Groups of small order type

Xueyu Pan

Main supervisor: Assoc. Prof. Heiko Dietrich

A thesis submitted for the degree of

Master of Philosophy

at Monash University in 2021

School of Mathematics

Monash University

Melbourne, Australia

2021

Contents

Copyright notice

I certify that I have made all reasonable efforts to secure copyright permissions for third-party content included in this thesis and have not knowingly added copyright content to my work without the owner's permission.

Abstract

It is a central theme in group theory to classify (finite) groups up to isomorphism. Of particular interest is the classification of all groups of a given order n; this has started with the work of Cayley and the introduction of axiomatically defined groups. Since then a vast amount of literature has emerged, dealing with groups of special orders or order types (that is, orders that factorise into a particular form, such as $n = pq$ for distinct primes p and q). The aim of this thesis is to investigate groups whose orders factorise into at most four primes. Theoretical classifications exist in the literature, but most expositions are lengthy and it is difficult to extract results. In this thesis we elaborate a new self-contained and independent determination of the isomorphism class representatives for these groups, presented in a unified and modern language; we derive explicit counting formulas and explicit group presentations. Importantly, our results lead to efficient construction algorithms for these groups, which we implement as a software package `SOTGrps` for the computer algebra system GAP. Our package extends the SmallGroups library of GAP and provides an identification functionality as well as a "construction-by-ID" method; this leads to a dynamic database of groups (where groups can be efficiently constructed on demand) and a practical isomorphism test. The approach used in this thesis can be extended to other order types. As an example, we include a new classification for the groups of order p^4q; this order type is also available in `SOTGrps`. Some results of this thesis also appear in the joint work (see [20]).

Declaration

I declare that this thesis contains no material which has been accepted for the award of any other degree or diploma at any university or equivalent institution and that, to the best of my knowledge and belief, this thesis contains no material previously published or written by another person, except where due reference is made in the text of the thesis.

Xueyu Pan

May 31, 2021

"You boil it in sawdust: you salt it in glue:
You condense it with locusts and tape:
Still keeping one principal object in view—
To preserve its symmetrical shape."

—Lewis Carroll (1876)

Acknowledgements

This thesis was supported by an Australian Government Research Training Program (RTP) Stipend and RTP Fee-Offset Scholarship through Federation University Australia.

Most of this work was written during a global pandemic. COVID-19 has greatly affected countless people's lives, including my own. This work and the published version would have not been possible were it not for the immense amount of support I have received.

First and most of all, I would like to express my deepest gratitude to my supervisor Assoc. Prof. Heiko Dietrich, for his kindest encouragement, patient guidance, extensive knowledge, and invaluable critiques. I am extremely grateful for his generous academic support throughout the years. I would also like to thank Prof. Bettina Eick for her collaboration, which brought about the published version of this work. I would like to express my appreciation to my co-supervisor Dr Santiago Barrera Acevedo, who has been exceedingly approachable; his invaluable advice and all the helpful discussions we had cannot be overestimated. Sincere thanks to Dr Daniel Mathews, Prof. Ian Wanless, Dr Norm Do, and Dr Mikhail Isaev, for their insightful comments and suggestions on this project. Thanks also to the friendly staff of the School of Mathematics, who offered me numerous resources and opportunities.

It has been an incredible journey, and I also wish to thank my peers and friends for their unwavering love and support during these two years. Many thanks to Alex, Kshitijia, and Jayden for the numerous interesting and useful discussions about and beyond mathematics. Special thanks to Fei, without whom the hundreds of days and nights during lockdown would be much less bearable.

Notation

$G, H, N, R, X, \Omega, \ldots$	groups, rings, sets, etc
Sym_n	symmetric group on $\{1, 2, \ldots, n\}$
Alt_n	alternating group on $\{1, 2, \ldots, n\}$
$\mathbb{N}$	non-negative integers
$\mathbb{Z}$	integers
$\mathbb{Z}_n$	integers $\{0, \ldots, n-1\}$
C_n	abstract multiplicative cyclic group of order n
$\mathrm{GF}(p^n)$	Galois field of order p^n, where p is a prime.
$\mathrm{GL}(V)$	group of all nonsingular linear transformations of the vector space V over a field $\mathbb{F}$
$\mathrm{GL}_n(\mathbb{F})$	general linear group of all invertible $n \times n$ matrices with coefficients in a field $\mathbb{F}$
$\mathrm{GL}_n(p^k)$	general linear group $\mathrm{GL}_n(\mathbb{F})$ where $\mathbb{F} \cong \mathrm{GF}(p^k)$
$\mathbb{I}_n$	the $n \times n$ multiplicative identity matrix
D_n	dihedral group of size $2n$
QD_n	quasidihedral group of size n
R^*	group of units of a unital ring R
$[g, h]$	commutator $g^{-1}h^{-1}gh$
$[G, H]$	subgroup generated by the set of all commutators $\{[g, h] : g \in G, h \in H\}$
$[G, G] = G'$	derived subgroup (commutator subgroup) of G
$Z(G) = \zeta(G)$	centre of G
$G^{(n)}$	the n-th term of the derived series of G, where $G^{(0)} = G$ and $G^{(i)} = [G^{(i-1)}, G^{(i-1)}]$ for $i \geq 1$
$\zeta_i(G)$	the i-th term in the upper central series of G, where $\zeta_0(G) = 1$ and $\zeta_i(G)/\zeta_{i+1}(G) = Z(G/\zeta_{i-1}(G))$ for $i \geq 1$

$\gamma_i(G)$	the i-th term in the lower central series of G, where $\gamma_0(G) = G$ and $\gamma_i(G) = [\gamma_{i-1}(G), G]$ for $i \geq 1$
$\mathrm{Aut}(G)$	automorphism group of G
$\mathrm{Inn}(G)$	inner automorphism group of G
$G \ltimes_\phi H$, $G \ltimes H$	semidirect product with a normal subgroup identified with H and the quotient isomorphic to G; G acts on H via $\varphi\colon G \to \mathrm{Aut}(H)$
$\mathrm{Stab}_G(X)$, $\mathrm{Stab}_G(x)$	stabiliser of a set X or an element x under the action of G
$\mathrm{Fix}_\Omega(G)$, $\mathrm{Fix}_\Omega(g)$	set of fixed points in a set Ω under the action of G or of $g \in G$
$N_G(H)$	normaliser of $H \leq G$ in G
$C_G(H)$	centraliser of $H \leq G$ in G
$\mathrm{Syl}_p(G)$	complete set of Sylow p-subgroups of G
$O_p(G)$	intersection of all Sylow p-subgroup of G
$\Phi(G)$	Frattini subgroup of G
$F(G)$	Fitting subgroup of G
Δ_x^y	divisibility Kronecker delta function for integers x and y where $\Delta_x^y = 1$ if $y \mid x$ and $\Delta_x^y = 0$ otherwise

Part I

Background

Chapter 1

Introduction

Group theory has ubiquitous applications in the study of mathematics as well as other subjects of science, including particle and quantum physics, crystallography, and molecular chemistry. In many of these areas, the theory of groups is applied to obtain information of the symmetry of an object, which benefits from a priori knowledge of the different structures of groups.

1.1 Groups of small order type

Following Cayley's classification [17] of all groups of order at most 6, the determination of a complete and irredundant list of groups of a given order up to isomorphism makes one of the oldest and most studied problems in finite group theory. A generalisation of this problem is to classify finite groups with a given order type given by a formula of the prime factorisation, which defines an infinite set of orders. As an example, for each positive integer $n \leq 7$ the groups of order p^n for all primes p have been explicitly classified (see [28, 31, 36, 41]) by a list parametrised presentations. The p-group generation algorithm developed by Newman [39] and O'Brien [40] can be used for the construction of these groups. In this thesis, we focus on groups *small order types*, namely, orders with a short prime factorisation and we derive a useful algorithm for the construction and enumeration for these groups. More specifically, we explicitly determine the isomorphism class representatives for all groups whose orders factorise into at most four (not necessarily distinct) primes and briefly discuss possible generalisations to more order types, such as order p^4q, where p and q are distinct primes.

A general approach to the determination of finite groups of a given order involves two steps: first construct a list of groups that contains each isomorphism type at least once, then reduce the list to isomorphism class representatives. Thanks to the Jordan–Hölder theorem and the classification of finite simple groups, the first step can be achieved by iterating group extensions with simple factors to construct nonsimple groups. The quest of finding all extensions of a given group N by a given group G is known as the *extension problem* of groups, formulated by Hölder. However, the process of iterated extensions often produces a redundant list. Thus, the predominant difficulty lies in the second step to determine the isomorphism classes of these extensions. This step is sometimes referred to as *solving the isomorphism problem*. In practice, another difficulty of listing the isomorphism representatives can be caused by the immensity of the list size. For example, Besche, Eick, and O'Brien [7] found in 2001 that there are 49 487 365 422 groups (up to isomorphism) of order 2^{10}. In fact, a closed formula for the number of

isomorphism types of groups of a given order is a closely related problem to the classification of finite groups; for more details we refer to the book of Blackburn et al. [11].

The classification of groups of some small order types appeared in many publications (for example, see [15, 18, 25, 31, 37, 51]), but the results are scattered over the literature and many of them are presented with terminology different from what is commonly seen today. It is also known that some papers contain erroneous classifications, which is unsurprising given that many of the early works involved a lot of technical (hand) calculations and case distinctions. Such factors often make it challenging to set a comprehensive overview on this topic. For this reason, this thesis reviews and integrates relevant literature to present an overview of the known results in a modern, unified language. More than just a revision of existing results, this integration complements our new results and makes this thesis a self-contained exposition of groups of some small order types. In particular, we give an explicit list of isomorphism class representatives for groups whose orders factorise into at most four primes. Our enumeration results for these groups follow from the explicit construction of the isomorphism class representatives. Moreover, our approach to studying these groups can be extended to more order types, such as $p^n q$, $p^n q^2$ for larger n and orders that are cubefree. Many results regarding orders with short prime factorisation length exist in the literature: Cole and Glover [18] determined groups whose orders are products of three primes; the enumeration of the isomorphism types of groups of order that factorises into at most four primes or of order $p^n q$ for $n \leq 5$ is known (see [24, 25, 37]); a construction function and an isomorphism test for cubefree groups arise from [19] and [22]. However, these works do not naturally give rise to an efficient identification function; that is, a function that determines the isomorphism type of a given group. On the other hand, our explicit determination of the isomorphism class representatives directly leads to an identification function. Furthermore, this function also relatively efficiently determines whether two groups (of order that we are concerned with in this thesis) are isomorphic. As many applications benefit from this information, such an identification function not only contributes to new results in computational group theory, but also contributes to other scientific areas where finite group theory applies.

We briefly comment on how the collaboration and joint paper [20] came about. As outlined above, the original aim of this MPhil thesis was to inspect existing classifications of groups of small order type, to write down a new compact comprehensive account using modern language of computational group theory, and to develop independent construction algorithms and implementations for the computer algebra system GAP. After we have achieved this revised classification, it turned out that we not only had the tools for an efficient construction algorithm, but also for a practical group identification routine. In particular, our explicit lists of group presentations also led to counting formulas for the isomorphism types of groups of a fixed small order type. In 2017, Bettina Eick has published an arXiv article [24] on the enumeration of groups of order $n \in \{p^2q, p^2q^2, p^3q, p^2qr\}$ and posed a research question asking for an explicit classification of these groups. This has been achieved by our work, and so we contemplated publishing our results. However, most of our construction proofs go hand in hand with proving an enumeration formula, so our paper would have had a significant overlap with Eick's preprint [24]. We decided that it would be most appropriate if we would publish all these results in a joint paper [20]. In turn, the work on this publication has led to a more efficient presentation of our original classification results, which is why some parts of this thesis now employ methods described in [20, 24].

1.2 Computational results

Many studies in group theory involve extensive calculations. For example, the aforementioned project of constructing all groups of order up to 2000 would be impractical were it not for some specialised computer performances. The area of computational group theory has advanced significantly with the assistance of computer algebra systems, such as GAP [27] and MAGMA [12]. These programmes provide efficient tools to carry out sophisticated calculations of groups and many other algebraic objects. Arguably, they lay the foundation for much recent research in computational algebra and have gain high popularity in the research community. For this thesis, we use GAP to generate and verify our computational results. Thanks to Besche, Eick, and O'Brien [49], a dynamic database of finite groups called the *SmallGroups Library* has been created and made available in both GAP and MAGMA, and is under ongoing development. A main result of this thesis is to extend the functionalities of GAP's SmallGroups Library to construct, enumerate, and identify the isomorphism types of groups of small order type by a new package called `SOTGrps`.[1] More specifically, given an order n that factorises into at most four primes or is of the form p^4q, we provide an algorithm to construct an ordered list $\mathcal{L}_n$ of all isomorphism representatives of the groups of order n. We also give an enumeration function that determines $|\mathcal{L}_n|$ without creating $\mathcal{L}_n$. Moreover, we provide an identification function: for a given group G, it determines the group ID (n, i) such that $n = |G|$ and G is isomorphic to the i-th group in $\mathcal{L}_n$; this group ID is an isomorphism invariant: two groups are isomorphic if and only if they have the same group ID.[2] We comment on the functionality of our implementations and development of the `SOTGrps` package in GAP at the end of the thesis.

1.3 Structure of the thesis

This thesis consists of three parts. The first part sets up the background theory, where we review some definitions and fundamental results of group extensions. We also underline a few specific results on the classification of split extensions, which are crucial to our later discussion in Part II. For convenience and ease of reference, we collect a number of general group theory definitions and preliminary results and present them in Appendix A. Although we employ different methods for the construction of groups of different order types, the overarching approach is via group extension. We observe that most of the order types discussed in this thesis define solvable groups. For example, all finite p-groups are solvable, all groups of order p^aq^b are solvable by a celebrated result of Burnside[14], and all groups of odd order are solvable by the famous odd-order theorem of Feit and Thompson [26]. Finite solvable groups have polycyclic presentations. Such presentations of groups allow us to employ efficient methods to study and construct group extensions computationally. We briefly recall the definitions and show an example of computations with polycyclic presentations in Chapter 3. In Chapter 4, we recall some results on automorphism groups and derive counting formulas for the conjugacy classes of certain subgroups in some low-dimensional general linear groups over finite fields. In conjunction with this, we introduce some notations that impose a *canonical* ordering of the lists of isomorphism class representatives that are constructed in Part II. Such a canonical ordering allows us to attach to each group a group ID, and is the key ingredient that leads to an identification function. This will be discussed in more detail in Part III.

[1] Short for "groups of small order types"; the `SOTGrps` package is available at github.com/xpan-eileen/sotgrps_gap_pkg.

[2] Throughout the thesis, by ID we implicitly mean the ordering of our construction in `SOTGrps` unless otherwise specified. It is noteworthy that this ordering is likely to differ from what is available in GAP's SmallGroups Library due to different methods and approaches used to construct the groups.

To be more specific, in Part II we explicitly determine the isomorphism representatives for groups whose orders factorise into at most four primes. As mentioned before, these groups have been discussed in many papers, but we collate and present the results in this self-contained exposition. We divide our discussion of these groups into three chapters. In Chapter 5, we review the known results of p-groups of order dividing p^4 and we present a summary of results using methods and notations in line with what we establish in Part I. Chapter 6 is dedicated to the groups of order $p^a q^b$ with $a, b \geq 1$ and $a + b \leq 4$. For these groups, we make case distinctions by the existence of normal Sylow p- and q-subgroups, and the isomorphism types of these Sylow subgroups. We devote Chapter 7 to squarefree groups with at most four prime factors and the groups of order p^2qr, where p, q, r are distinct primes. We recall the Burnside–Hölder–Zassenhaus theorem [43, (10.1.10)] on groups whose Sylow subgroups are all cyclic, and apply the results to construct and identify the squarefree groups. For these groups, we make case distinction on the sizes of the centres and the derived subgroups. We observe that all groups discussed in Part II are solvable except for Alt_5, which has order 60. This group makes a special case of the groups of order p^2qr, and the remaining groups of such order type are all solvable with an abelian Fitting subgroup. We make a case distinction on the isomorphism types of the Fitting subgroups for the construction of such groups. We give polycyclic presentations for all relevant solvable groups. For each order type we also provide a brief historical summary of known results; see also Section 1.4 for further background.

In Part III we comment on the computational aspects and the development of the `SOTGrps` package. In particular, we compare the performance of the `SOTGrps` package with the existing functionalities in GAP and comment on the accuracy and efficiency of our algorithm. We give a brief discussion on potential further studies. For instance, we may generalise our results to more order types such as $p^n q$, $p^n q^2$, and cubefree orders. Indeed, we derive a complete list of explicit isomorphism representatives for groups of order $p^4 q$, which in combination with Chapter 6 makes most of the enumeration results of Eick and Moede [25] constructive. Moreover, we discuss how to extend the isomorphism test in `SOTGrps` (namely, the identification functionality) to an explicit isomorphism construction.

In conclusion, the main results of this thesis are the following:

1. A new concise and self-contained description of the determination of groups of order $n \in \{pq, p^2q, p^2q^2, p^3q, pqr, pqrs, p^2qr\}$ with p, q, r, s distinct primes, see Chapters 6 and 7.
2. New compact group presentations describing these groups, see Tables 6.1, 6.2, 6.3, 6.4, 7.1, 7.2, 7.3, and Notations 4.1.1, 4.2.1, 4.2.6.
3. New efficient construction and identification algorithms for these groups implemented for the computer algebra system GAP, see Section 8.2.

Lastly, we remark that in this thesis we try to be consistent with terminology and notation that are commonly seen, but sometimes it is inevitable to introduce some nonstandard ones for easy reference and better readability.

1.4 Historical background

In the following and throughout this thesis, let p, q, r, s denote primes. We classify orders that factorise into at most four primes into four types: prime powers dividing p^4, products of precisely two prime powers, products of precisely three prime powers, and products of precisely four primes.

Besche, Eick, and O'Brien [6] provided a historical background of the determination of small groups; here we present a summary for the history of p-group construction. We refer to [6] for further references.

- **1854**: Cayley determined the groups of order p.
- **1882**: Netto determined the groups of order p^2.
- **1893**: Cole and Glover, Young, and Hölder independently classified the groups of order p^3 and p^4.
- **1898**: Bagnera determined the groups of order p^5, but his initial work contained errors for order 2^5 and 3^5, the former of which was pointed out by Miller, and corrected by Bagnera in 1899.
- **1904**: Potron attempted to list the isomorphism representatives for the groups of odd order p^4.
- **1927**: Bender pointed out the errors of in the list for groups of order 3^5 in Bagnera's results and gave a list of groups of order dividing p^5 for odd primes. His list for order 3^5 was also incomplete for one maximal-class group was missing, which was included by Blackburn in 1958.
- **1930s–1960s**: Hall and Senior first independently and then collaboratively worked to give a list of the 2-groups of order up to 64.
- **1958**: Blackburn initiated the study of p-groups of maximal class, and gave a complete classification of 2- and 3-groups of maximal class.
- **1969**: James gave a list for the isomorphism types of groups of order 3^5.
- **1980**: James gave a list of groups of order p^6 for odd p.
- **1990**: O'Brien and Newman derived an algorithm, the p-group generation algorithm, for constructing p-groups up to isomorphism. In the same year, James, Newman, and O'Brien determined the groups of order 2^7.
- **2005**: O'Brien and Vaughan-Lee determined the number of isomorphism types of groups of order p^7 for odd p, and gave a list of the groups of order 3^7 and 5^7 using the p-group generation algorithm.

For groups of order $p^a q^b$ with p, q distinct primes, the following are recorded in the literature. For further background and reference, see [6] and [37].

- **1893**: Cole and Glover, and Hölder independently determined groups of order pq, p^2q.
- **1902**: La Vavasseur determined groups of order p^2q^2.
- **1903**: La Vavasseur determined groups of order $16p$ for odd prime p.
- **1909**: Tripp determined groups of order p^3q^2.
- **1919**: Nyhlén determined groups of order $16p^2$ and $8p^3$ for odd prime p.
- **1934**: Lunn and Senior determined groups of $16p$ and $32p$.

