Green, S. McKay, *The Structure of Groups of Prime Power Order*. London Mathematical Society Monographs. New Series, vol. 27 (Oxford Science Publications, Oxford University Press, Oxford, 2002), xii+334 pp
83. A. Lubotzky, A. Mann, Powerful p-groups. I. Finite groups. J. Algebra **105**, 484–505 (1987)
84. I.D. Macdonald, Some p-groups of Frobenius and extra-special type. Isr. J. Math. **40**, 350–364 (1981)
85. S. Mac Lane, *Homology*. Classics in Mathematics. Reprint of the 1975 edition (Springer, Berlin, 1995), x+422 pp
86. J.S. Maginnis, Outer automorphisms of upper triangular matrices. J. Algebra **161**, 267–270 (1993)
87. W. Malfait, The (outer) automorphism group of a group extension. Bull. Belg. Math. Soc. **9**, 361–372 (2002)
88. J. Martino, S. Priddy, On the dimension theory of dominant summands, in *Adams Memorial Symposium on Algebraic Topology (Manchester, 1990)*. London Mathematical Society Lecture Note Series 175, vol. 1 (1992), pp. 281–292
89. V.D. Mazurov, E.I. Khukhro, *The Kourovka Notebook, Unsolved Problems in Group Theory*, 17th augmented edn. (Russian Academy of Sciences Siberian Division, Institute of Mathematics, 2010)
90. B. Mashayekhy, A. Hokmabadi, M. Mohammadzadde, On a conjecture of a bound for the exponent of the Schur multiplier of a finite p-group. Bull. Iran. Math. Soc. **37**, 235–242 (2011)
91. O. Müller, On p-automorphisms of finite p-groups. Arch. Math. (Basel) **32**, 533–538 (1979)
92. V.T. Nagrebeckii, The periodic part of a group with a finite number of automorphisms, (Russian). Dokl. Akad. Nauk SSSR **205**, 519–521 (1972)
93. J. Neukirch, A. Schmidt, K. Wingberg, *Cohomology of Number Fields*. Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 323, 2nd edn. (Springer, Berlin, 2008), xvi+825 pp
94. M.F. Newman, On subgroup commutators. Proc. Am. Math. Soc. **14**, 724–728 (1963)
95. M.F. Newman, E.A. O'Brien, *A CAYLEY library for the groups of order dividing 128*. Group theory (Singapore, 1987) (de Gruyter, Berlin, 1989), pp. 437–442
96. P. Niroomand, On the order of Schur multiplier of non-abelian p-groups. J. Algebra **322**, 4479–4482 (2009)
97. E.A. O'Brien, The groups of order 256. J. Algebra **143**(1), 219–235 (1991)
98. A.D. Otto, Central automorphisms of a finite p-group. Trans. Am. Math. Soc. **125**, 280–287 (1966)
99. I.B.S. Passi, M. Singh, M.K. Yadav, Automorphisms of abelian group extensions. J. Algebra **324**, 820–830 (2010)
100. A. Ranum, The group of classes of congruent matrices with application to the group of isomorphisms of any abelian group. Trans. Am. Math. Soc. **8**, 71–91 (1907)
101. R. Ree, The existence of outer automorphisms of some groups. II. Proc. Am. Math. Soc. **9**, 105–109 (1958)
102. D.J.S. Robinson, A contribution to the theory of groups with finitely many automorphisms. Proc. Lond. Math. Soc. **35**, 34–54 (1977)
103. D.J.S. Robinson, *A Course in the Theory of Groups*. Graduate Texts in Mathematics, vol. 80 (Springer, New York, 1982), xvii+481 pp
104. D.J.S. Robinson, Applications of cohomology to the theory of groups, in *Groups - St. Andrews 1981 (St. Andrews, 1981)*. London Mathematical Society Lecture Note Series, vol. 71 (Cambridge University Press, Cambridge, 1982), pp. 46–80