- **1982**: For positive integers a, b such that $a, b \neq 5$ and $a + b \leq 6$, Laue enumerated the isomorphism types of groups of order $p^a q^b$ for odd primes, and determined all groups of order 96. There are some errors in Laue's results for the special cases where $p = 2$ and $q = 3$ for groups of order $p^3 q$ and $p^4 q$, which are pointed out in [24].
- **1977**: Western determined the groups of order $p^3 q$. In the summary section [51, Section 26], a group is missing for the case $q \equiv 1 \bmod p$, but it is included in [51, Section 13]; this is pointed out in [24].
- **2001**: Besche and Eick [5] gave an algorithmic description of the construction of groups of order $p^n q$.
- **2018**: Eick and Moede [25] enumerated the groups of order $p^n q$ for $n \leq 5$.

The remaining order types pqr, $pqrs$, and p^2qr (with p, q, r, s pairwise distinct) often appear in the discussion of squarefree and cubefree orders in the literature. A brief timeline is as follows.

- **1893**: Hölder [31] determined groups of order pqr.
- **1895**: Hölder [32] classified groups of squarefree order.
- **1906**: Glenn [29] considered groups of order p^2qr but his work contains a few errors, some of which are pointed out in [24].
- **1982**: Laue [37] enumerated the isomorphism types of groups of order p^2qr without normal Sylow subgroups.
- **2005**: Dietrich and Eick [19] developed a construction algorithm for groups of cubefree order.
- **2007**: Slattery [16] developed an algorithm for the construction and identification of squarefree groups.
- **2011**: Qiao and Li [42] gave structural characterisation for groups of cubefree order.
- **2017**: Eick [24] enumerated the isomorphism types of groups of order p^2qr.
- **2020**: Dietrich and Wilson [22] developed an isomorphism test algorithm for cubefree groups.
- **2021**: Dietrich and Low [21] generalised [16] to groups whose Sylow subgroups are cyclic (C-groups), and developed an algorithm for the construction and identification of C-groups.

Chapter 2

Group extensions and cohomology

The Jordan–Hölder theorem on finite groups allows us to study a finite group via its composition series. Informally speaking, we can decompose a finite group into smaller building blocks and study the group in terms of its normal subgroups, quotients, and how they interact. On the other hand, if one knows how to build larger groups from small groups, then it is possible to survey all nonsimple finite groups inductively with information of smaller groups. In particular, the *extension problem* asks for all possible ways one can reconstruct a group with information of a normal subgroup and the corresponding quotient. In light of the Jordan–Hölder theorem, one can enumerate and classify finite nonsimple groups of a given order by solving the extension problem and the isomorphism problem at each point of the composition series.

In this chapter, we recall some relevant results about group extensions and cohomology groups, which are important and useful for our later investigation of groups of some small order types. Unless otherwise specified, all groups we consider are finite. For further background, we refer to [43, Chapter 11], [44, Chapter 9], and [45, Chapter 7].

Definition 2.0.1. Let N and G be groups. A group E is an *extension* of N by G if E has a normal subgroup $M \cong N$ with quotient $E/M \cong G$.

The group Sym_3, for example, has a cyclic normal subgroup $\mathrm{Alt}_3 \cong C_3$ with cyclic quotient $\mathrm{Sym}_3/\mathrm{Alt}_3 \cong C_2$, so Sym_3 is an extension of C_3 by C_2. In particular, such an extension is an example of *metacyclic* extensions. On the other hand, the direct product $C_3 \times C_2 \cong C_6$ is also an extension of C_3 by C_2, but nonisomorphic to Sym_3. In general, any direct product $G \times N$ is an extension of N by G, as well as an extension of G by N.

In the context of Definition 2.0.1, since we can embed N into E and identify G with the corresponding quotient, we lose no generality by considering N as a subgroup of E. By abuse of language, we use the term *group extension* for both the short exact sequence induced by $E/N \cong G$ and the extension group E.

We now introduce some notation and present some results regarding group extensions of abelian groups, which are crucial in later chapters. Suppose G acts on N via $\varphi\colon G \to \mathrm{Aut}(N)$. Then for each $g \in G$ and $n \in N$ we denote the image of n under the automorphism $\varphi(g)$ by $n^{\varphi(g)}$; often we simply write $n^g = n^{\varphi(g)}$ when the action φ is implicit. If N is abelian, then this furnishes N with the structure of a G-module. Conversely, if N is a G-module, then N is an abelian group such that G acts on N via some induced homomorphism $\varphi\colon G \to \mathrm{Aut}(N)$. Although the additive notation is commonly used to describe a module, in this thesis we use the

multiplicative notation for a G-module N, for it is more convenient when describing extensions by group presentations.

With said setting, suppose a group E contains a normal subgroup N and $G = E/N$. For the natural projection $\pi\colon E \to G$, we choose a transversal map $\tau\colon G \to E$ with $\tau(1) = 1$, such that $\pi \circ \tau$ is the identity map on G, with $T = \tau(G)$ a left transversal of N in E. In the following, for a fixed choice of τ, we denote $t_g = \tau(g)$ for $g \in G$. Since $E = \bigsqcup_{t\in T} tN$ is a disjoint union, every $x \in E$ can be written uniquely as $x = t_g n$ for $t_g \in T$ and $n \in N$. Since N is abelian, the conjugation action $\kappa\colon E \to \mathrm{Aut}(N)$ satisfies that $N \leq \mathrm{Ker}\,\kappa$, thus induces a well-defined action of E/N on N. This corresponds to the homomorphism $\varphi\colon G \to \mathrm{Aut}(N)$ given by $n^g = t_g^{-1} n t_g$ for all $g \in G$ and $n \in N$. Observe that $\pi(t_g) = g \in G$ for all $g \in G$, thus $\pi(t_{gh}) = \pi(t_g)\pi(t_h)$. Since $\mathrm{Ker}\,\pi = N$, we have $t_{gh} n_{gh} = t_g t_h$ for a unique $n_{gh} \in N$. Therefore, we can construct a well-defined map $\gamma\colon G \times G \to N$ by $\gamma(g,h) = t_{gh}^{-1} t_g t_h = n_{gh}$.

Moreover, suppose $a, b \in N$ and $g, h \in G$, then there exist $t_g, t_h, t_{gh} \in N$ such that $a t_h = t_h a^h$ and $t_{gh}\gamma(g,h) = t_g t_h$, it follows that

$$t_g a t_h b = t_g t_h t_h^{-1} a t_h b = t_{gh}\gamma(g,h) a^h b. \tag{2.0.1}$$

For a fixed transversal T, since every $e \in E$ can be written uniquely as $t_g a$ for some $t_g \in T$ and $a \in N$, the associativity of E shows that

$$\gamma(g,h)^k \gamma(gh,k) = \gamma(h,k)\gamma(g,hk) \tag{2.0.2}$$

for all $g, h, k \in G$. This describes an important identity of the map $\gamma\colon G \times G \to N$, related to so-called "2-cocyles" in the context of group cohomology, which we discuss in more detail in the following section.

Remark 2.0.2. If N is nonabelian, then the conjugation action of $E \to \mathrm{Aut}(N)$ does not induce an action of $G \to \mathrm{Aut}(N)$, but an "outer action" $G \to \mathrm{Aut}(N)/\mathrm{Inn}(N) \cong \mathrm{Out}(N)$. In the context of cohomology, the classification of equivalence classes of these extensions becomes much more complicated, but we will see in Section 2.4 that there are many results we can apply to classify the isomorphism classes in some special cases. For the purpose of this thesis, we thus restrict our attention to group extensions of abelian normal subgroups when we discuss their cohomology. We refer to [13, Chapter IV Section 6] for more details in regards to the cohomology of group extensions of nonabelian normal subgroups.

2.1 Cohomology of groups

There are many different ways to define group cohomology, arising from various contexts. In this thesis, we are only concerned with the 1- and 2-cohomology groups, which are closely related to group extensions. However, to acknowledge that concepts from homological algebra naturally and greatly contribute to the understanding of group extensions, we briefly digress to put this into a broader context by including a description of n-th cohomology groups. The following definition arises from the context of (co)chain complexes; it is an adaptation of Brown's discussion in [13, pp. 4–5]. For further discussion on group extensions and the relevant homological machinery, we refer to [13, 30, 44].

Definition 2.1.1. Let G be a group and let N be a G-module. Define $\tilde{C}^0(G,N) = N$, and for $n \geq 1$, write $\tilde{C}^n(G,N)$ for the set of all maps from G^n to N with component-wise multiplication; that is, if $\omega, v \in \tilde{C}^n(G,N)$, then ωv is defined by

$$(\omega v)(x_1,\ldots,x_n) = \omega(x_1,\ldots,x_n)v(x_1,\ldots,x_n), \forall x_i \in G.$$

With this multiplication, $\tilde{C}^n(G,N)$ is an abelian group, where elements are called *n-cochains*. An n-cochain $\omega \in \tilde{C}^n(G,N)$ is *normalised* if $\omega(x_1,x_2,\ldots,x_n) = 1$ whenever $x_i = 1$ for any $i \in \{1,\ldots,n\}$. Denote the subgroup of $\tilde{C}^n(G,N)$ consisting of all normalised cochains by $C^n(G,N)$. For $n \geq 0$, define $\partial^n \colon \tilde{C}^n(G,N) \to \tilde{C}^{n+1}(G,N)$ by

$$\begin{aligned}(\partial^n(\omega))(x_1,\ldots,x_{n+1}) = {} & \omega(x_1,\ldots,x_n)^{x_{n+1}} \cdot \omega(x_1,\ldots,x_n)^{(-1)^{n+1}} \\ & \cdot \prod_{i=1}^{n} \omega(x_1,\ldots,x_{i-1},x_ix_{i+1},x_{i+1},\ldots,x_{n+1})^{(-1)^i}.\end{aligned}$$

One defines $\tilde{Z}^n(G,N) = \operatorname{Ker}\partial^n$ as the group of *n-cocycles* of G with coefficients in N with respect to the G-module structure of N, and $Z^n(G,N)$ is the subgroup of all *normalised n-cocycles*. For $n \geq 1$, the image $\tilde{B}^n = \operatorname{Im}\partial^{n-1}$ is the group of *n-coboundaries*; $B^n(G,N)$ the group of all *normalised n-coboundaries*, and $\tilde{B}^0(G,N) = 1$. A straightforward calculation shows that $\tilde{Z}^n(G,N)/\tilde{B}^n(G,N) \cong Z^n(G,N)/B^n(G,N)$. The *n-th cohomology group* of G with coefficients in N is defined by

$$H^n(G,N) = Z^n(G,N)/B^n(G,N).$$

It is sometimes customary to write $H^n_\varphi(G,N)$ to highlight the G-action on N, but in this thesis we often drop the subscripts when there is no ambiguity of the G-module structure. Since we only consider normalised cocycles in our discussions, we often also drop the adjective "normalised".

Note that $Z^n(G,N)$ is not empty for it always contains the trivial map. For the case $n = 2$, the cocycles are precisely maps $\gamma \colon G \times G \to N$ that satisfy the relation in (2.0.2). In particular, this characterisation of 2-cocyles defined by (2.0.2) is called the *cocycle identity*. In addition, if $\gamma(g,1) = (1,g) = 1$, then γ is exactly a normalised 2-cocycle. Since (2.0.2) is a consequence of (2.0.1) in tandem with associativity of the multiplication in E, one can obtain an alternative definition of 2-cocylces and 2-coboundaries by generalising (2.0.1). For example, the following is adapted from Rotman's definition in [44, p. 504].

Definition 2.1.2. Let G be a group with a G-module N, and let E be an extension of N by G. A function $\gamma \colon G \times G \to N$ is a 2-cocycle if there exists a transversal map $\tau \colon G \to E$ such that

$$\gamma(g,h) = \tau(g)\tau(h)\tau(gh)^{-1}$$

for all $g,h \in G$; such a 2-cocycle is sometimes denoted by γ_τ. A function $\beta \colon G \times G \to N$ is a 2-coboundary if there exists a map $f \colon G \to N$ such that $f(1) = 1$ and

$$\beta(g,h) = f(gh)^{-1}f(g)^h f(h)$$

for all $g,h \in G$; such a 2-coboundary is sometimes denoted by β_f.

Since N is abelian, a direct computation shows that $Z^2(G,N)$ is an abelian group under multiplication $(\gamma\delta)(g,h) = \gamma(g,h)\delta(g,h)$ for all $\gamma,\delta \in Z^2(G,N)$ and $g,h \in G$. Further, Definition 2.1.2 gives the construction of a 2-cocycle using a transversal map from the quotient $G = E/N$ to E, where N is furnished with a G-module structure. Conversely, every 2-cocycle

defines an extension of N by G, as shown by the following well-known result; see also [43, pp. 316–317] and [44, Theorem 9.9].

Theorem 2.1.3 ([43], pp. 316–317, [44], Theorem 9.9)**.** *Let G be a group with a G-module N. For a 2-cocycle $\gamma \in Z^2(G,N)$, let*

$$E_\gamma = \{(g,n) \colon g \in G, n \in N\}$$

with multiplication

$$(g,n)(h,m) = \left(gh, n^h m \gamma(g,h)\right),$$

for all $(g,n),(h,m) \in E_\gamma$. Then the following statements hold.

(i) *E_γ is a group.*

(ii) *If E is an extension of N by G, then there exists a 2-cocycle $\gamma \in Z^2(G,N)$ such that $E \cong E_\gamma$.*

Proof. (i) First note that E_γ is closed under this multiplication by construction. A direct calculation shows that $1_{E_\gamma} = (1_G, 1_N)$, and for every $(g,n) \in E_\gamma$, there exists a unique inverse $(g,n)^{-1} = \left(g^{-1}, (n^{-1})^{(g^{-1})} \left(\gamma(g,g^{-1})\right)^{-1}\right) \in E_\gamma$. Associativity of the multiplication follows from the defining property of the 2-cocycle γ.
(ii) Let $\tau \colon G \to E$ be a transversal map, write $T = \operatorname{Im}\tau$ and $t_g = \tau(g)$. Let $\gamma \colon G \times G \to N$ be the 2-cocycle defined by $\gamma(g,h) = t_{gh}^{-1} t_g t_h$. Now consider the map $\alpha \colon E \to E_\gamma, \alpha(t_g a) = (g,a)$: it is well-defined and injective by the uniqueness of $t_g \in T$ and $a \in N$ in expressing $x = t_g a$ for any $x \in E$; it is surjective by construction. It follows from (2.0.2) and the definition of α that

$$\alpha((t_g a)(t_h b)) = \alpha(t_{gh}\gamma(g,h) a^h b) = (gh, a^h b \gamma(g,h)) = \alpha(t_g a)\alpha(t_h b),$$

which shows that α is a homomorphism. In conclusion, α is an isomorphism. □

From Theorem 2.1.3 it immediately follows that given a group G and a G-module N, every extension E of N by G is isomorphic to E_γ for some $\gamma \in Z^2(G,N)$, where E_γ is as described in Theorem 2.1.3. Note that in this construction, if γ is the trivial map, then $E_\gamma = G \ltimes N$ is a semidirect product of G and N.

Remark 2.1.4. In this thesis, when we write $G \ltimes_\varphi N$ for a semidirect of N by G, we usually consider the underlying set to be $G \times N$ with multiplication $(g,n)(h,m) = (gh, n^{\varphi(h)}m)$, where $n^{\varphi(h)}$ denotes h acting on n via $\varphi \colon G \to \operatorname{Aut}(N)$. When there is no ambiguity of the G-action on N, we often write $G \ltimes N$ with multiplication $(g,n)(h,m) = (gh, n^h m)$. Similar to that we write n^g for $(\varphi(g))(n)$, we generalise this superscript notation further to avoid clustered brackets. For example, since $\operatorname{Aut}(N)$ naturally acts on N, for a given $\alpha \in \operatorname{Aut}(N)$, we use n^α and $\alpha(n)$ intechangeably for the image of n under α; for $\alpha, \alpha' \in \operatorname{Aut}(N)$, we often write $n^{\alpha'\alpha}$ for $(\alpha \circ \alpha')(n)$ in line with the multiplication of $\operatorname{Aut}(N)$ defined by $\alpha'\alpha = \alpha \circ \alpha'$.

Definition 2.1.5. Let G be a group, N be a G-module, and E be an extension of N by G. If there exists a left transversal $T \subseteq E$ of N that is a group isomorphic to G, then E is a *split extension* of N by G, and the subgroup T is a complement of N in E.

Equivalently, an extension E *splits* over N by G if there exists a transversal map $\tau \colon G \to E$ that is a group homomorphism. For a semidirect product $G \ltimes N$, the map $g \mapsto (g,1)$ is such a transversal homomorphism. Conversely, suppose an extension E splits via a homomorphism $\tau \colon G \to E$, then for the natural projection $\pi \colon E \to G$, the transversal $T = \tau(G)$ of N in E

forms a group. Moreover, since every element in E can be then written uniquely in the form $t_g n$ for some $t_g \in T$ and $n \in N$, a direct computation shows that E is isomorphic to a semidirect product $G \ltimes N = \{(g,n)\colon g \in G, n \in N\}$ where the G-action on N is induced by a fixed isomorphism $T \cong G$ and the conjugation of T on N. In conclusion, an extension of N by G splits if and only if it is isomorphic to a semidirect product $G \ltimes N$. Moreover, it is known that the set of complements of N in $E = G \ltimes N$ is in bijection with the group of 1-cocycles, namely, $Z^1(G,N)$ (see [43, (11.1.2)]). We recall the definition of 1-cocycle in the following.

Definition 2.1.6. Let G be a group with a G-module N. Then a map $\theta\colon G \to N$ satisfying that $\theta(1) = 1$ and

$$\theta(gh) = \theta(g)^h \theta(h)$$

for all $g, h \in G$, is a *normalised* 1-*cocycle* (1-cocycles are also known as *derivations*). The set $Z^1(G,N)$ of all such maps with multiplication $(\theta\xi)(g) = \theta(g)\xi(g)$ is an abelian group.

Let $E = G \ltimes N$ as above. Then $G \cong \{(g,1)\colon g \in G\}$ is a complement of N in E. For every $\theta \in Z^1(G,N)$, a straightforward calculation shows that

$$(g,\theta(g))\,(h,\theta(h)) = \Big(gh, \theta(g)^h\theta(h)\Big) = (gh, \theta(gh)),$$

and

$$G_\theta = \{(g,\theta(g))\colon g \in G\} \cong G$$

is a complement of N in E. It is known [43, (11.1.2)] that all complements of N in $E = G \ltimes N$ can be constructed this way.

2.2 Equivalent extensions and 2-cohomology

We now investigate the so-called equivalence classes of extensions of N by G.

Theorem 2.1.3 shows that every extension E of an abelian $N \trianglelefteq E$ with quotient $G = G/N$ is isomorphic to a group E_γ for some $\gamma \in Z^2(G,N)$. Recall that it involves a choice of the transversal of N in E in constructing the 2-cocyle. It is known that two 2-cocycles defined by different choices of transversals differ by a 2-coboundary. To verify this, let $\tau, \tau'\colon G \to E$ be two transversal maps with $\tau(1) = \tau'(1) = 1$, and abbreviate $s_g = \tau'(g)$ and $t_g = \tau(g)$. Since $\pi(t_g) = g = \pi(s_g)$, where $\pi\colon E \to N$ is the natural projection, there is a unique $n_g \in N$ such that $s_g = t_g n_g$. This gives rise to a well-defined map $f\colon G \to N, g \mapsto n_g$ with $f(1) = 1$. Define $\gamma, \gamma'\colon G \times G \to N$ to be the corresponding 2-cocyles such that $\gamma(g,h) = t_{gh}^{-1} t_g t_h$ and $\gamma'(g,h) = s_{gh}^{-1} s_g s_h$, respectively. Then for all $g, h \in G$:

$$\begin{aligned}\gamma'(g,h) = s_{gh}^{-1} s_g s_h &= \left(t_{gh} n_{gh}\right)^{-1} t_g n_g t_h n_h = n_{gh}^{-1} t_{gh}^{-1} t_g n_g t_h n_h \\ &= n_{gh}^{-1} t_{gh}^{-1} t_g t_h n_g^h n_h = n_{gh}^{-1} \gamma(g,h) n_g^h n_h = n_{gh}^{-1} n_g^h n_h \gamma(g,h) = \beta_f(g,h)\gamma(g,h),\end{aligned}$$

where $\beta_f = f(gh)^{-1} f(g)^h f(h) \in B^2(G,N)$; this shows that $\gamma' = \gamma\beta_f$.

Conversely, if γ and γ' differ by an element in $B^2(G,N)$, then they define what is called equivalent extension.

Definition 2.2.1. Let G be a group with a G-module N. Two extensions $1 \to N \xrightarrow{i_1} E_1 \xrightarrow{\pi_1} G \to 1$ and $1 \to N \xrightarrow{i_2} E_2 \xrightarrow{\pi_2} G \to 1$ are *equivalent* if there exists an isomorphism $\alpha\colon E_1 \to E_2$ that renders the following diagram commutative.

$$\begin{array}{ccccccccc} 1 & \longrightarrow & N & \xrightarrow{i_1} & E_1 & \xrightarrow{\pi_1} & G & \longrightarrow & 1 \\ \downarrow & & \downarrow{=} & & \downarrow{\alpha} & & \downarrow{=} & & \downarrow \\ 1 & \longrightarrow & N & \xrightarrow{i_2} & E_2 & \xrightarrow{\pi_2} & G & \longrightarrow & 1. \end{array}$$

By the Five Lemma [44, Proposition 2.72], any homomorphism α that renders the diagram commutative is an isomorphism. Further, it follows from Theorem 2.1.3 that every such extension is isomorphic to E_γ for some $\gamma \in Z^2(G,N)$. We observe the following; see also [44, Proposition 9.12].

Theorem 2.2.2. *Let G be a group with a G-module N, and let $\gamma, \delta \in Z^2(G,N)$ be 2-cocycles. Two extensions E_γ and E_δ of N by G are equivalent if and only if $\gamma \equiv \delta \bmod B^2(G,N)$.*

Proof. Let $i_1\colon N \to E_\gamma$ and $i_2\colon N \to E_\delta$ be the natural inclusions, and let $\pi_1\colon E_\gamma \to G$ and $\pi_2\colon E_\delta \to G$ be the natural projections. Suppose there exists an isomorphism $\alpha\colon E_\gamma \to E_\delta$ such that the diagram is commutative; that is,

$$\alpha \circ i_1(n) = \alpha((1,n)) = i_2(n) = (1,n) \in E_\delta,$$

and

$$\pi_1((g,n)) = g = \pi_2 \circ \alpha((g,n)) \in G$$

for all $g \in G, n \in N$. Since $G = E_\gamma/N$, for every $g \in G$ there exists some $m_g \in N$ such that $\alpha((g,1)) = (g, m_g)$. It follows that $\alpha((g,n)) = (g, nm_g)$ for any $(g,n) \in E_\gamma$ since α is a homomorphism and $(g,n) = (g,1)(1,n)$. Thus, α induces a well-defined map $f\colon G \to N$ given by $f(g) = m_g$. Moreover, for all $(g,a), (h,b) \in E_\gamma$, we have

$$\alpha\left((gh, a^h b\gamma(g,h)\right) = \alpha\left((g,a)(h,b)\right) = \alpha((g,a))\alpha((h,b)) = (g, am_g)(h, bm_h).$$

That is, $\left(gh, a^h b\gamma(g,h)m_{gh}\right) = \left(gh, (am_g)^h (bm_h)\delta(g,h)\right)$, from which we deduce that $a^h b\gamma(g,h)m_{gh} = (am_g)^h(bm_h)\delta(g,h)$. Since N is abelian, it follows that

$$\gamma(g,h)m_{gh} = m_g^h m_h \delta(g,h),$$

or equivalently, $\gamma(g,h) = m_{gh}^{-1} m_g^h m_h \delta(g,h) = \beta_f(g,h)\delta(g,h)$. By definition, the map β_f is a 2-coboundary. Hence, $\gamma \equiv \delta \bmod B^2(G,N)$.

Conversely, suppose $\gamma \equiv \delta \bmod B^2(G,N)$. Then by definition there exists a map $f\colon G \to N$ with $f(1) = 1$ and $f(g) = m_g$ such that $\gamma = \beta_f \delta$, where $\beta_f(g,h) = m_{gh}^{-1} m_g^h m_h$ for all $g, h, \in G$. Define $\alpha\colon E_\gamma \to E_\delta$ by

$$\alpha((g,a)) = (g, am_g).$$

Since $\alpha((1,a)) = (1,a)$ and $\pi_2 \circ \alpha((g,a)) = \pi_2((g,am_g)) = g$, it follows that α renders the diagram commutative. Moreover, it is straightforward to check that α is a homomorphism with the relation $\gamma(g,h) = m_{gh}^{-1} m_g^h m_h \delta(g,h)$ and the fact that N is abelian. By the Five Lemma, α is an isomorphism as desired. □

Corollary 2.2.3. *Let G be a group and N be a G-module. If $\beta \in Z^2(G,N)$, then the extension E_β of N by G splits if and only if $\beta \in B^2(G,N)$; all split extensions of N by G are equivalent.*

Proof. An extension E_β of N by G is a split extension if and only if it is isomorphic to the semidirect product $G \ltimes_\varphi N$, where φ is the underlying G-action on N defined by the given G-module structure. Further, the semidirect product is isomorphic to the extension E_η, where η is the trivial 2-cocycle. However, Theorem 2.2.2 shows that E_β and E_η are equivalent if and only if β and η differ by an element in $B^2(G,N)$. Since η is the identity element of $B^2(G,N)$, it follows that E_β splits if and only if $\beta \in B^2(G,N)$. This also shows that for a fixed G-module structure on N, all split extensions of N by G are equivalent to E_η. □

Since $H^2(G,N) = Z^2(G,N)/B^2(G,N)$, the preceding discussions prove a famous result regarding second cohomology group of group extensions; see also [43, (11.1.4)] and [44, Theorem 9.13].

Theorem 2.2.4 (Schreier; [44], Theorem 9.13)**.** *Let G be a group and N be a G-module. Let $e(G,N)$ be the family of all equivalence classes of extensions of N by G. Then there is a bijection*

$$\Phi\colon H^2(G,N) \to e(G,N),$$

and Φ maps the identity element of $H^2(G,N)$ to the equivalent class of split extensions.

We remark that when studying groups, it is usually desirable to classify groups up to isomorphism. We have discussed a way to classify extensions up to equivalence, but often two group extensions are isomorphic despite being nonequivalent. For example, consider $N = \mathbb{Z}_2$, $G = \mathbb{Z}_2 \times \mathbb{Z}_2$. We know that there are only four groups (up to isomorphism) of order 8 that have a normal subgroup of order 2 with quotient isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$. However, there are eight nonequivalent group extensions of N by G, in one-to-one correspondence with the elements of $H^2(G,H)$. Since the main goal of this thesis is to find explicit construction and identification functions of the isomorphism class representatives of groups of small order type, we need to reduce the list of extensions by solving the isomorphism problem. The following section is devoted to a special type of isomorphisms.

2.3 Strong isomorphisms

We first recall some notation. Let H be a group. Then the automorphism group $\mathrm{Aut}(H)$ acts naturally on H; we use h^α and $\alpha(h)$ interchangeably for $\alpha \in \mathrm{Aut}(H)$ and $h \in H$. We remark that $h^{\alpha\beta} = \beta \circ \alpha(h)$ for $\alpha, \beta \in \mathrm{Aut}(H)$ and $h \in H$. In this section, we look into the so-called "strong isomorphisms"; for further discussion we refer to Besche and Eick's [4, Section 4.2.1].

Definition 2.3.1. Let G be a group and N be a G-module. For $i \in \{1,2\}$, let E_i be an extension of N by G with the canonical identification between N and the corresponding normal subgroup of $N_i \trianglelefteq E_i$. If there exists an isomorphism $\alpha\colon E_1 \to E_2$ such that $\alpha(N_1) = N_2$, then E_1 and E_2 are *strongly isomorphic*; such an isomorphism α is called a *strong isomorphism*. Equivalently, two extensions E_1, E_2 of N by G are strongly isomorphic if there exist isomorphisms $\alpha\colon E_1 \to E_2$,

$\beta\colon N \to N$, and $\tau\colon G \to G$ such that the following diagram is commutative:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & N & \xrightarrow{i_1} & E_1 & \xrightarrow{\pi_1} & G & \longrightarrow & 1 \\ \downarrow & & \cong\downarrow\beta & & \downarrow\alpha & & \cong\downarrow\tau & & \downarrow \\ 1 & \longrightarrow & N & \xrightarrow{i_2} & E_2 & \xrightarrow{\pi_2} & G & \longrightarrow & 1. \end{array}$$

Remark 2.3.2. Although the commutative diagram in Definition 2.3.1 resembles the one in Definition 2.2.1, we draw attention to the key difference: we do not insist an identity map (an isomorphism suffices) on N nor on G in the commutative diagram of Definition 2.3.1.

Definition 2.3.3. Let G and N be groups. If every isomorphism between two extensions of N by G maps the normal subgroup N to itself, then N is called a *strong G-group*.

For example, $N \cong C_3$ is a strong G-group for any G with $\gcd(3, |G|) = 1$, because in any such extension N is a characterstic Sylow 3-subgroup. Note that Definition 2.3.3 is not confined to extensions with abelian normal subgroups N. In general, if N is a strong G-group with a fixed G-action on N, and two extensions E_1 and E_2 of N by G are isomorphic via $\alpha\colon E_1 \to E_2$, then α induces an automorphism $\alpha|_N \in \mathrm{Aut}(N)$ and an isomorphism $\overline{\alpha}\colon E_1/N \to E_2/N$ via $xN \mapsto x^{\alpha}N$ for all $x \in E$. Since $G \cong E_i/N$, we can identify $\overline{\alpha}$ with an automorphism of G. Without loss of generality, we may consider $\overline{\alpha} \in \mathrm{Aut}(G)$. Observe that $(n^g)^{\alpha|_N} = (n^{\alpha|_N})^{(g^{\overline{\alpha}})}$. This relation can be generalised to more elements of $\mathrm{Aut}(G) \times \mathrm{Aut}(N)$, which motivates the following definition. For further details, we refer to [33, p. 55] and [44, pp. 570–571].

Definition 2.3.4. Let G be a group with a G-module N via $\varphi\colon G \to \mathrm{Aut}(N)$. A pair of automorphisms $(\nu, \mu) \in \mathrm{Aut}(G) \times \mathrm{Aut}(N)$ is called a *compatible pair* if $(n^g)^{\mu} = (n^{\mu})^{(g^{\nu})}$ for all $n \in N$ and $g \in G$. We denote the set of all compatible pairs in $\mathrm{Aut}(G) \times \mathrm{Aut}(N)$ with respect to the G-action φ by $\mathrm{Comp}(\varphi)$.

We observe that if the G-action on N is trivial, then $(n^g)^{\mu} = n^{\mu} = (n^{\mu})^{(g^{\nu})}$ for all $(\nu, \mu) \in \mathrm{Aut}(G) \times \mathrm{Aut}(N)$, in which case $\mathrm{Comp}(\varphi) = \mathrm{Aut}(G) \times \mathrm{Aut}(N)$. We further observe that $\mathrm{Aut}(G) \times \mathrm{Aut}(N)$ acts on the set of all group homomorphisms $\varphi\colon G \to N$ via

$$\varphi^{(\alpha,\beta)}(g) = \beta^{-1} \circ \varphi(\alpha(g)) \circ \beta. \tag{2.3.1}$$

By definition, for any homomorphism $\varphi\colon G \to \mathrm{Aut}(N)$, the stabiliser of φ is the subgroup

$$\mathrm{Stab}_{\varphi} = \left\{(\alpha, \beta) \in \mathrm{Aut}(N) \times \mathrm{Aut}(G)\colon \left(\beta^{-1} \circ \varphi(\alpha(g)) \circ \beta\right)(n) = \varphi(g)(n)\ \forall g \in G, n \in N\right\},$$

which can be rewritten as

$$\left\{(\alpha, \beta) \in \mathrm{Aut}(N) \times \mathrm{Aut}(G)\colon \left((n^{\beta})^{(g^{\alpha})}\right)^{(\beta^{-1})} = n^g,\ \forall n \in N, g \in G\right\},$$

but $\left((n^{\beta})^{(g^{\alpha})}\right)^{(\beta^{-1})} = n^g \iff (n^{\beta})^{(g^{\alpha})} = (n^g)^{\beta}$, which shows that $\mathrm{Comp}(\varphi) = \mathrm{Stab}_{\varphi}$.

Reminiscent to that the equivalence classes of extensions can be classified by the cohomology classes, the following theorem shows that the strong isomorphism classes of extensions with an abelian normal subgroup can be classified by the orbits of cohomology group under a compatible-pair action.

Theorem 2.3.5 ([33], p. 55)**.** *Let G be a group and N be a G-module. For $\gamma, \delta \in Z^2(G,H)$, let E_γ and E_δ be the corresponding extensions of N by G. Then E_γ and E_δ are strongly isomorphic if and only if there exists $(\nu,\mu) \in \mathrm{Comp}(\varphi)$ such that*

$$\gamma^{(\nu,\mu)} \equiv \delta \bmod B^2(G,N),$$

where

$$\gamma^{(\nu,\mu)}(g,h) = \gamma(g^{(\nu^{-1})}, h^{(\nu^{-1})})^\mu. \tag{2.3.2}$$

Proof. Suppose $\alpha\colon E_\gamma \to E_\delta$ is a strong isomorphism. Then α restricts to an automorphism $\alpha|_N = \mu \in \mathrm{Aut}(N)$, and induces an automorphism $\nu = \alpha|_{E_\gamma/N} \in \mathrm{Aut}(G)$ with the usual identification $N \trianglelefteq E_\gamma$ and $G = E_\gamma/N$. Also, for all $(1,n),(g,1) \in E_\gamma$, we have $\alpha((1,n)) = (1,n^\mu)$ and $\alpha((g,1)) = (g^\nu, a_g)$ for some $a_g \in N$. Moreover, since α is an isomorphism, it follows that $\alpha((g,n)) = \alpha((g,1))\alpha((1,n)) = (g^\nu, a_g n^\mu)$. We also know that $(1,n)(g,1) = (g,n^g)$. Thus, we can compute the image of (g,n^g) under α in two ways:

$$\alpha((g,n^g)) = \left(g^\nu, a_g (n^g)^\mu\right) \text{ and } \alpha((1,n))\alpha((g,1)) = (1,n^\mu)(g^\nu,a_g) = (g^\nu, (n^\mu)^{(g^\nu)} a_g).$$

Since N is abelian, this implies that

$$(n^\mu)^{(g^\nu)} = (n^g)^\mu,\ \forall n \in N, g \in G, \tag{2.3.3}$$

which shows that $(\nu,\mu) \in \mathrm{Comp}(\varphi)$. Since $\alpha((g,n)(h,m)) = \alpha((g,n))\alpha((h,m))$ for all for any $(g,n),(h,m) \in E_\gamma$, we have

$$\begin{aligned} &\left((gh)^\nu, a_{gh}\left(n^h m \gamma(g,h)\right)^\mu\right) = \left((gh)^\nu, a_{gh}(n^h)^\mu m^\mu \gamma(g,h)^\mu\right) \\ &= \left((gh)^\nu, (a_g n^\mu)^{(h^\nu)} a_h m^\mu \delta(g^\nu,h^\nu)\right) = \left((gh)^\nu, a_g^{(h^\nu)} (n^\mu)^{(h^\nu)} a_h m^\mu \delta(g^\nu,h^\nu)\right). \end{aligned} \tag{2.3.4}$$

Applying (2.3.3) to (2.3.4) yields that $\gamma(g,h)^\mu = a_{gh}^{-1} a_g^{(h^\nu)} a_h \delta(g^\nu,h^\nu)$. Since $\nu^{-1} \in \mathrm{Aut}(G)$, we further deduce that

$$\gamma(g^{(\nu^{-1})}, h^{(\nu^{-1})})^\mu = a^{-1}_{g^{(\nu^{-1})}h^{(\nu^{-1})}} a^h_{g^{(\nu^{-1})}} a_{h^{(\nu^{-1})}} \delta(g,h),$$

where the left-hand side is equal to $\gamma^{(\nu,\mu)}(g,h)$. This shows that $\gamma^{(\nu,\mu)} \equiv \delta \bmod B^2(G,N)$, since $\nu \in \mathrm{Aut}(G)$ and $(g^\nu,h^\nu) \mapsto a_{gh}^{-1} a_g^{(h^\nu)} a_{h^\nu}$ is a 2-coboundary.

Conversely, suppose there exists $(\nu,\mu) \in \mathrm{Comp}(\varphi)$ such that $\gamma^{(\nu,\mu)} \equiv \delta \bmod B^2(G,N)$. Then there exists a map $f\colon G \to N$ via $g \mapsto a_g$ with $f(1) = 1$ that defines a 2-coboundary β_f such that $\gamma^{(\nu,\mu)} = \delta\beta_f$. Define $\alpha\colon E_\gamma \to E_\delta$ by $(g,n) \mapsto (g^\nu, a_g n^\mu)$. A direct computation verifies that α is an isomorphism. Lastly, we check that $(1,m)^\alpha = (1,m^\mu) \in \{(1,n)\colon n \in N\} \trianglelefteq E_\delta$ for all $(1,m) \in E_\gamma$; that is, α preserves N. Therefore, E_γ and E_δ are strongly isomorphic. □

It follows from Theorem 2.3.5 that we have a group action of $\mathrm{Comp}(\varphi)$ on $Z^2(G,N)$. To see this, we show that the map $\chi\colon Z^2(G,H) \to Z^2(G,H)$, $\gamma \mapsto \gamma^{(\nu,\mu)}$ is an automorphism of $Z^2(G,N)$

for any $(\nu, \mu) \in \mathrm{Comp}(\varphi)$. We first check that χ is a homomorphism: for all $\gamma, \delta \in Z^2(G, N)$,

$$\begin{aligned}\left(\gamma^{(\nu,\mu)}\delta^{(\nu,\mu)}\right)(g,h) &= \gamma\left(g^{(\nu^{-1})}, h^{(\nu^{-1})}\right)^{\mu}\delta\left(g^{(\nu^{-1})}, h^{(\nu^{-1})}\right)^{\mu} \\ &= (\gamma\delta)\left(g^{(\nu^{-1})}, h^{(\nu^{-1})}\right)^{\mu} = (\gamma\delta)^{(\nu,\mu)}(g,h).\end{aligned}$$

Since $(\nu, \mu) \in \mathrm{Aut}(G) \times \mathrm{Aut}(N)$, it follows that if $\gamma^{(\nu,\mu)}(g,h) = \delta^{(\nu,\mu)}(g,h)$ for all $g, h \in G$, then $\gamma = \delta$; that is, χ is injective. Lastly, since $\gamma = (\gamma^{(\nu^{-1},\mu^{-1})})^{(\nu,\mu)}$ for all $\gamma \in Z^2(G, N)$, we know χ is also surjective. We check that $\beta^{(\nu,\mu)} \in B^2(G, N)$ for all $\beta \in B^2(G, N)$, which shows that $\chi|_{B^2(G,N)}$ is an automorphism on $B^2(G, N)$. Hence, χ induces an automorphism of $H^2(G, N)$. In combination with Theorem 2.3.5, we conclude that there is a bijection between the $\mathrm{Comp}(\varphi)$-classes of $H^2(G, N)$ and the strong isomorphism classes of extensions of N by G.