105. D.J.S. Robinson, *Automorphisms of Group Extensions*. Lecture Notes in Pure and Applied Mathematics, vol. 91 (1984), pp. 163–167
106. D.J.S. Robinson, Inducibility of automorphism pairs in group extensions, in *Encuentro en Teoría de Grupos y sus Aplicaciones (Zaragoza 2011)* (Revista Matemática Iberoamericana, Madrid, 2012), pp. 233–241
107. D.J.S. Robinson, Automorphisms of group extensions. Note Mat. **33**, 121–129 (2013)
108. E. Schenkman, The existence of outer automorphisms of some nilpotent groups of class 2. Proc. Am. Math. Soc. **6**, 6–11 (1955)
109. R. Schmidt, *Subgroup Lattices of Groups*. De Gruyter Expositions in Mathematics, vol. 14 (Walter de Gruyter & Co., Berlin, 1994), xvi+572 pp
110. T. Satô, The derivations of the Lie algebras. Tôhoku Math. J. **23**, 21–36 (1971)
111. P. Schmid, Normal p-subgroups in the group of outer automorphisms of a finite p-group. Math. Z. **147**, 271–277 (1976)
112. I. Schur, Über die Darstellung der endlichen Gruppen durch gebrochene lineare Substitutionen. J. Reine Angew. Math. **127**, 20–50 (1904)
113. I. Schur, Untersuchungen über die Darstellung der endlichen Gruppen durch gebrochene lineare Substitutionen. J. Reine Angew. Math. **132**, 85–137 (1907)
114. W.R. Scott, On the order of the automorphism group of a finite group. Proc. Am. Math. Soc. **5**, 23–24 (1954)
115. W.R. Scott, *Group Theory* (Prentice-Hall, Inc., Englewood Cliffs, 1964), xi+479 pp
116. Urs Stammbach, *Homology in Group Theory*. Lecture Notes in Mathematics, vol. 359 (Springer, Berlin, 1973), viii+183 pp
117. M. Suzuki, *Structure of a Group and the Structure of its Lattice of Subgroups*. Ergebnisse der Mathematik und ihrer Grenzgebiete, Neue Folge, Heft 10 (Springer, Berlin, 1956), 96 pp
118. M. Suzuki, *Group Theory II*, Translated from the Japanese. Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 248 (Springer, New York, 1986), x+621 pp
119. P. Symonds, T. Weigel, Cohomology of *p-adic analytic groups*, in *New Horizons in pro-p Groups*. Progress in Mathematics, vol. 184 (Birkhäuser, Boston, 2000), pp. 349–410
120. P. Symonds, The action of automorphisms on the cohomology of a p-group. Math. Proc. Camb. Philos. Soc. **127**(3), 495–496 (1999)
121. A. Thillaisundaram, The automorphism group for p-central p-groups. Int. J. Group Theory **1**, 59–71 (2012)
122. L.R. Vermani, *An Elementary Approach to Homological Algebra*. Monographs and Surveys in Pure and Applied Mathematics, vol. 130 (Chapman & Hall/CRC, Boca Raton, 2003), x+315 pp
123. U.H.M. Webb, An elementary proof of Gaschütz's theorem. Arch. Math. (Basel) **35**, 23–26 (1980)
124. P.M. Weichsel, On isoclinism. J. Lond. Math. Soc. **38**, 63–65 (1963)
125. A.J. Weir, Sylow p-subgroups of the general linear group over finite fields of characteristic p. Proc. Am. Math. Soc. **6**, 454–464 (1955)
126. C. Wells, Automorphisms of group extensions. Trans. Am. Math. Soc. **155**, 189–194 (1971)
127. J. Wiegold, Multiplicators and groups with finite central factor groups. Math. Zeit. **89**, 345–347 (1965)
128. M.K. Yadav, On automorphisms of finite p-groups. J. Group Theory **10**, 859–866 (2007)

Index

I. B. S. Passi et al., *Automorphisms of Finite Groups*, Springer Monographs in Mathematics, https://doi.org/10.1007/978-981-13-2895-4