2.4 Split extensions

In the preceding section, we looked at the classification of groups extensions of a G-module N by G up to strong isomorphism. However, for the purpose of this thesis, we also encounter extensions of a nonabelian normal subgroup. Moreover, two isomorphic extensions are not necessarily strongly isomorphic. For example, two split extensions of N and G with different G-actions on N can still be isomorphic. The aim of this section is to present some results regarding isomorphic split extensions that are crucial to later chapters.

Recall that if G is a finite group of order m and H is a subgroup of G with index n, then H is a *Hall subgroup* if $\gcd(\frac{m}{n}, n) = 1$. The following theorem is a fundamental result of finite group theory.

Theorem 2.4.1 (Schur–Zassenhaus, [43], Theorem 9.1.2)**.** *Let G be a finite group. If H is a normal Hall subgroup of G, then $G = K \ltimes H$ for some $K \leq G$. If $K_1, K_2 \leq G$ are both complements of H, then K_1 and K_2 are conjugate in G.*

In particular, Theorem 2.4.1 shows that if two groups N and G have coprime orders, then every extension of N by G splits over N.

Theorem 2.4.2. *Let G and N be finite groups, and let $\varphi, \psi\colon G \to \mathrm{Aut}(N)$ be nontrivial group actions. Let $G \ltimes_\varphi N$ and $G \ltimes_\psi N$ be the respective split extensions (see Remark 2.1.4).*

(i) *If there exist some $(\nu, \mu) \in \mathrm{Aut}(G) \times \mathrm{Aut}(N)$ such that $\varphi(h) = \mu\psi(h^\nu)\mu^{-1}$ for all $h \in G$, then $G \ltimes_\varphi N \cong G \ltimes_\psi N$.*

(ii) *If N is an abelian strong G-group or if $\gcd(|N|, |G|) = 1$, then $G \ltimes_\varphi N \cong G \ltimes_\psi N$ if and only if there exists some $(\nu, \mu) \in \mathrm{Aut}(G) \times \mathrm{Aut}(N)$ such that $\varphi(h) = \mu\psi(h^\nu)\mu^{-1}$ for all $h \in G$.*

Proof. Note that (i) applies to all semidirect products of finite groups, although its converse is not necessarily true. To show (ii), it is sufficient to show the converse of (i) holds under those special conditions.

(i) Define $\alpha\colon G \ltimes_\varphi N \to G \ltimes_\psi N$ by $\alpha((g, n)) = (g^\nu, n^\mu)$. By hypothesis, the following diagram

commutes:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & N & \xrightarrow{i_1} & G \ltimes_\varphi N & \xrightarrow{\pi_1} & G & \longrightarrow & 1 \\ \downarrow & & \downarrow{\scriptstyle \mu} & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \nu} & & \downarrow \\ 1 & \longrightarrow & N & \xrightarrow{i_2} & G \ltimes_\psi N & \xrightarrow{\pi_2} & G & \longrightarrow & 1 \end{array},$$

where i_1, i_2 are inclusions $n \mapsto (1, n)$, and π_1, π_2 are projections $(g, n) \mapsto g$. The Five Lemma asserts that α is an isomorphism if and only if it is a homomorphism. Thus, to prove the claim it suffices to show that

$$\alpha((g,s)(h,t)) = \alpha((g,s))\alpha((h,t)) \tag{2.4.1}$$

for all $g, h \in G$ and $s, t \in N$. By definition, $\alpha((g,s)) = (g^\nu, s^\mu)$ for all $g \in G$ and $s \in N$. For any $g, h \in G$ and $s, t \in N$, we compute that

$$\alpha((g,s)(h,t)) = ((gh)^\nu, (s^{\varphi(h)}t)^\mu)$$

and

$$\alpha((g,s))\alpha((h,t)) = ((gh)^\nu, (s^\mu)^{\psi(h^\nu)}t^\mu).$$

Since $\varphi(h) = \mu\psi(h^\nu)\mu^{-1}$ for all $h \in G$ by assumption, it follows that $s^{\varphi(h)\mu} = s^{\mu\psi(h^\nu)}$ for all $s \in N$, and the equality in (2.4.1) holds. Thus α is an isomorphism and the two split extensions are isomorphic.

(ii) Denote $G \ltimes_\varphi N$ and $G \ltimes_\psi N$ by E_1 and E_2 respectively. Identify N with $N_i \trianglelefteq E_i$ for each $i = 1, 2$.

- If N_i is abelian and a strong G-group, then an isomorphism $\alpha\colon E_1 \to E_2$ induces automorphisms $\alpha|_{N_1} = \mu \in \mathrm{Aut}(N)$ and $\alpha_{E_1/N_1} \in \mathrm{Aut}(E_1/N_1)$. Thus $\alpha((1,n)) = (1, n^\mu)$ for all $(1,n) \in E_1$, and $\alpha((g,1)) = (g^\nu, \theta(g))$ for some map $\theta\colon G \to N$. Since

  $$((gh)^\nu, \theta(gh)) = \alpha((g,1)(h,1)) = \Big((gh)^\nu, \theta(g)^{\psi(h^\nu)}\theta(h)\Big)$$

  for all $g, h \in G$, it follows that $\theta \in Z^1(G, N)$. Moreover, for all $(g,n) \in E_1$,

  $$\alpha((g,n)) = (g^\nu, \theta(g))(1, n^\mu) = (g^\nu, \theta(g)n^\mu).$$

  Similarly, we compute

  $$\begin{aligned} &\alpha((g,s)(h,t)) = \alpha\left((gh, s^{\varphi(h)}t)\right) = \left((gh)^\nu, \theta(gh)(s^{\varphi(h)}t)^\mu\right) \\ =&\alpha((g,s))\alpha((h,t)) = (g^\nu, \theta(g)s^\mu)\,(h^\nu, \theta(h)t^\mu) \\ =&\left(g^\nu h^\nu, (\theta(g)s^\mu)^{\psi(h^\nu)}\theta(h)t^\mu\right), \end{aligned}$$

  which yields that $\theta(gh)\mu(s^{\varphi(h)})t = (\theta(g)\nu(s))^{\psi(h^\nu)}\theta(h)t^\mu$ for all $(g,s), (h,t) \in E_1$. Since N is abelian and $\theta \in Z^1(G,N)$, it follows that $s^{\varphi(h)\mu} = s^{\mu\psi(h^\nu)}$ for all $(h,s) \in G \ltimes_\varphi N$, implying that $\varphi(h)\mu = \mu\psi(h^\nu)$; that is, $\varphi(h) = \mu\psi(h^\nu)\mu^{-1}$ for all $h \in G$.

- If $\gcd(|G|, |N|) = 1$, then $N_i \cong N$ is a normal Hall subgroup of E_i for each i. In particular, N_i is characteristic in E_i and Theorem 2.4.1 shows that N_i has a complement G_i, isomorphic to G, in E_i. This implies that if $\alpha\colon E_1 \to E_2$ is an isomorphism then $\alpha(N_1) = N_2$. Moreover, since α is a homomorphism and $E_1 = G_1 \ltimes N_1$, the semidirect product decomposition is preserved by α, namely, $\alpha(E_1) = \alpha(G_1) \ltimes \alpha(N_1)$. Theorem 2.4.1 also asserts that $\alpha(G_1)$ is conjugate to G_2. This implies that there exists an inner automorphism $\beta \in \mathrm{Aut}(E_2)$ such that $\beta(\alpha(G_1)) = G_2$. Then $\alpha_0 = \beta \circ \alpha$ is also an iso-

morphism from E_1 to E_2, and by construction it satisfies that $\alpha_0(g,s) = (g^\nu, s^\mu)$, where $\alpha_0|_N = \mu \in \mathrm{Aut}(N)$ and $\nu = \alpha_0|_G \in \mathrm{Aut}(G)$. Since α_0 is a homomorphism, it follows that for any $(g,s),(h,t) \in E_1$,

$$\left((gh)^\nu, (s^{\varphi(h)}t)^\mu\right) = \left((gh)^\nu, (s^\mu)^{\psi(h^\nu)}t^\mu\right),$$

forcing that $(s^{\varphi(h)})^\mu = (s^\mu)^{\psi(h^\nu)}$ for all $s \in N$ and $h \in G$. In particular, this shows that $\varphi(h) = \mu\psi(h^\nu)\mu^{-1}$, as claimed. □

As a corollary, we consider the case where G is cyclic.

Corollary 2.4.3. *Let G be a cyclic group, and $\varphi, \psi\colon G \to \mathrm{Aut}(N)$ be nontrivial G-actions.*

(i) *If $\varphi(G)$ and $\psi(G)$ are conjugate in $\mathrm{Aut}(N)$, then $G \ltimes_\varphi N \cong G \ltimes_\psi N$.*

(ii) *If $|N|$ and $|G|$ are coprime, then the split extensions $G \ltimes_\varphi N$ and $G \ltimes_\psi N$ are isomorphic if and only if $\varphi(G)$ and $\psi(G)$ are conjugate in $\mathrm{Aut}(N)$.*

Proof. (i) Let a be a generator of G. By assumption we know that $|\varphi(G)| = |\psi(G)|$ and there exists some $\mu \in \mathrm{Aut}(N)$ such that $\varphi(G) = \mu\psi(G)\mu^{-1}$. It follows that there must exist a generator $g \in G$ such that $\varphi(a) = \mu\psi(g)\mu^{-1}$. In particular, $g = a^k$ for some positive integer $k < |G|$ coprime to $|G|$. Every element of G is of the form a^x for some non-negative integer $x < |G|$ and we observe

$$\begin{aligned}\varphi(a^x) &= (\varphi(a))^x = \left(\mu\psi(g)\mu^{-1}\right)^x \\ &= \mu(\psi(g))^x\mu^{-1} = \mu\psi(g^x)\mu^{-1} \\ &= \mu\psi((a^k)^x)\mu^{-1}.\end{aligned}$$

Since $\gcd(k,|G|) = 1$, the power map $\nu\colon G \to G, \nu(a) = a^k$ is an automorphism of G and $\varphi(h) = \mu\varphi(h^\nu)\mu^{-1}$ for all $h \in G$. It follows from Theorem 2.4.2(i) that $G \ltimes_\varphi N \cong G \ltimes_\psi N$.

(ii) Since (i) applies to the special case where $\gcd(|G|,|N|) = 1$, it remains to show the converse. Since Theorem 2.4.1 implies that N is a strong G-group, it follows from Theorem 2.4.2(ii) that two split extensions of N by G are isomorphic if and only if there exist some $\nu \in \mathrm{Aut}(G)$ and $\mu \in \mathrm{Aut}(N)$ such that $\varphi(h) = \mu\psi(h^\nu)\mu^{-1}$ for all $h \in G$. This implies that $\varphi(G) = \mu\psi(G)\mu^{-1}$, as claimed. □

We conclude this section by presenting a counting formula with some variations for the isomorphism types of a special class of split extensions. We note that these results can be directly derived from Theorem 2.4.2; for more details we refer to Taunt's paper [50] and Eick's arXiv preprint [24]. As mentioned in the Introduction, we merged our results and Eick's and subsequently, we borrowed some of the notation from [24] and made adjustments to our initial proofs. Here, we present the version after we had made such changes; see also [20, Section 3.2] and [24, Section 4.2].

Definition 2.4.4. For N and G finite solvable groups with $\gcd(|N|,|G|) = 1$, let $\mathcal{S}$ be a set of representatives for the conjugacy classes of subgroups in $\mathrm{Aut}(N)$, let $\mathcal{K}$ be a set of representatives for the $\mathrm{Aut}(G)$-classes of normal subgroups in G, and let

$$\mathcal{X} = \{(S,K) : S \in \mathcal{S}, K \in \mathcal{K} \text{ with } S \cong G/K\}.$$

For $(S,K) \in \mathcal{X}$, let A_K be the subgroup induced by the action of $\mathrm{Stab}_{\mathrm{Aut}(G)}(K)$ on G/K; let the group A_S be the preimage under a fixed isomorphism $G/K \to S$ of the subgroup of $\mathrm{Aut}(S)$ induced by the action of $N_{\mathrm{Aut}(N)}(S)$. Finally, we let

$$\mathrm{ind}_K = [\mathrm{Aut}(G/K) : A_K] \quad \text{and} \quad \mathrm{DC}(S,K) = A_K \backslash \mathrm{Aut}(G/K)) / A_S.$$

Recall that there is a well-defined $\mathrm{Aut}(G) \times \mathrm{Aut}(N)$-action on the set of group homomorphisms $\varphi\colon G \to \mathrm{Aut}(N)$ as described in (2.3.1), and the stabiliser of such a homomorphism φ is the group of compatible pairs $\mathrm{Comp}(\varphi)$.

In light of Theorem 2.4.2, we obtain the following result using the notation introduced in Definition 2.4.4.

Theorem 2.4.5. *Let G be a finite group and let N be a finite strong G-group. Let $\omega(G,N)$ denote the number of isomorphism classes of split extensions of N by G.*

(i) *If N is abelian, then let $\mathcal{O}$ be a complete set of representatives for the orbits of $\mathrm{Aut}(G)\times\mathrm{Aut}(N)$ acting on the set of group homomorphisms from G to $\mathrm{Aut}(N)$. For each $\varphi \in \mathcal{O}$ let o_φ be the number of $\mathrm{Comp}(\varphi)$-orbits in $H^2_\varphi(G,N)$. Then $\omega(G,N) = \sum_{\varphi\in\mathcal{O}} o_\varphi$.*

(ii) *If N and G have coprime orders, then $\omega(G,N) = \sum_{(S,K)\in\mathcal{X}} |\mathrm{DC}(S,K)|$.*

Proof. (i) To emphasise the G-action on N via φ, write $E_{\varphi,\gamma}$ for the extension E_γ of N by G with a 2-cocycle $\gamma \in Z^2_\varphi(G,N)$. Suppose $\alpha\colon E_{\varphi,\gamma} \to E_{\psi,\delta}$ is an isomorphism. Then

$$\alpha((g^{-1},1)(1,n)(g,1)) = \alpha((g^{-1},1))\alpha((n,1))\alpha((g,1))$$

for all $g \in G, n \in N$. Proceeding from the calculation in proof of Theorem 2.4.2(ii), it follows that

$$\alpha\left((1,n^{\varphi(g)})\right) = \left(1,(n^\mu)^{\psi(g^\nu)}\right),$$

which shows that $\varphi(g) = \mu^{-1}\circ\psi(g)\circ\mu$ for all $g \in G, n \in N$. In particular, this means that if $E_{\varphi,\gamma} \cong E_{\psi,\delta}$ then φ and ψ are in the same $\mathrm{Aut}(G)\times\mathrm{Aut}(N)$-orbit. That is, if the respective $\mathrm{Aut}(G)\times\mathrm{Aut}(N)$-orbits containing φ and ψ have different representatives in $\mathcal{O}$, then $E_{\varphi,\gamma}$ and $E_{\psi,\delta}$ are nonisomorphic. Now if φ and ψ are in the same $\mathrm{Aut}(G)\times\mathrm{Aut}(N)$-orbit, then it suffices to consider the representative $\varphi \in \mathcal{O}$. It follows from Theorem 2.3.5 that $E_{\varphi,\gamma} \cong E_{\varphi,\delta}$ if and only if the γ and δ are in the same $\mathrm{Comp}(\varphi)$-orbit. The claimed result follows.

(ii) By Theorem 2.4.1, every extension of N by G splits. Theorem 2.4.2(ii) implies that if two split extensions $G \ltimes_\varphi N$ and $G \ltimes_\psi N$ are isomorphic, then $\varphi(G)$ and $\psi(G)$ are conjugate in $\mathrm{Aut}(G)$, and both isomorphic to G/K, where $K = \mathrm{Ker}\,\varphi$ is in the same $\mathrm{Aut}(G)$-class as $\mathrm{Ker}\,\psi$. Conversely, for each $(S,K) \in \mathcal{X}$, if $\mathrm{Ker}\,\varphi = \mathrm{Ker}\,\psi = K$ and $\varphi(G) = \psi(G) = S$, then $G \ltimes_\varphi N \cong G \ltimes_\psi N$ if and only if there exist $\alpha \in A_K$ and $\beta \in A_S$ such that $i = \alpha j \beta$, where $i, j \in \mathrm{Aut}(G/K)$ are the isomorphisms induced by $\varphi|_{G/K}$ and $\psi|_{G/K}$ onto $S \cong G/K$, respectively. It follows that the number of split extensions of N by G is counted by $\omega(G,N) = \sum_{(S,K)\in\mathcal{X}} |\mathrm{DC}(S,K)|$. □

Theorem 2.4.2(ii) simplifies to the following result when N and $\mathrm{Aut}(N)$ are cyclic. This holds when N is a cyclic group of order 2, 4, or p^n when $p > 2$.

Corollary 2.4.6. *Let N be a finite cyclic group such that $\mathrm{Aut}(N)$ is cyclic, and let G be a finite group with order coprime to $|N|$. Let $\pi = \gcd(|G|, |\mathrm{Aut}(N)|)$, and let $\mathcal{K}_\ell = \{K \in \mathcal{K} \colon G/K \cong C_\ell\}$ where $\mathcal{K}$ is as defined in Definition 2.4.4. Then the number of isomorphism types of extensions of N by G is given by*

$$\sum_{\ell \mid \pi} \sum_{K \in \mathcal{K}_\ell} \mathrm{ind}_K,$$

where ind_K is as defined in Definition 2.4.4.

Proof. Since $|G|$ and $|N|$ are coprime, it follows from Theorem 2.4.1 that any extensions of N by G splits over G. On the other hand, N is a normal Hall subgroup in any such extension, thus a strong G-group. Let $\varphi_1, \varphi_2 \colon G \to \mathrm{Aut}(N)$ be two nontrivial group actions, and let $E_1 \cong G \ltimes_{\varphi_1} N$ and $E_2 \cong G \ltimes_{\varphi_2} N$ be the corresponding split extension. Since $\mathrm{Aut}(N)$ is cyclic, Theorem 2.4.2(ii) implies that $E_1 \cong E_2$ if and only if there exists some $\nu \in \mathrm{Aut}(G)$ such that $\varphi_1(g) = \varphi_2(g^\nu)$ for all $g \in G$. Since $\varphi_i(G) \cong G/\mathrm{Ker}\ \varphi_i$ embeds into $\mathrm{Aut}(N)$, thus is cyclic, it follows that $E_1 \cong E_2$ if and only $\mathrm{Ker}\ \varphi_1 \cong \mathrm{Ker}\ \varphi_2$ are in the same $\mathrm{Aut}(G)$-class as $K \in \mathcal{K}_\ell$ for some $\ell \mid \pi$ and there exists some $\nu_K \in \mathrm{Aut}(G/K)$ such that $\overline{\varphi_1}(G/K)) = \overline{\varphi_2}((G/K)^{\nu_K})$, where $\overline{\varphi_i} \in \mathrm{Aut}(G/K)$ are the isomorphisms induced by $G/K \mapsto \varphi_i(G)$. That is, $\overline{\varphi_1}$ and $\overline{\varphi_2}$ are in the same coset of A_K in $\mathrm{Aut}(G)/K$. This shows that for each $\ell \mid \pi$, the isomorphism types of N by G are in one-to-one correspondence with the cosets of A_K in $\mathrm{Aut}(G/K)$ where $K \in \mathcal{K}_\ell$. □

Chapter 3

Polycyclic groups

Recall that a group is *solvable* if it has an abelian subnormal series.The celebrated odd-order theorem, proved by Feit & Thompson [26], asserts that every group of odd order is solvable. Moreover, Burnside's pq-theorem shows that all groups of order $p^a q^b$ for distinct primes p, q are solvable. It follows from these results that many of the order types that we consider in this thesis will always admit solvable groups. Recall that a finite group is solvable if and only all its composition factors are cyclic of prime order. Such groups are polycyclic and can be efficiently represented by so-called polycyclic presentations. Importantly, there are many efficient algorithms to compute with groups defined by polycyclic presentations. The aim of this chapter is to recall some definitions and well-known facts from [33, Chapter 8], [43, Chapters 2], and [45, Chapters 11–12].

3.1 Group presentations

Let X be a nonempty set and F_X be the free group on X. We say $\omega = x_1^{e_1} x_2^{e_2} \cdots x_m^{e_m}$ is a *word on* X if each $x_i \in X$ and each $e_i \in \mathbb{Z}$. Let $\mathcal{R}$ be a subset of F_X and denote $N(\mathcal{R})$ for the normal closure of the subgroup generated by $\mathcal{R}$. We say $\langle X \mid \mathcal{R} \rangle$ is a presentation of G if $G \cong F_X / N(\mathcal{R})$. Conversely, given a presentation $\langle X \mid \mathcal{R} \rangle$, the group it yields is uniquely determined by the quotient $F_X / N(\mathcal{R})$. By abuse of notation, we identify words on X with elements they represent in $G = \langle X \mid \mathcal{R} \rangle$. If X is finite, then we say G is *finitely generated*; if both X and $\mathcal{R}$ are finite, then we say G is *finitely presented* or has a finite presentation. Every group has at least one presentation and every finite group has a *finite presentation*. We say two presentations are isomorphic if the groups they define are isomorphic. For further background we refer to [43, Chapter 2] and [45, Chapter 11].

Group presentations give a useful way to describe a group. However, there are serious algorithmic problems: in general, there is no algorithm to determine whether two presentations are isomorphic. In fact, there is not even an algorithm to determine whether a presentation defines a trivial group [45, Chapter 12]. Given a group presentation, it is natural to ask whether a word on the generators and the inverses represents the identity of the group: this gives an informal description of the *word problem*. Novikov, Boone, and Britton independently proved that there exists a finitely presented group for which this is an algorithmically indecisive problem; see also [45, Chapter 12] for further background. Nonetheless, there are special classes of groups for which such an algorithm exists. In particular, a group $G = \langle X \mid \mathcal{R} \rangle$ is said to have a *solvable*

word problem if there exists an algorithm that determines whether $\omega = 1_G$ for all words ω on X. For further details we refer to [43, Section 2.2] and [45, Chapter 12].

Although there is no algorithm to determine whether two arbitrary presentations are isomorphic, the following theorem due to von Dyck is useful in practice because it can be used to attempt solving the isomorphism problem. We refer to [43, Theorem 2.2.1] for a proof.

Theorem 3.1.1 (von Dyck). *Let $G = \langle X \mid \mathcal{R} \rangle$ be a finitely presented group. Let H be a group and let $\alpha\colon X \to H$ be a map. If $\alpha(x_1)^{e_1} \cdots \alpha(x_r)^{e_r} = 1$ for every relator $x_1^{e_1} \cdots x_r^{e_r} \in \mathcal{R}$, then α extends to a group epimorphism $G \to \langle \alpha(x)\colon x \in X \rangle \leq H$. Thus, if $\langle \alpha(x)\colon x \in X \rangle = H$ and $|G| = |H|$ is finite, then α extends to an isomorphism.*

Conversely, given $G = \langle X \mid \mathcal{R} \rangle$ and a homomorphism $\varphi\colon G \to H$, it suffices to describe the image $\varphi(x)$ for each $x \in X$ in order to describe the homomorphism φ and the image $\operatorname{Im}\varphi$. In this thesis, we often work with group presentations. Thus, for abbreviation we often define a group homomorphism by describing the image of the generators of the domain. For example, if $G = \mathrm{Pc}\langle a, b \mid a^p, b^p \rangle$, then we write $\{a \mapsto a^{-1}, b \mapsto b\}$ for the isomorphism $\iota\colon G \to G$ induced by this map on the generators. Furthermore, if the map α described in Theorem 3.1.1 extends to an isomorphism, then $\{\alpha(x_1), \ldots, \alpha(x_r)\}$ forms a generating set of H, and the map $\{\alpha(x_1) \mapsto x_1, \ldots, \alpha(x_r) \mapsto x_r\}$ extends to the inverse of the isomorphism induced by α. For example, the map $\{a^{-1} \mapsto a, b \mapsto b\}$ extends to $\iota^{-1} \in \mathrm{Aut}(G)$, where ι and G are as described before.

3.2 Polycyclic presentations

Recall that a group G is *polycyclic* if it has a subnormal series $G = G_1 \trianglerighteq G_2 \trianglerighteq \cdots \trianglerighteq G_{n+1} = 1$ such that each section G_i/G_{i+1} is cyclic for all $i \in \{1, \ldots, n\}$; such a series is called a *cyclic subnormal series*. With respect to this subnormal series, a *polycyclic sequence* is an ordered list $X = [g_1, \ldots, g_n]$ with each $g_i \in G_i \setminus G_{i+1}$ such that $G_i/G_{i+1} = \langle g_i G_{i+1} \rangle$; the corresponding list of *relative orders* is denoted by $R(X) = [r_1, \ldots, r_n]$ with each $r_i = |G_i/G_{i+1}|$. In general, $r_i = \infty$ is possible, but in this thesis we focus on finite groups, so we consider each r_i to be a positive integer. A polycyclic sequence is sometimes also called a *polycyclic generating set*, abbreviated as *pcgs*.

Definition 3.2.1. Let $X = [x_1, \ldots, x_n]$ be a finite ordered list. With respect to the ordering of X, a presentation $\langle X \mid \mathcal{R} \rangle$ is a *polycyclic presentation* (or *pc-presentation*) with *power exponents* $s_1, \ldots, s_n \in \mathbb{N}$, if the only relations in $\mathcal{R}$ are

$$\begin{aligned} x_i^{s_i} &= x_{i+1}^{a_{i,i+1}} \cdots x_n^{a_{i,n}} && (1 \leq i \leq n), \\ x_i^{x_j} &= x_{j+1}^{b_{i,j,j+1}} \cdots x_n^{b_{i,j,n}} && (1 \leq j < i \leq n), \end{aligned}$$

where $a_{i,k}, b_{i,j,k}, c_{i,j,k} \in \mathbb{Z}$ such that $0 \leq a_{i,k}, b_{i,j,k}, c_{i,j,k} \leq s_k - 1$.

Usually, it is conventional to omit trivial commutator relations $x_i^{x_j} = x_i$. It is also common to replace relations $x_i^{s_i} = 1$ by standalone relators $x_i^{s_i}$. To highlight when this has happened, we write $\mathrm{Pc}\langle X \mid \mathcal{R} \rangle$ for both the presentation $\langle X \mid \mathcal{R} \rangle$ and the polycyclic group it defines. For example, $\mathrm{Pc}\langle a, b \mid a^2, b^2 \rangle = \langle a, b, \mid a^2 = 1, b^a = 1, b^a = b \rangle \cong C_2 \times C_2$. The group G defined by the above polycyclic presentation in Definition 3.2.1 is polycyclic with pcgs X and

polycyclic series $G = G_1 \trianglerighteq G_2 \trianglerighteq \cdots \trianglerighteq G_{n+1} = 1$, where each $G_i = \langle x_i, \ldots, x_n \rangle$. By construction, $|G_i/G_{i+1}| = |x_i G_{i+1}| = r_i$, which divides s_i, but it is possible that $r_i \neq s_i$. We call $S(X) = [s_i, \ldots, s_n]$ the power exponents of the presentation with respect to the ordering of X.

Definition 3.2.2. A pc-presentation $\mathrm{Pc}\langle X \mid \mathcal{R} \rangle$ with power exponents $S(X)$ is *consistent* (or *confluent*) if and only if $R(X) = S(X)$. A consistent pc-presentation is called a *refined pc-presentation* if the relative orders are all primes.

Let $G = \mathrm{Pc}\langle X \mid \mathcal{R} \rangle$ be a finite polycyclic group with $X = [x_1, \ldots, x_n]$ and $S(X) = [s_1, \ldots, s_n]$. An inductive argument shows that every element in G can be uniquely expressed as $g = x_1^{e_1} \cdots x_n^{e_n}$ with each $0 \leq e_i < s_i$ and $0 \leq e_i < r_i$ if $i \in \mathcal{F}(X)$. This word is called the *normal form* of g with respect to X and $S(X)$; we say a word is *collected* if it is given in normal form. The following theorem leads to an algorithm to determine whether a presentation is consistent by collecting words to their normal form.

Theorem 3.2.3 ([48], Proposition 8.3)**.** *A pc-presentation $\mathrm{Pc}\langle X \mid \mathcal{R} \rangle$ with pcgs $X = [x_1, \ldots, x_n]$ and power exponents $S(X) = [s_1, \ldots, s_n]$ is consistent if and only if the normal forms of the following pairs of words coincide, where the subwords in brackets are to be collected first:*

$$
\begin{array}{lll}
x_k(x_j x_i) \quad \text{and} \quad (x_k x_j)x_i & & \text{for } 1 \leq i < j < k \leq n, \\
(x_j^{s_j})x_i \quad \text{and} \quad x_j^{s_j - 1}(x_j x_i) & & \text{for } 1 \leq i < j \leq n \text{ with } s_i < \infty, \\
x_j(x_i^{s_i}) \quad \text{and} \quad (x_j x_i)x_i^{s_i - 1} & & \text{for } 1 \leq i < j \leq n \text{ with } s_j < \infty, \\
x_j(x_j^{s_j}) \quad \text{and} \quad (x_j^{s_j})x_j & & \text{for } 1 \leq j \leq n \text{ with } s_j < \infty.
\end{array}
$$

We illustrate this in an example as follows.

Example 3.2.4. If $G = \mathrm{Pc}\langle x_1, x_2, x_3 \mid x_1^3 = x_3,\ x_2^2 = x_3,\ x_3^5 = 1,\ x_2^{x_1} = x_2 x_3 \rangle$, then

$$(x_2^2)x_1 = x_3 x_1 = (x_1^3)x_1 = x_1 x_3 \quad \text{and} \quad x_2(x_2 x_1) = (x_2 x_1)x_2 x_3 = x_1 x_2 x_3 x_2 x_3 = x_1 x_2^2 x_3^2 = x_1 x_3^3.$$

Since $x_1 x_3 = x_1 x_3^3$ are both normal forms of the word $x_2 x_2 x_1$ with respect to the power exponents $[3, 2, 5]$, the presentation is *not* consistent. Indeed, we deduce that $x_3 = 1$ in G, and $G \cong C_6$.

We note that the polycyclic presentation obtained from a given pcgs and associated polycyclic series is always consistent. In the following, all our polycyclic presentations are consistent, so we often omit the term "consistent".

Recall that a finite group is nilpotent if it has a *central series*. Theorem A.0.9 assets that a nilpotent group is a direct product of its Sylow subgroups. We now present a result that follows directly from the Sylow theorems and the Schur–Zassenhaus theorem.

Corollary 3.2.5. *Every finite nilpotent group G has a polycyclic presentation*

$$\mathrm{Pc}\langle X_1 \cup \cdots \cup X_n \mid \mathcal{R}_1 \cup \cdots \cup \mathcal{R}_n \rangle,$$

where each $\mathrm{Pc}\langle X_i \mid \mathcal{R}_i \rangle$ is a polycyclic presentation for the Sylow p_i-subgroup of G.

3.3 Computing cohomology using polycyclic presentations

Let $G = \mathrm{Pc}\langle X \mid \mathcal{R}\rangle$ be a polycyclic group with composition series $G = G_1 \trianglerighteq \cdots \trianglerighteq G_{n+1} = 1$ with respect to the pcgs $X = [x_1, \ldots, x_n]$. Let $N = \mathrm{Pc}\langle Y \mid \mathcal{T}\rangle$ be a G-module with composition series $N = N_1 \trianglerighteq \cdots \trianglerighteq N_{m+1} = 1$. If E is an extension with $N \trianglelefteq E$ and $E/N = G$, then let $\tilde{G}_i$ be the full preimage of G_i under the natural projection map $E \to G$. It follows that E is also polycyclic, as it admits a subnormal series $E = \tilde{G}_1 \trianglerighteq \cdots \trianglerighteq \tilde{G}_n \trianglerighteq N_1 \trianglerighteq \cdots N_{m+1} = 1$ where each section is cyclic. Let w_i be the image of $x_i \in X$ under a fixed transversal map $G \to E$, then E has a pcgs $W = [w_i, \ldots, w_n, y_1, \ldots, y_m]$, where $[y_1, \ldots, y_m] = Y$ is the corresponding pcgs of N. Moreover, if $R(x) = [r_1, \ldots, r_n]$ and $R(Y) = [u_1, \ldots, u_m]$ are the relative orders of X and Y, respectively, then $R(W) = [r_1, \ldots, r_n, u_1, \ldots, u_m]$. Let $x_i^{r_i} = \omega_{i,i}(x_{i+1}, \ldots, x_n)$ be a relation in $\mathrm{Pc}\langle X, \mathcal{R}\rangle$, where $\omega_{i,i}$ is a collected word in $x_{i+1}, \ldots, x_n$. Then in E there exists some $t_{i,i} \in N$ such that $w_i^{r_i} = \omega_{i,i}(w_{i+1}, \ldots, w_n)t_{i,i}$; we can assume that $t_{i,i}$ is a collected word in $\langle Y \mid \mathcal{T}\rangle$. Similarly, for a relation $x_i^{x_j}$ in $\mathrm{Pc}\langle X \mid \mathcal{R}\rangle$ with $i > j$, there exists $t_{i,j} \in N$ such that $w_i^{w_j} = \omega_{i,j}(w_j + 1, \ldots, w_n)t_{i,j}$. Analogously, we can readily write every word on W in normal form and find a consistent pc-presentation $E = \mathrm{Pc}\langle W \mid \mathcal{R}_t\rangle$ with relative orders $R(w)$, where the only relations in $\mathcal{R}_t$ are the following:

$$\begin{aligned}
w_i^{r_i} &= \omega_{i,i}(w_{i+1}, \ldots, w_n)t_{i,i} && (1 \le i \le n),\\
w_i^{w_j} &= \omega_{i,j}(w_{j+1}, \ldots, w_n)t_{i,j} && (1 \le j < i \le n),\\
y_i^{u_i} &= 1 && (1 \le i \le m),\\
y_i^{w_j} &= y_1^{e_{i,j,1}} \cdots y_m^{e_{i,j,m}} && (1 \le i \le m, 1 \le j \le n),
\end{aligned}$$

where $1 \le e_{a,b,c} \le u_c$ for all $1 \le c \le m$, and $t = [t_{k,\ell}]_{1 \le k \le \ell \le n}$ is an ordered list of collected words $t_{k,\ell} \in N$ on $[y_1, \ldots, y_m]$. Such a list t is sometimes called a *tail-vector*, coined by the authors of [33, Chapter 8], and each word $t_{k,\ell}$ is called a *tail*. Note that in this thesis we focus on finite groups so we omit all relators of the forms $w_i^{(w_j^{-1})}$ and $y_i^{(w_j^{-1})}$, which results in that t has length $\frac{1}{2}(n^2 + n)$, instead of n^2 as seen in [33, Chapter 8]. Observe that if $t_{k,\ell} = 1$ for all k, ℓ, then $\mathrm{Pc}\langle W \mid \mathcal{R}_t)\rangle$ splits over N. More generally, two extensions $E_1 = \mathrm{Pc}\langle W \mid \mathcal{R}_{t_1}\rangle$ and $E_2 = \mathrm{Pc}\langle W \mid \mathcal{R}_{t_2}\rangle$ with pc-relations $\mathcal{R}_{t_1}$ and $\mathcal{R}_{t_2}$ only differ in the tail-vectors. We exemplify this in the following.

Example 3.3.1. Let $G = \mathrm{Pc}\langle a \mid a^2 = 1\rangle \cong C_2$. Let $N = \mathrm{Pc}\langle b \mid b^4 = 1\rangle$ be a G-module via $\varphi\colon G \to \mathrm{Aut}(N)$, $a \mapsto (b \mapsto b^3)$. Let E be an extension of N by G. Such an extension E has a pc-presentation of the form

$$\mathrm{Pc}\langle a, b \mid a^2 = t, b^4 = 1, b^a = b^3\rangle,$$

where $t \in \langle b\rangle = N$. It follows that $t = b^x$ for some $x \in \mathbb{Z}_4$. Writing $b^4 = b(b^3)$, a direct manipulation shows that if $x = 1$ or 3, the presentation would be inconsistent. Thus, $x = 0$ or 2. Let $D = \mathrm{Pc}\langle a, b \mid a^2 = 1, b^4 = 1, b^a = b^3\rangle$ and $Q = \mathrm{Pc}\langle a, b \mid a^2 = b^2, b^4 = 1, b^a = b^3\rangle$. Observe that $D \cong D_4$ has 5 elements of order 2, whereas $Q \cong Q_8$ only has 2 elements of order 2: this shows that $D \ncong Q$. In particular, these are the only two isomorphism types of such extensions with the given G-module structure.

Let $G = \mathrm{Pc}\langle X \mid \mathcal{R}\rangle$ with $X = [x_1, \ldots, x_n]$ and let $N = \mathrm{Pc}\langle Y \mid \mathcal{T}\rangle$ be a G-module. Theorem 2.1.3(ii) asserts that every group extension E of N by G can be identified with E_γ for some (normalised) 2-cocycle class representative $\gamma \in Z^2(G, N)$. In particular, with respect to the map $\tau\colon G \to E_\gamma, g \mapsto (g, 1)$, if $x_i^{r_i} = \omega_{i,i}$ and $x_i^{x_j} = \omega_{i,j}$ are relations of $\mathcal{R}$, then in E_γ there

exist $t_{i,i}, t_{i,j} \in N$ such that $(x_i,1)^{r_i} = (\omega_{i,i}, t_{i,i})$ and $(x_i,1)^{(x_j,1)} = (\omega_{i,j}, t_{i,j})$, respectively. By evaluating the relations of G in E_γ, we obtain a pc-presentation of E_γ; to emphasise the tail-vector $t \in N^{\frac{1}{2}(n^2+n)}$, we denote the pc-presentation obtained this way by $P(t)$. Furthermore, we can apply this "evualuation" to an arbitrary extension E_γ with $\gamma \in Z^2(G,N)$; this gives a map $\zeta\colon Z^2(G,N) \to N^{\frac{1}{2}(n^2+n)}, \gamma \mapsto t$. We have the following result; see also [33, Lemma 8.47].

Lemma 3.3.2 ([33], Lemma 8.47)**.** *With the above setting, the map $\zeta\colon Z^2(G,N) \to N^{\frac{n^2+n}{2}}, \gamma \mapsto t$ is a homomorphism of abelian groups with* $\operatorname{Ker}\zeta \leq B^2(G,N)$*. Moreover,*

$$H^2(G,N) \cong Z^2(G,N)^\zeta / B^2(G,N)^\zeta.$$

Proof. First note that every extension E_γ of N by G is polycyclic. As explained above, E_γ can be described by a pc-presentation $P(t)$. Now consider $\gamma_1, \gamma_2 \in Z^2(G,N)$ with images $t_1 = \gamma_1^\zeta$ and $t_2 = \gamma_2^\zeta$, respectively. To show that ζ is a homomorphism, we need to show that $(\gamma_1\gamma_2)^\zeta = t_1t_2$. This is equivalent to saying that the extension $E_{\gamma_1\gamma_2}$ has a pc-presentation $P(t_1t_2)$, which follows from the fact that $N = \operatorname{Pc}\langle Y \mid \mathcal{T}\rangle$ is abelian; that is, reordering the entries of any word in Y does not change the element it represents. Now suppose $\gamma \in \operatorname{Ker}\zeta$. By definition, $\gamma^\zeta = t = [1,\dots,1]$; that is, $t_{i,j} = 1$ for all $1 \leq i \leq j \leq n$, which implies that $E_\gamma \cong P(t)$ splits over N. Then it follows from Corollary 2.2.3 that $\gamma \in B^2(G,N)$. This shows that $\operatorname{Ker}\zeta \leq B^2(G,N)$. Since $\operatorname{Ker}\zeta$ is normal in $Z^2(G,N)$, the third isomorphism theorem implies that $H^2(G,N) = Z^2(G,N)/B^2(G,N) \cong (Z^2(G,N)/\operatorname{Ker}\zeta)/(B^2(G,N)/\operatorname{Ker}\zeta)$. Finally, applying the first isomorphism theorem gives the claimed result. □

From the preceding discussion, it follows that there exists $\gamma \in Z^2(G,N)$ such that $\zeta(\gamma) = t$ if and only $P(t) \cong E_\gamma$ and $P(t)$ is a consistent pc-presentation; see also [33, Lemma 8.48]. In particular, Lemma 3.3.2 instructs how to compute $H^2(G,N)$ using the pc-presentations of G and N. We conclude this chapter with an example.

Example 3.3.3. Let p be an odd prime. Let $G = \operatorname{Pc}\langle x_1 \mid x_1^p = 1\rangle$ be a cyclic group of order p and let $N = \operatorname{Pc}\langle y_1, y_2 \mid y_1^p = 1, y_2^p = 1\rangle \cong C_p^2$ be a G-module via $y_1^{x_1} = y_1y_2$ and $y_2^{x_1} = y_2$. Suppose E is an extension of N by G, then E can be described by a pc-presentation $P(t)$, with $t \in N$, of the following form:

$$P(t) = \operatorname{Pc}\langle x_1, y_1, y_2 \mid x_1^p = t, y_1^p = 1, y_2^p = 1, y_1^{x_1} = y_1y_2\rangle;$$

here $t = y_1^m y_2^n$ for some $m, n \in \mathbb{Z}_p$. In light of Lemma 3.3.2, we can compute $H^2(G,N)$ by finding the values of t such that $P(t)$ is a consistent pc-presentation. Applying Theorem 3.2.3, we see that such $P(t)$ is consistent if and only if $(x_1^p)x_1 = x_1(x_1^p)$; that is, $tx_1 = x_1t$, which is equivalent to $t = t^{x_1}$. Thus, to compute $Z^2(G,N)^\zeta$, it is equivalent to solving for $m, n \in \mathbb{Z}_p$ such that $(y_1^m y_2^n)^{x_1} = y_1^m y_2^n$: the left-hand side equals $y_1^m y_2^m y_2^n = y_1^m y_2^{m+n}$, and equating both sides yields $m = 0$. This shows that $Z^2(G,N)^\zeta = \langle y_2\rangle$. Since $B^2(G,N)^\zeta \trianglelefteq Z^2(G,N)^\zeta$, and $B^2(G,N)^\zeta$ define split extensions, we find that $B^2(G,N)^\zeta$ is the trivial subgroup. It follows from Lemma 3.3.2 that $H^2(G,N) \cong Z^2(G,N)^\zeta/B^2(G,N)^\zeta \cong C_p$. This shows that there are p equivalence classes of extensions of N by G, with pc-presentations $P(t)$ of said form, parametrised by $t = y_2^k$ for $k \in \mathbb{Z}_p$. Observe that if $k \in \mathbb{Z}_p^*$, then the isomorphism type of $P(t = y_2^k)$ is independent of the choice of k, since rewriting y_2^k for y_2 extends to an isomorphism (Theorem 3.1.1). In particular, such groups have exponent p^2. On the other hand, if $k = 0$, then $P(t) \cong C_p \ltimes C_p^2$ has exponent p. This shows that there are in total two isomorphism types of extensions with the given G-module structure.

Chapter 4

Automorphism groups

From Chapter 2 we have seen that group actions play a crucial role in the construction and classification of group extensions. Recall that a group action of G on N is a homomorphism $\varphi\colon G \to \mathrm{Aut}(N)$. We now focus on automorphism groups and present some results that lay the basis for our determination of groups of order $n \in \{pq, p^2q, p^2q^2, p^3q, pqr, pqrs, p^2qr\}$ where p, q, r, s are distinct primes. We refer to [8], [9], [10], and [47, Chapter 2] for further discussion on this topic.

One main goal of this thesis is to derive an algorithm to identify the isomorphism type of a given group of certain order type. For this purpose, we assign each isomorphism type an "ID", as discussed in Section 1.2. Since in this thesis we determine most of the groups by recognising them as group extensions and the isomorphism types of group extensions are closely related to subgroups of automorphism types as seen in Corollary 2.4.3 and Corollary 2.4.6, the assignment of group IDs often relies on sorting automorphisms in a "canonical" way. We exemplify this in the following.

Example 4.0.1. Groups of order pq, where p, q are distinct primes such that $q \mid (p-1)$, are isomorphic to split extensions $C_q \ltimes C_p$. It follows from Theorem 2.4.2(ii) that there are two isomorphism types of such extensions, dependent on the C_q-module C_p. More specifically, if C_q acts trivially on C_p, then we assign the corresponding split extension $C_q \times C_p$ with ID $(pq, 1)$. On the other hand, if C_q acts nontrivially on C_p, then such split extensions are isomorphic to

$$G(k) = \mathrm{Pc}\langle a, b \mid a^q, b^p, b^a = b^{k\phi(p)/q}\rangle,$$

where ϕ is the Euler totient function and $k \in \mathbb{Z}_q^*$; Corollary 2.4.3(ii) shows that $G(k) \cong G(1)$ for any $k \in \mathbb{Z}_q^*$. In this case, we choose $G(1)$ to be the isomorphism class representative with ID $(pq, 2)$, and call the automorphism induced by $b \mapsto b^{k\phi(p)/q}$ the "canonical" automorphism of $\langle b\rangle$, and call the C_q action described by $b^a = b^{k\phi(p)/q}$. the "canonical" C_q-action on C_p. Conversely, a group of order pq that is abelian is of isomorphism type $(pq, 1)$, and its nonabelian counterpart is of type $(pq, 2)$. We introduce some notations and explain the canonical choices of automorphisms in more general settings in Notations 4.1.1, 4.2.1, and 4.2.6.

4.1 Automorphism groups of finite abelian groups

Bidwell and Curran [9] classified the automorphism groups of finite abelian groups. Here we only selectively present some results that we use in later chapters. We refer to [9] for proofs

and more details on this subject.

Notation 4.1.1. Let a be a positive integer such that C_a has a cyclic automorphism group of order $\phi(a)$, where ϕ is the Euler totient function; that is, $\mathrm{Aut}(C_a) \cong \mathbb{Z}_{\phi(a)}$. In particular, this holds if and only if $a = 1, 2, 4, p^k, 2p^k$, where p is an odd prime. Let

$$\sigma_a \in \mathbb{Z}_a^*$$

denote the smallest positive integer such that $\mathbb{Z}_a^* = \langle \sigma_a \rangle$. Let b be a positive integer dividing $\phi(a)$. We define the *canonical generator* of the (unique) cyclic subgroup of order b in $\mathrm{Aut}(C_a)$ by

$$\rho(a,b)\colon C_a \to C_a,\ x \mapsto x^{(\sigma_a^{\phi(a)/b})},\ \forall x \in C_a.$$

For $k \in \mathbb{Z}_b$, we write

$$\rho(a,b,k) = \rho(a,b)^k,$$

and abbreviate $\rho(a,b,1)$ as $\rho(a,b)$. Note that we allow $k = 0$, and $\rho(a,b,0)$ is the trivial automorphism. We observe that the map ρ is naturally identified with an integer-value function such that $\rho(a,b,k) = \sigma_a^{k\phi(a)/b} \in \mathbb{Z}_a^*$.

Theorem 4.1.2 ([9], Theorems 2.4 & 2.5)**.** *Let p be a prime and $G = C_{p^m} \times C_{p^n}$ with $m > n$. If $p = 2$ then $|\mathrm{Aut}(G)| = 2^{m+3n-2}$. If $p > 2$, then $\mathrm{Aut}(G)$ has order $(p-1)^2 p^{m+3n-2}$, with a group presentation as follows:*

$$\langle a, b, c, d \mid a^{\phi(p^m)}, b^{p^n}, c^{p^n}, d^{\phi(p^n)}, b^a = b^{(\sigma_{p^n}^{-1})}, b^d = b^{\sigma_{p^n}},$$
$$c^a = c^{\sigma_{p^m}}, c^d = c^{(\sigma_{p^n}^{-1})}, cb = a^{-w}bcd^w, d^a = d\rangle,$$

where $w < \phi(p^n)$ is a positive integer such that $\sigma_{p^m}^w \equiv 1 + p^{m-n} \bmod p^m$.

Note that if $m = n$, then $\mathrm{Aut}(G)$ is in one-to-one correspondence with the group of 2×2 invertible matrices with coefficients in $\mathbb{Z}_{p^n}$; for the special case $m = n = 1$ it follows that $\mathrm{Aut}(C_p^2) \cong \mathrm{GL}_2(p)$. In general, treating elementary abelian groups of order p^n as n-dimensional vector spaces over $\mathbb{Z}_p$, we see that if P is an elementary abelian p-group of order p^n, then $\mathrm{Aut}(P) \cong \mathrm{GL}_n(p)$. For the generalisation of Theorem 4.1.2 to groups with more than two direct factors, see [9, § 4].

Let G be a group acting on an elementary abelian group $P \cong C_p^n$. Then every G-action on P via $\rho\colon G \to \mathrm{Aut}(P) \cong \mathrm{GL}_n(p)$ is a linear representation of G over $\mathbb{Z}_p$. Conversely, any $\mathbb{Z}_p$-representation of G of dimension n defines an action of G on an elementary abelian group of order p^n. We thus recall some relevant terminology and results in representation theory. For further background, we refer to [34, Chapter 1].

Recall that a G-module is *irreducible* if it is nontrivial and contains no nontrivial proper G-submodules. A G-module is *reducible* if it is not irreducible. A G-module V is *completely reducible* if it can be written as a direct sum of irreducible G-submodules. The following is a well-known result in representation theory.

Theorem 4.1.3 (Maschke, [34], Theorem 1.9)**.** *Let G be a finite group and let $\mathbb{F}$ be a field whose characteristic does not divide $|G|$. Then every $\mathbb{F}$-representation of G is completely reducible.*

Theorem 4.1.3 plays a key role in our classification of semidirect products, especially when we consider the split extensions of elementary abelian groups.

If G is a subgroup of $\mathrm{GL}_n(\mathbb{F})$, then the inclusion $\iota\colon G \hookrightarrow \mathrm{GL}_n(\mathbb{F})$ is an $\mathbb{F}$-representation of G. Recall that G is an *irreducible subgroup* of $\mathrm{GL}_n(\mathbb{F})$ if such a representation is irreducible, and G is called a *reducible subgroup* if the representation induced by this inclusion is reducible. A direct consequence of Theorem 4.1.3 is that if G is a subgroup of $\mathrm{GL}_n(\mathbb{F})$ with order coprime to the characteristic of $\mathbb{F}$, then every element of G is conjugate to a block diagonal matrix with irreducible blocks. If G is conjugate to a group of diagonal matrices, then we say G is *diagonalisable* and G acts *diagonalisably* on $\mathbb{F}$. Moreover, the inclusion ι induces a G-action on $\mathbb{F}^n$. We say G acts *irreducibly* on $\mathbb{F}^n$ if G is a irreducible subgroup of $\mathrm{GL}_n(\mathbb{F})$, and use analogous terminology for its reducible and diagonalisable counterparts.

4.2 Subgroup classes of small linear groups $\mathrm{GL}_n(p)$

We now look into the conjugacy classes of cyclic subgroups in linear groups $\mathrm{GL}_n(p)$, where $n \in \{2,3,4\}$. In combination with Theorem 2.4.2, the results we present in this section are fundamental to our determination of groups that contain a normal Sylow p-subgroup of order dividing p^4. We first introduce some notation for the cyclic reducible subgroups in $\mathrm{GL}_2(p)$.

Notation 4.2.1. Let p be a prime and b be a positive integer with $b \mid (p-1)$. Let H be a cyclic subgroup of order b in $\mathrm{GL}_2(p)$. By Maschke's theorem (Theorem 4.1.3), we know H is a completely reducible. In $\mathrm{GL}_2(p)$ this implies that H is conjugate to a subgroup of diagonal matrices. In particular, the conjugacy class containing H has a representative generated by $\begin{pmatrix} \rho(p,b) & 0 \\ 0 & \rho(p,b,k) \end{pmatrix}$ for some $k \in \mathbb{Z}_b$, regarding ρ as an integer value function explained in Notation 4.1.1. We call this matrix the *canonical generator* of H and denote it by

$$M(p,b,k) = \mathrm{diag}(\rho(p,b), \rho(p,b,k)).$$

In line with Notation 4.1.1, we have

$$M(p,b,0) = \mathrm{diag}(\rho(p,b), 1)$$

and abbreviate

$$M(p,b,1) = M(p,b).$$

Further, since $\mathrm{GL}_2(p) \cong \mathrm{Aut}(C_p^2)$, we define the canonical generator of the H-action on the elementary abelian group $\mathrm{Pc}\langle x,y \mid x^p, y^p\rangle \cong C_p^2$ by $(x,y)^{M(p,b,k)} = (x^{\rho(p,b)}, y^{\rho(p,b,k)})$, which means that $M(p,b,k)$ maps the generators x and y to $x^{\rho(p,b)}$ and $y^{\rho(p,b,k)}$, respectively.

The following theorem asserts that there is, up to conjugacy, at most one cyclic irreducible subgroup of a given order in $\mathrm{GL}_n(p)$.

Theorem 4.2.2 (Short, [47], Theorems 2.3.2 & 2.3.3)**.** *There exists a cyclic irreducible subgroup $A \leq \mathrm{GL}_n(p^k)$ of order m if and only $m \mid (p^{nk}-1)$ and $m \nmid (p^{dk}-1)$ for all $d < n$. If such a cyclic subgroup exists, then it is unique up to conjugacy in $\mathrm{GL}_n(p^k)$.*

An immediate implication of Theorem 4.2.2 is that if a cyclic subgroup of $\mathrm{GL}_n(p)$ has order m such that $m|(p^d-1)$ for some positive $d < n$, then it is reducible in $\mathrm{GL}_n(p)$. It also follows from Theorem 4.2.2 that the maximal cyclic irreducible groups of $\mathrm{GL}_n(p^k)$ are of order $p^{kn}-1$; such groups are called the *Singer cycles* of $\mathrm{GL}_n(p^k)$.

Applying Theorem 4.2.2 to the case where $k = 1$, we have the following corollary.

Corollary 4.2.3. *Let p, q be distinct primes. If G is an irreducible subgroup of order q in $\mathrm{GL}_n(p)$, then G is conjugate to a subgroup of a Singer cycle of $\mathrm{GL}_n(p)$.*

The following lemma gives a formula for finding a generator of Singer cycle in $\mathrm{GL}_2(p)$.

Lemma 4.2.4 ([47], Proposition 2.3.6)**.** *If β is a primitive element of $\mathrm{GF}(p^2)^*$, then*

$$B = \begin{pmatrix} 0 & -1 \\ 1 & \beta + \beta^p \end{pmatrix}$$

is a generator of a Singer cycle of $\mathrm{GL}_2(p)$.

Proof. Observe that B is the companion matrix of the minimal polynomial of the diagonal matrix $\mathrm{diag}(\beta, \beta^p)$. Thus $|B| = |\mathrm{diag}(\beta, \beta^p)| = p^2 - 1$ and $\langle B \rangle$ is a Singer cycle. Since all Singer cycles are conjugate in $\mathrm{GL}_2(p)$ by Theorem 4.2.2, the claim follows. □

Similarly, Lemma 4.2.4 generalises to larger linear groups. The following result is briefly discussed in [47, p. 15]; we provide a sketch of a proof.

Theorem 4.2.5. *For each $k \in \{2, 3, 4\}$ fix a primitive element $\beta \in \mathrm{GF}(p^k)^*$. Then the companion matrix of the minimal polynomial of the matrix $\mathrm{diag}(\beta, \beta^p, \ldots, \beta^{(p^{k-1})})$ generates a Singer cycle of $\mathrm{GL}_k(p)$.*

Sketch of proof. Let $P_X(t)$ by the minimal polynomial of $X = \mathrm{diag}(\beta, \beta^p, \ldots, \beta^{(p^{k-1})})$. Since the eigenvalues $\beta, \beta^p, \ldots, \beta^{(p^{k-1})}$ of X are distinct roots of unity in $\mathrm{GF}(p^k)^*$, the characteristic polynomial of X is equal to $P_X(t)$ in this case. By definition, the companion matrix of $P_X(t)$ is conjugate to X in the extension field $\mathrm{GF}(p^k)$, thus $|C| = |X|$. It remains to show that all entries of C lie in $\mathbb{Z}_p$. To see this, it is sufficient to check that all coefficients of $P_X(t)$ are integers. However, we know that $P_X(t) = \sum_{i=0}^{k} (-1)^i \mathrm{tr}(\wedge^i X) t^{k-i}$ since it equals the characteristic polynomial of X, and $\mathrm{tr}(\wedge^i X)$ equals the sum of all principal minors of X of dimension i. An inductive argument shows that $\mathrm{tr}(\wedge^m X) = \sum_{j=0}^{k-1} (\beta^{\sum_{i=0}^{m-1} p^i})^{(p^j)}$ for all $m > 1$. Since the sum $\sum_{j=0}^{k-1} (\beta^{\sum_{i=0}^{m-1} p^i})^{(p^j)}$ is an integer, and the claim follows. □

Since $\mathrm{Aut}(C_p^k) \cong \mathrm{GL}_k(p)$ and all the Singer cycles of $\mathrm{GL}_k(p)$ are conjugate, it follows that the cyclic irreducible subgroups of order b (with $b \mid (p^k - 1)$ and $b \nmid (p^d - 1)$ for all $d < k$) lie in the same subgroup class. We define the canonical choice of the conjugacy class representative for such cyclic irreducible subgroups as follows.

Notation 4.2.6. Let p be a prime. For each $k \in \{2, 3, 4\}$, if b is a positive integer with $b \mid (p^k - 1)$ and $b \nmid (p^d - 1)$ for all $d < k$, then fix a primitive element $\beta \in \mathrm{GF}(p^k)^*$. Let $\gamma = \beta^{(p^k - 1)/b}$. Define

$$\mathrm{Irr}_k(p, b)$$

to be the companion matrix of the minimal polynomial of $\mathrm{diag}(\gamma, \gamma^p, \ldots, \gamma^{(p^{k-1})})$. The cyclic group $\langle \mathrm{Irr}_k(p, b) \rangle$ acts irreducibly on $\mathbb{Z}_p^k$. We say $\mathrm{Irr}_k(p, b)$ is the *canonical generator* of both this irreducible action and the subgroup class representative for cyclic irreducible subgroups of order b in $\mathrm{GL}_k(p)$. We write

$$\mathrm{Irr}_k(p, b, x) = \mathrm{Irr}_k(p, b)^x$$

for $x \in \mathbb{Z}_b$.

The following theorem presents some useful counting formulas for the conjugacy classes of subgroups of $\mathrm{GL}_k(p)$, where $k \in \{2,3,4\}$; see also [24, Theorem 15] or [20, Theorem 3.2] for the first four parts. Recall that

$$\Delta_x^y = \begin{cases} 1 & \text{if } x \mid y \\ 0 & \text{otherwise.} \end{cases}$$

Theorem 4.2.7. *Let p, q, r be distinct primes, and denote the number of conjugacy classes of subgroups of order m in G by $s_m(G)$. Then we have the following results.*

(i) *If $q > 2$, then* $s_q(\mathrm{GL}_2(p)) = \frac{1}{2}(q+3)\Delta_{p-1}^q + \Delta_{p+1}^q$;
$s_2(\mathrm{GL}_2(p)) = 2$.

(ii) $s_{q^2}(\mathrm{GL}_2(p)) = \Delta_{p-1}^q + \frac{1}{2}(q^2+q+2)\Delta_{p-1}^{q^2} + \Delta_{p+1}^{q^2}$.

(iii) *If $q, r > 2$, then* $s_{qr}(\mathrm{GL}_2(p)) = \frac{1}{2}(qr+q+r+5)\Delta_{p-1}^{qr} + \Delta_{p+1}^{qr}$;
if $r > 2$, then $s_{2r}(\mathrm{GL}_2(p)) = \frac{1}{2}(3r+7)\Delta_{p-1}^r + 2\Delta_{p+1}^r$.

(iv) *If $q > 2$, then*

$$\begin{aligned} s_q(\mathrm{GL}_3(p)) = {} & \frac{1}{6}(q^2+4q+9+4\Delta_{q-1}^3)\Delta_{p-1}^q \\ & + \Delta_{(p+1)(p^2+p+1)}^q(1-\Delta_{p-1}^q); \end{aligned}$$

$s_2(\mathrm{GL}_3(p)) = 3$.

(v) *If $q > 2$, then*

$$\begin{aligned} s_q(\mathrm{GL}_4(p)) = {} & \frac{1}{24}(q^3+7q^2+21q+39+16\Delta_{q-1}^3+12\Delta_{q-1}^4)\Delta_{p-1}^q \\ & + \frac{1}{4}(q+5+2\Delta_{q-1}^4)\Delta_{p+1}^q \\ & + \Delta_{p^2+p+1}^q(1-\Delta_q^3) \\ & + \Delta_{p^2+1}^q; \end{aligned}$$

$s_2(\mathrm{GL}_4(p)) = 4$.

Proof. For each $n \in \{2,3,4\}$, let $\mathrm{Diag}_n \cong C_{p-1}^n$ be the subgroup of diagonal matrices in $\mathrm{GL}_n(p)$. By [19, Lemma 8], each subgroup $H \leq \mathrm{GL}_2(p)$ with cubefree order coprime to p is conjugate to a subgroup of $N \cong C_2 \ltimes S$ (Singer normaliser), where $S = \langle \mathrm{Irr}_2(p, p^2-1) \rangle$ is the canonical Singer cycle defined in Notation 4.2.6, or of a subgroup $C_2 \ltimes \mathrm{Diag}_2$ (maximal primitive).

Since two diagonalisable matrices are conjugate if and only if they have the same multiset of eigenvalues, it follows that two cyclic subgroups of Diag_n are conjugate if and only if they are equivalent under the permutation action of Sym_n on the diagonal entries. It follows that a cyclic subgroup in Diag_n of order $m > 1$ is generated by $\mathrm{diag}(a, a^{k_1}, \ldots, a^{k_n})$ where $a \in \mathbb{Z}_p^*$ has order m and $k_i \in \mathbb{Z}_m$. In particular, a direct calculation shows that cyclic subgroups generated by $\mathrm{diag}(a, a^k)$ and $\mathrm{diag}(a, a^\ell)$, with $k, \ell \in \mathbb{Z}_m$, are conjugate in $\mathrm{GL}_2(p)$ if and only if $k = \ell$ or there exists some $x \in \mathbb{Z}_m^*$ such that $k = x^{-1}$ and $\ell = x$. Analogously, subgroups $\langle \mathrm{diag}(a, a^k, a^\ell) \rangle$ and $\langle \mathrm{diag}(a, a^u, a^v) \rangle$ with $k, \ell, u, v \in \mathbb{Z}_m$ are conjugate in $\mathrm{GL}_3(p)$ if and only if $\{k, \ell\} \in \{\{u, v\}, \{uv^{-1}, v^{-1}\}, \{u^{-1}v, u^{-1}\}\}$. Similarly, for $k, \ell, m, u, v, w \in \mathbb{Z}_m$, the subgroups $\langle \mathrm{diag}(a, a^k, a^\ell, a^m) \rangle$ and $\langle \mathrm{diag}(a, a^u, a^v, r^w) \rangle$ are conjugate in $\mathrm{GL}_4(p)$ if and only if

$\{k,\ell,m\} \in \{\{u,v,w\},\{u^{-1},u^{-1}v,u^{-1}w\},\{v^{-1},v^{-1}w,uv^{-1}\},\{w^{-1},uw^{-1},vw^{-1}\}\}$. We use these results in tandem with Theorem 4.2.2, Corollary 4.2.3, and Notations 4.1.1, 4.2.1, 4.2.6 in the following.

(i) Since $|\mathrm{GL}_2(p)| = p(p-1)^2(p+1)$, there exists a cyclic group of order q in $\mathrm{GL}_2(p)$ if and only if $q \mid (p-1)(p+1)$. In particular, there exists a unique conjugacy class of irreducible subgroup of order q if and only if $q \mid (p+1)$ and $q \nmid (p-1)$ by Theorem 4.2.2 and Corollary 4.2.3, which requires $q > 2$, accounting for the summand Δ^q_{p+1}. If $q \mid (p-1)$, then every subgroup of order q is diagonalisable in $\mathrm{GL}_2(p)$, thus conjugate to a subgroup of $D = \mathrm{Diag}_2$. Let $a = \rho(p,q)$ and let $r = \sigma_q$ (see Notation 4.1.1). Then a has order q in $\mathbb{Z}_p^*$ and r has order $q-1$ in $\mathbb{Z}_q^*$. There are $1 + \frac{1}{2}(q+1-\Delta_q^2)$ conjugacy classes of cyclic reducible subgroups with representatives generated by $\mathrm{diag}(a,1)$ and $\mathrm{diag}(a,a^{(r^k)})$ with $k \in \{0,\ldots,\lfloor\frac{1}{2}(q-1)\rfloor\}$, accounting for the summand $\frac{1}{2}(q+3)\Delta^q_{p-1}$. Lastly, since any subgroup of order 2 in $\mathrm{GL}_2(p)$ is reducible, there are two conjugacy classes of such subgroups with representatives generated by $\mathrm{diag}(1,-1)$ and $\mathrm{diag}(-1,-1)$; we obtain $s_2(\mathrm{GL}_2(p)) = 2$.

(ii) If $q \mid (p+1)$ and $q \nmid (p-1)$, then all cyclic subgroups of order q in $\mathrm{GL}_2(p)$ are irreducible and conjugate to subgroups of S, the canonical Singer cycle. This shows that for a group Q of exponent q, if $q \mid (p+1)$ and $q \nmid (p-1)$, then Q is conjugate to a subgroup of S. It follows that there exists a noncyclic subgroup of order q^2 in $\mathrm{GL}_2(p)$ if and only if $q \mid (p-1)$. Moreover, such groups are reducible and conjugate to the unique elementary abelian subgroup of order q^2 in $\mathrm{Diag}_2 \cong C_{p-1}^2$, accounting for the summand Δ^q_{p-1}. It remains to consider the cyclic subgroups of order q^2. In particular, a cyclic irreducible subgroup of order q^2 exists in $\mathrm{GL}_2(p)$ if and only if $q^2 \mid (p+1)$ and $q^2 \nmid (p-1)$; such groups lie in a single conjugacy class, accounting for the summand $\Delta^{q^2}_{p+1}(1-\Delta^{q^2}_{q-1}) = \Delta^{q^2}_{p+1}$. On the other hand, a cyclic reducible subgroup of order q^2 exists if and only if $q^2 \mid (p-1)$; such groups are diagonalisable and conjugate to subgroups of Diag_2. Let $\alpha = \sigma_{q^2}$ and $a = \rho(p,q^2)$. Then we count the subgroup classes by explicitly determining the representatives: there is a unique class represented by $\langle \mathrm{diag}(a,1)\rangle$; there are $q^2 - q(q-1)$ classes represented by $\langle \mathrm{diag}(a,a^x)\rangle$ with non-units $x \in \mathbb{Z}_{q^2}\backslash\mathbb{Z}_q^*$; there are $\frac{1}{2}(q^2+q+2)$ classes with representatives $\langle \mathrm{diag}(a,a^{(\sigma_q^k)})\rangle$, where $0 \le k \le \frac{1}{2}q(q-1)$, in one-to-one correspondence with the orbits of $\mathbb{Z}_{q^2}^*$ under inversion. Thus, we count $\frac{1}{2}(q^2+q+2)\Delta^{q^2}_{p-1}$ conjugacy classes of cyclic reducible subgroups of order q^2 in $\mathrm{GL}_2(p)$.

(iii) A cyclic irreducible subgroup of order qr exists in $\mathrm{GL}_2(p)$ if and only if $qr \mid (p^2-1)$ and $qr \nmid (p-1)$; such a group is unique up to conjugacy, accounting for the summand $\Delta^{qr}_{p+1}(1-\Delta^{qr}_{p-1})$. In particular, if $q,r > 2$, then this summand simplifies to Δ^{qr}_{p+1}; if $q = 2$, then it simplifies to Δ^r_{p+1}. On the other hand, if $qr \mid (p-1)$, then every cyclic subgroup of such order is reducible and diagonalisable in $\mathrm{GL}_2(p)$; such a subgroup is conjugate to a subgroup in $D = \mathrm{Diag}_2$ and has a generator of the form $\mathrm{diag}(a,a^k)$ for some $a \in \mathbb{Z}_p^*$ with order qr and $k \in \mathbb{Z}_{qr}$, or $\mathrm{diag}(b,c)$ with $b,c \in \mathbb{Z}_p^*$ of order q,r respectively. In the latter case, there is a unique such subgroup in D. It remains to count the conjugacy classes of the subgroups of the form $\langle \mathrm{diag}(a,a^k)\rangle$. If $k \in \mathbb{Z}_{qr}\backslash\mathbb{Z}_{qr}^*$, then there exists no $x \in \mathbb{Z}_{qr}^*$ such that $k = x^{-1}$, thus the $q+r-1$ non-units in $\mathbb{Z}_{qr}$ account for $(q+r-1)\Delta^{qr}_{p-1}$ classes. If $k \in \mathbb{Z}_{qr}^*$, then it is equivalent to counting the number of orbits of $\mathbb{Z}_{qr}^*$ under inversion: there are $\frac{1}{2}(qr-q-r+5-2\Delta_q^2)$ orbits in this case. Thus, we count $\frac{1}{2}(qr+q+r+5-2\Delta_q^2)\Delta^q_{p-1}$ classes of cyclic reducible subgroups of order qr.

A nonabelian subgroup H of order qr exists in $\mathrm{GL}_2(p)$ if and only if $qr \mid 2(p^2-1) = |N|$ or $qr \mid 2(p-1)^2 = 2|D|$. Both cases require that $q = 2$ and $r \mid (p^2-1)$. In particular, if $r \mid (p+1)$, then H is irreducible and conjugate to a subgroup in $N \cong C_2 \ltimes S$; if $r \mid (p-1)$, then H is reducible and conjugate to a subgroup in $C_2 \ltimes D$. In either case, H is unique up to conjugacy, accounting for the summand $(\Delta_{p+1}^r + \Delta_{p-1}^r)\Delta_q^2$. More specifically, if $r \mid (p+1)$, then the subgroup class containing H has a representative generated by $\{\left(\begin{smallmatrix}0&1\\1&0\end{smallmatrix}\right), \mathrm{Irr}_2(p,r)\}$; if $r \mid (p-1)$, then the subgroup class has a representative generated by $\{\left(\begin{smallmatrix}0&1\\1&0\end{smallmatrix}\right), \mathrm{diag}(\rho(p,r), \rho(p,r,r-1))\}$.

In total, we find

$$\frac{1}{2}(qr+q+r+5-\Delta_q^2)\Delta_{p-1}^{qr} + \Delta_{p+1}^{qr}(1-\Delta_{p-1}^{qr}) + (\Delta_{p+1}^r + \Delta_{p-1}^r)\Delta_q^2$$

classes, which simplifies to the claimed result if we consider the cases $q, r > 2$ and $r > q = 2$ separately.

(iv) A cyclic subgroup of order q in $\mathrm{GL}_3(p)$ is diagonalisable if and only if $q \mid (p-1)$. Since two diagonalisable matrices are conjugate if and only if they have the same multiset of eigenvalues, we can count the conjugacy classes of such groups by considering three non-conjugate types, namely, groups with a generating element of the form $\mathrm{diag}(a,1,1)$, $\mathrm{diag}(a, a^{(\alpha^k)}, 1)$, and $\mathrm{diag}(a, a^{(\alpha^k)}, a^{(\alpha^\ell)})$, where $a \in \mathbb{Z}_p^*$ has order q, and $\alpha \in \mathbb{Z}_q^*$ has order $q-1$. In particular, the first two types embed into $\mathrm{GL}_2(p)$, which are considered in (i), and we find $\frac{1}{2}(q+3)\Delta_{p-1}^q$ classes of these groups for $q > 2$ and 2 classes for $q = 2$. It remains to consider the third type. For $q = 2$, there is a unique conjugacy class of such groups. If $q > 2$ then the cyclic subgroups $\langle \mathrm{diag}(a, a^{(\alpha^k)}, a^{(\alpha^\ell)})\rangle$ and $\langle \mathrm{diag}(a, a^{(\alpha^x)}, a^{(\alpha^y)})\rangle$ are conjugate if and only if $\{x,y\} \in \{\{k,\ell\}, \{-k, \ell-k\}, \{-\ell, k-\ell\}\}$. This is equivalent to saying that (x,y) and (k,ℓ) are in the same orbits under the action of $\mathrm{Sym}_3 \cong \langle \left(\begin{smallmatrix}0&1\\1&0\end{smallmatrix}\right), \left(\begin{smallmatrix}0&1\\-1&-1\end{smallmatrix}\right)\rangle$ on the set $\mathbb{Z}_{q-1}^2$. Thus the number of conjugacy classes of such subgroups of order q in $\mathrm{GL}_3(p)$ coincides with the size of the Sym_3-orbits in $\mathbb{Z}_{q-1}^2$. Let $\Omega = \mathbb{Z}_{q-1}^2$ and let $\mathrm{Fix}_\Omega(g)$ be the set of fixed points in Ω of g for each $g \in \mathrm{Sym}_3$. A direct computation shows that

$$|\mathrm{Fix}_\Omega(g)| = \begin{cases} (q-1)^2 & \text{if } g = \left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right); \\ q-1 & \text{if } g = \left(\begin{smallmatrix}0&1\\1&0\end{smallmatrix}\right); \\ q & \text{if } g \in \{\left(\begin{smallmatrix}-1&-1\\0&1\end{smallmatrix}\right), \left(\begin{smallmatrix}1&0\\-1&-1\end{smallmatrix}\right)\}; \\ 2\Delta_{q-1}^3 & \text{if } g \in \{\left(\begin{smallmatrix}0&1\\-1&-1\end{smallmatrix}\right), \left(\begin{smallmatrix}-1&-1\\1&0\end{smallmatrix}\right)\}. \end{cases}$$

Using the Cauchy–Frobenius orbit-counting formula (see Theorem A.0.14), we count $\frac{1}{6}(q^2+q+4\Delta_{q-1}^3)\Delta_{p-1}^q$ orbits. Together, there are $\frac{1}{6}(q^2+4q+9+4\Delta_{q-1}^3)\Delta_{p-1}^q$ classes of diagonalisable groups of order q if $q > 2$, and 3 classes if $q = 2$. The non-diagonalisable groups exist if only if $q \mid (p+1)(p^2+p+1)$ and $q \nmid (p^2-1)$, requiring $q > 2$. Such groups arise from the irreducible subgroups of $\mathrm{GL}_2(p)$ if $2 < q \mid (p+1)$, or from that of $\mathrm{GL}_3(p)$ if $3 < q \mid (p^2+p+1)$, accounting for the summand $\Delta_{(p+1)(p^2+p+1)}^q(1-\Delta_{p-1}^q)$, which is equivalent to $\Delta_{p+1}^q(1-\Delta_q^2) + \Delta_{p^2+p+1}^q(1-\Delta_q^2)(1-\Delta_q^3)$.

(v) A cyclic subgroup of order q in $\mathrm{GL}_4(p)$ is diagonalisable if and only if $q \mid (p-1)$. The conjugacy classes of these subgroups have representatives in Diag_4, which are generated by four types of matrices: $\mathrm{diag}(a,1,1,1)$, $\mathrm{diag}(a, a^{(\alpha^k)}, 1, 1)$, $\mathrm{diag}(a, a^{(\alpha^k)}, a^{(\alpha^\ell)}, 1)$, and $\mathrm{diag}(a, a^{(\alpha^k)}, a^{(\alpha^\ell)}, a^{(\alpha^m)})$, where $a \in \mathbb{Z}_p^*$ has order q, $\alpha \in \mathbb{Z}_q^*$ has order $q-1$, and

$k, \ell, m \in \mathbb{Z}_{q-1}$. The first three types of groups embed into $\mathrm{GL}_3(p)$ and fall into $\frac{1}{6}(q^2+4q+9+4\Delta_{q-1}^3)\Delta_{p-1}^q + \Delta_{(p+1)(p^2+p+1)}^q(1-\Delta_{p-1}^q)$ classes if $q > 2$, or 3 classes if $q = 2$, as counted in (iv). It remains to count the number of classes of the fourth type. A direct computation shows that two cyclic subgroups $\langle \mathrm{diag}(a, a^{(\alpha^k)}, a^{(\alpha^\ell)}, a^{(\alpha^m)})\rangle$ and $\langle \mathrm{diag}(a, a^{(\alpha^x)}, a^{(\alpha^y)}, a^{(\alpha^z)})\rangle$ are conjugate if and only if the parameters $x, y, z, k, \ell, m \in \mathbb{Z}_{q-1}$ satisfy

$$\{x,y,z\} \in \{\{k,\ell,m\}, \{-k, \ell-k, m-k\}, \{-\ell, m-\ell, k-\ell\}, \{-m, k-m, \ell-m\}\}.$$

It is equivalent to saying that the triples $(x,y,z), (k,\ell,m) \in \mathbb{Z}_{q-1}^3$ lie in the same orbit under the action of

$$\mathrm{Sym}_4 \cong \langle \begin{pmatrix} -1 & 0 & 0 \\ -1 & 1 & 0 \\ -1 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & -1 & 0 \\ 0 & -1 & 1 \\ 1 & -1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & -1 \\ 1 & 0 & -1 \\ 0 & 1 & -1 \end{pmatrix} \rangle$$

on $\mathbb{Z}_{q-1}^3$. Similar to (iv), we can explicitly count the fixed points of each element in Sym_4, and then applying the orbit-counting formula yields that there are 4 classes of the diagonalisable subgroups of the fourth type when $q = 2$ and $\frac{1}{24}(q^3+3q^2+5q+3+12\Delta_{q-1}^4)$ classes when $q > 2$. Adding up all four cases, we obtain $s_2(\mathrm{GL}_4(p)) = 4$ and the summand $\frac{1}{24}(q^3+7q^2+21q+39+16\Delta_{q-1}^3+12\Delta_{q-1}^4)\Delta_{p-1}^q$ for $q > 2$. A cyclic reducible subgroup is non-diagonalisable in $\mathrm{GL}_4(p)$ if and only if its generator is conjugate to a block diagonal matrix $\mathrm{diag}(M, N)$ with at least one of M, N being non-diagonalisable. Thus, the representatives for the conjugacy classes of the reducible non-diagonalisable subgroup of order q are generated by $\mathrm{diag}(\mathrm{Irr}_2(p,q), \mathrm{Irr}_2(p,q,k))$, where $\mathrm{Irr}_2(p,q,k)$ is conjugate to $\mathrm{Irr}_2(p,q)^k$ for $k \in \mathbb{Z}_q$, or $\mathrm{diag}(\mathrm{Irr}_3(p,q), 1)$. The latter case exists if and only if $q \mid (p^2+p+1)$ and $q \nmid (p-1)$; the group generated by $\mathrm{diag}(\mathrm{Irr}_3(p,q), 1)$ is unique up to conjugacy and contributes to the summand $\Delta_{p^2+p+1}^q(1-\Delta_{p-1}^q)$. The former case requires that $q \mid (p+1)$ and $p \nmid (p-1)$; two such groups are conjugate if and only if they have the same set of eigenvalues over $\mathrm{GF}(p^2)$. If $k = 0$ then there is a unique conjugacy class of such groups. It remains to consider $k \in \mathbb{Z}_q^*$. Let $\alpha \in \mathbb{Z}_q^*$ have order $q-1$. Since two matrices $\mathrm{diag}(\mathrm{Irr}_2(p,q), \mathrm{Irr}_2(p,q,\alpha^k))$ and $\mathrm{diag}(\mathrm{Irr}_2(p,q), \mathrm{Irr}_2(p,q,\alpha^\ell))$ are conjugate in $\mathrm{GL}_2(p)$ if and only if they have the same multiset of eigenvalues in $\mathrm{GL}_2(\mathrm{GF}(p^2))$, we deduce that two cyclic groups $\langle \mathrm{diag}(\mathrm{Irr}_2(p,q), \mathrm{Irr}_2(p,q,\alpha^k))\rangle$ and $\langle \mathrm{diag}(\mathrm{Irr}_2(p,q), \mathrm{Irr}_2(p,q,\alpha^\ell))\rangle$ are conjugate in $\mathrm{GL}_2(p)$ if and only if $k \in \{\ell, -\ell, -\ell+\frac{1}{2}(q-1), -\ell-\frac{1}{2}(q-1)\}$. This shows that if $q \mid (p+1)$ and $q > 2$ then the conjugacy subgroup class representatives have the form $\langle \mathrm{diag}(\mathrm{Irr}(p,q), 1)\rangle$ or $\langle \mathrm{diag}(\mathrm{Irr}_2(p,q), \mathrm{Irr}(p,q,\alpha^k))\rangle$ with $0 \le k \le \frac{1}{4}(q-1)$, accounting for the summand $\frac{1}{4}(q+5+2\Delta_{q-1}^4)\Delta_{p+1}^q$. Lastly, an irreducible subgroup exists if and only if $q \mid (p^4-1)$ and $q \nmid (p^3-1)(p^2-1)$. This requires that $q > 2$ and $q \mid (p^2+1)$; such groups are conjugate to the unique subgroup of order q in the Singer cycle of $\mathrm{GL}_4(p)$, which accounts for the summand $\Delta_{p^2+1}^q$ for $q > 2$. □

Theorem 4.2.7 plays a significant role in later chapters when we enumerate and construct the isomorphism classes of split extensions of elementary abelian groups. Moreover, the proof of Theorem 4.2.7 is "constructive", in the sense that we have implicitly found conjugacy class representatives, which in conjunction with Corollary 2.4.3 gives a way to find the isomorphism classes representatives of certain split extensions. We conclude this section by presenting a result that gives a useful method to count the conjugacy classes of subgroups of prime order in a more general setting.

Lemma 4.2.8 ([25], Lemma 9)**.** *Let p and q be distinct primes and let G and H be finite groups. If there exists a homomorphism $\varphi\colon G \to H$ such that* Ker *φ is a p-group, then G and H have the same number of conjugacy classes of subgroups of order q.*

Let G be a finite group. Recall that $O_p(G)$ is the largest normal p-subgroup of G. The natural projection $\pi\colon G \to O_p(G)$ is a homomorphism with p-group kernel and Im $\pi \cong G/O_p(G)$. Thus Lemma 4.2.8 applies and the number of conjugacy classes of subgroups of order q in G coincides with that in $G/O_p(G)$. Once we know an explicit presentation of P whose order divides p^4, we can directly compute $\mathrm{Aut}(P)/O_p(\mathrm{Aut}(P))$ (see also [46] for computation of automorphisms of p-groups). In accompany with Corollary 2.4.3(ii), this result provides a powerful tool for enumerating the isomorphism types of split extensions of P by a cyclic group.

Part II

Determination of groups whose order factors into at most four primes

In this part of the thesis, we explicitly determine the isomorphism types of groups whose orders factorise into at most four primes. Finite abelian groups are fully classified by the fundamental theorem of finitely generated abelian groups (Theorem A.0.12). For this reason, we omit further details for the determination of finite abelian groups. Groups of order dividing p^4 and squarefree groups are well-studied and there are abundant theoretical and computational results in the literature. We thus concentrate on the remaining order types and only include a brief summary of results regarding squarefree and p-power orders for the sake of completeness. For all order types that are products of at most four primes, we list the isomorphism class representatives in Tables 5.1, 5.3, 5.4, 6.1, 6.2, 6.3, 6.4, 7.1, 7.2, and 7.3. To make the tables less clustered, we omit the list of pcgs and abbreviate every pc-presentation by only listing its nontrivial relators. For example, we write $a^p, b^p, c^p, b^a/bc$ for the group described by $\mathrm{Pc}\langle a, b, c \mid a^p, b^p, c^p, b^a/bc\rangle$. Furthermore, we use notations defined in Chapter 4 for the canonical automorphisms throughout the rest of the thesis.

We remark that our counting formulas for groups of order $n \in \{p^2q, p^2q^2, p^3q, p^2qr\}$ agree with Eick's results in [24], which motivated our collaboration with Eick. In 2021, we merged our results to present both the enumeration results and a complete list of isomorphism class representatives of the groups of said order types. Along the way, we noticed that a few methods and results of Eick could be applied to simplify some of our proofs in this thesis. We now present the modified version, which shares some similarities with [20, 24]. We also note that the published version of these results is very concise, but in this thesis we provide more details on how to explicitly determine the isomorphism representatives and we verify that our results give nonisomorphic groups by studying the possible isomorphisms. Our proofs in this thesis involve more technical manipulations of polycyclic presentations and some number theoretical discussion, along with a brief discussion of isomorphisms between two groups with different presentations that are in the same isomorphism class, which will be useful for our later derivation of an isomorphism function (see Section 8.3).

We present our main results in three chapters: we discuss the p-groups of order dividing p^4 in Chapter 5, followed by the determination of groups whose orders are of the form p^aq^b with $a + b \leq 4$ in Chapter 6, and then we look into groups whose orders have three or more distinct prime factors in Chapter 7. The approach described in Chapter 5 is different to what is used in Chapters 6 and 7, which results in different table layouts in the result summary. In addition to the determination of the isomorphism types in Chapter 5, we present some information about the subgroup analysis and some results regarding relevant automorphism groups, which provide useful references for later chapters. For each order type, we structure the respective section as follows: we first summarise the results in the main theorem and corresponding tables, then we present the proofs of the determination of the isomorphism types. The derivation of these proofs involves some technical manipulation of pc-presentations, but as the main technique is repetitively used in such calculations in later parts of the proofs, thus we omit some of the details. The main approach to derive the explicit construction is to exploit the presentations of polycyclic group extensions in combination with our classification of split extensions and the enumeration of conjugacy classes of subgroups with certain properties in small linear groups that we discussed in Part I.

Chapter 5

Groups of order p^n with $n \leq 4$

Let p denote a prime number. Groups of p-power order are well-studied and the p-group generation algorithm [39, 40] can be used for the construction of such groups; this algorithm is available in GAP [27] and MAGMA [12], efficient for groups of order dividing p^7. In particular, Cole and Glover [18] determined groups of order dividing p^3, Adler, Garlow, and Wheland [1] explicitly determined groups of order off order p^4, and Wild [52] determined groups of order 16. It is thus not the focus of this exposition to study p-groups in depth. Nevertheless, as building blocks for larger solvable groups, the isomorphism class representatives of the groups of order dividing p^4 are of great importance. We list the isomorphism types using pc-presentations, and discuss a few structural results that are fundamental to later chapters; we include some proofs for the sake of completeness. A few general results from [3, Chapter 4], [23, § 5.3 - 6.1], and [45] regarding p-groups are essential to the classification of p-groups. For an extensive account on the structure of groups of p-power order, we refer to the series of books of Berkovich [3] and Leedham-Green & McKay [38].

5.1 Groups of order p^n with $n \leq 3$

5.1.1 Summary of results

We introduce a nonstandard but convenient notation for the p-groups in the tables by assigning each isomorphism type an "SOT ID", namely, $(n : i)$, where n denotes the order of the group, and i is the ordinal mark given to the type.[1] The same assignment of these IDs is implemented in our package `SOTGrps` [20], which we discuss in more detail in Chapter 8. Note that GAP's SmallGroups library already stores an identification code for each group of order dividing p^4. As a reminder that the SOT IDs are not necessarily the same as the GAP IDs, we also list the GAP IDs in the tables for p-groups. However, by "ID" we always mean the SOT ID throughout the thesis. If we recognise a group as an extension of certain groups, say A and B, then we write $A \ltimes B$ for an extension that splits over B, where A acts nontrivially on B, and write $A.B$ exclusively for a nonsplit extensions of B by A.

Recall that a group G of order p^{1+2m} is an *extraspecial* group if $[G, G] = \Phi(G) = Z(G) \cong C_p$ and $G/Z(G)$ is a nontrivial elementary abelian group. For each $m \in \mathcal{N}^+$, there are exactly two

[1] Note that this colon-notation is only used in this thesis as a differentiation between the SOT IDs and the GAP IDs of p-groups, but in our implementation `SOTGrps` [20] we simply write $[n, i]$.

nonisomorphic extraspecial groups of order p^{1+2m} (see Theorem A.0.7). Recall that for a finite group G, the least nonzero number n such that $g^n = 1$ for all $g \in G$ is called the *exponent* of G, often denoted by $\exp(G)$. For $p > 2$ and each positive integer m, it is conventional to denote the isomorphism type of exponent p by p_+^{1+2m} and denote the one of exponent p^2 by p_-^{1+2m}. For $p = 2$ and $m = 1$, we adopt the convention to denote 2_+^{1+2} for D_4 and 2_-^{1+2} for Q_8; for $p = 2$ and $m > 2$, the "+" type denotes the groups that contains an even number of copies of Q_8 in the central product, and the "−" type denotes the groups that contain an odd number of copies of Q_8.

TABLE 5.1: Groups whose orders divide p^3.

Order type	SOT ID	PC-relators	Structure	GAP ID
$\|G\| = p$				
	$(p:1)$	a^p	C_p	$(p, 1)$
$\|G\| = p^2$				
	$(p^2:1)$	a^{p^2}	C_{p^2}	$(p^2, 1)$
	$(p^2:2)$	a^p, b^p	C_p^2	$(p^2, 2)$
$\|G\| = p^3$				
	$(p^3:1)$	a^{p^3}	C_{p^3}	$(p^3, 1)$
	$(p^3:2)$	a^{p^2}, b^p	$C_{p^2} \times C_p$	$(p^3, 2)$
	$(p^3:3)$	a^p, b^p, c^p	C_p^3	$(p^3, 5)$
$p > 2$	$(p^3:4)$	$a^p, b^p, c^p, b^a/bc$	p_+^{1+2}	$(p^3, 3)$
	$(p^3:5)$	$a^p/c, b^p, c^p, b^a/bc$	p_-^{1+2}	$(p^3, 4)$
2^3	$(8:4)$	$a^2, b^2, c^2, b^a/bc$	D_4	$(8, 3)$
	$(8:5)$	$a^2/b^2, b^4, b^a/b^3$	Q_8	$(8, 4)$

Theorem 5.1.1. *A group of order p is cyclic and simple. A group of order p^2 is either cyclic or elementary abelian. There are three abelian and two isomorphism types of nonabelian groups of order p^3; the two nonabelian groups of order p^3 are extraspecial. Up to isomorphism, the groups of order dividing p^3 are the ones given in Table 5.1.*

Recall that we abuse the notation: For example, the group with SOT ID $(p^3 : 4)$ is

$$\mathrm{Pc}\langle a, b, c \mid a^p, b^p, c^p, b^a/bc\rangle = \langle a, b, c \mid a^p, b^p, c^p, b^a/bc, c^a = c, c^b = c\rangle.$$

This group is isomorphic to the extraspecial group p_+^{1+2} of order p^3 of exponent p.

5.1.2 Determination of groups of order dividing p^3

The classification of groups of prime order p follows directly from Lagrange's theorem: a group of prime order is simple as it contains no nontrivial proper subgroups and each non-identity element of a group of order p is a generator of the entire group. It remains to consider p-groups with order p^n where $n > 1$. The next theorem summarises some well-known results.

Theorem 5.1.2 ([15], Theorem III; [45], Theorem 4.4; [23]). *Let G be a nontrivial finite p-group.*

(i) *If $p^k \mid |G|$, then G contains a normal subgroup of order p^k.*

(ii) *If H is a subgroup of G of index p, then $H \lhd G$.*

(iii) *G has a nontrivial centre.*

(iv) *If G is nonabelian, then $G/Z(G)$ is not cyclic.*

The classification of groups of order p^2 and nonabelian groups of order p^3 follows from Theorem 5.1.2 directly.

Corollary 5.1.3. *If G is a group of order p^2, then G is isomorphic to C_p^2 or C_{p^2}.*

Proof. Let G be a group of order p^2. Then Theorem 5.1.2 asserts that G has a nontrivial centre. Suppose that G is nonabelian, then $|Z(G)| = p$ and $G/Z(G)$ is cyclic, which contradicts Theorem 5.1.2(iv). Hence, G is abelian and Theorem A.0.12 shows G is isomorphic to C_p^2 or C_{p^2}. □

It remains to consider the groups of order p^3. The abelian isomorphism types of subgroups are characterised by Theorem A.0.12.

Lemma 5.1.4. *There are three abelian isomorphism types of the groups of order p^3, namely,*

$$C_{p^3}, \quad C_p \times C_{p^2}, \quad C_p^3.$$

Nonabelian groups of order p^3 are extraspecial.

Proof. Suppose that G is a nonabelian group of order p^3. Then Theorem 5.1.2 implies that $Z(G) \cong C_p$. Since $G/Z(G)$ is noncyclic and has order p^2, it is isomorphic to C_p^2 by Corollary 5.1.3. Hence, $[G, G] \leq Z(G)$. Since $[G, G] \neq 1$, it follows that $[G, G] = Z(G)$ and G is extraspecial. □

The following commutator formula follows from a direct computation; it is useful for our later discussion.

Lemma 5.1.5. *Let G be a group with $[G, G] \leq Z(G)$. Then for any $x, y \in G$ and $n \in \mathbb{N}^+$, we have $(xy)^n = x^n y^n [y, x]^{\frac{1}{2}n(n-1)}$.*

Proof. Since $[y, x] \in Z(G)$, we have that $yx = xy[y, x] = [y, x]xy$, and so

$$\begin{aligned}(xy)^n &= (xy) \cdots (xy) = x^n [y, x] y \ldots [y, x] y \\ &= x^n y^n [y, x]^{(n-1)+(n-2)+\cdots+1} = x^n y^n [y, x]^{\frac{1}{2}n(n-1)}.\end{aligned}$$ □

The following result about nonabelian groups of order p^3 seems well-known, we present a proof for the sake of completeness. [46].

Lemma 5.1.6. *Let G be a nonabelian group of order p^3. If $p > 2$, then G has a normal subgroup isomorphic to C_p^2; if $p = 2$, then G has a cyclic normal subgroup of order 4.*

Proof. If $p > 2$, then Corollary 5.1.4 and Lemma 5.1.5 imply that $[G, G] \cong C_p$, and for all $x, y \in G$, we have

$$(xy)^p = x^p y^p [y, x]^{\frac{1}{2}p(p-1)} = x^p y^p.$$

Thus, the power map $f\colon G \to G, g \mapsto g^p$ is an endomorphism of G. We claim that the kernel of this power map is isomorphic to C_p^2. To see this, first note that $Z(G)$ is contained in Ker f as $Z(G)$ is cyclic of order p. We now show that $Z(G)$ is properly contained in Ker f: suppose for contradiction that $Z(G)$ equals the kernel, then the first isomorphism theorem implies that the image of f is isomorphic to $G/Z(G)$, which is isomorphic to C_p^2 by Corollary 5.1.4. Since the power map is an endomorphism of G, this shows that G has a subgroup isomorphic to C_p^2. However, such a subgroup has exponent p, hence must also be in Ker f, contradicting our assumption. Hence Ker f has at least p^2 elements and is of exponent p. If it has order p^2, then Ker $f \cong C_p^2$, and it is normal in G; if it has order p^3, then G must have exponent p. In the latter case, take $g \in G \backslash Z(G)$, then $\langle g, Z(G)\rangle \cong C_p^2$, which is normal in G by Theorem 5.1.2(ii). If $p = 2$, then there is $a \in G$ such that $|a| > 2$, since otherwise G is abelian by Theorem A.0.4; now $\langle a\rangle \cong C_4$ is normal in G by Theorem 5.1.2(ii). □

It follows from Theorem 5.1.2 that every finite p-group admits a cyclic subnormal series, thus is polycyclic. Lemma 5.1.6 implies that, if p is an odd prime, then all nonabelian groups of order p^3 can be constructed by extending C_p^2 by C_p; all nonabelian groups of order 2^3 can be constructed by extending C_4 by C_2.

Lemma 5.1.7. *A nonabelian group G of order 8 is isomorphic to D_4 or Q_8.*

Proof. Any nonabelian group G of order 8 contains a normal subgroup $N \cong C_4$ by Lemma 5.1.6. The determination of such groups follows from Example 3.3.1. □

Lemma 5.1.8. *A nonabelian group of odd order p^3 is isomorphic to p_+^{1+2} or p_-^{1+2} with a presentation encoded Table 5.1.*

Proof. It follows from Lemma 5.1.4 that such a group G is extraspecial. We now show that there are two isomorphism types of such groups and present the isomorphism class representatives. Note that Lemma 5.1.6 asserts that there exists a normal subgroup $N \cong C_p^2$ in G. Since G/N is cyclic, N contains $[G, G] = Z(G)$. Thus, every such group has a pc-presentation of the form

$$G(i, j, e, f) = \mathrm{Pc}\langle a, b, c \mid a^p = b^i c^j, b^p, c^p, b^a = b^e c^f\rangle,$$

for some $i, j, e, f \in \mathbb{Z}_p$ such that $e > 0$ and $Z(G) = \langle c\rangle \leq N = \langle b, c\rangle$. The relations $b^a = b^e c^f$ and $c^a = c$ reflect the G/N-module structure of N, which is represented by $a \mapsto \left(\begin{smallmatrix} e & f \\ 0 & 1 \end{smallmatrix}\right)$ acting from the right on the row vectors generated by $b = (1\ 0)$ and $c = (0\ 1)$. Since $|a| = p$, we have

$$\begin{pmatrix} e & f \\ 0 & 1 \end{pmatrix}^p = \begin{pmatrix} e^p & f\sum_{i=0}^{p-1} e^i \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

In particular, this shows that $e^p = 1$, forcing $e = 1$. Since $b \notin Z(G)$ by assumption, we must have $f \neq 0$. For any $f \in \mathbb{Z}_p^*$ the change of basis from $\{b, c\}$ to $\{b, c^f\}$ does not change the C_p-module structure on N; thus it suffices to consider $f = 1$.

Fixing this module structure, Example 3.3.3 shows that there are at most two isomorphism types in this case, namely,

$$G_1 = \mathrm{Pc}\langle a, b, c \mid a^p, b^p, c^p, b^a = bc \rangle,$$

and

$$G_2 = \mathrm{Pc}\langle a, b, c \mid a^p = c, b^p, c^p, b^a = bc \rangle,$$

where G_1 splits over N. Observe that any element in G_1 can be written in normal form $a^u b^v c^w$ for some $u, v, w \in \mathbb{Z}_p$. By construction, we have $[b^v, a^u], c \in Z(G_1)$, thus for any $u, v, w \in \mathbb{Z}_p$ we have $(a^u b^v c^w)^p = (a^u b^v)^p c^{wp} = a^{up} b^{vp} [b^v, a^u]^{\frac{1}{2}p(p-1)} = 1$. This shows that $G_1 \cong p_+^{1+2}$ has exponent p. On the other hand, $G_2 \cong p_-^{1+2}$ has exponent p^2 as it is isomorphic to the semidirect product $C_p \ltimes C_{p^2}$ with presentation $\mathrm{Pc}\langle x, y \mid x^p, y^{p^2}, y^x = y^{p+1} \rangle$, via an isomorphism described by $\{a \mapsto y, b \mapsto x, c \mapsto y^p\}$. The claim follows. □

Before we move on to the groups of order p^4, we examine the presentations listed in Table 5.1 for isomorphism types of groups of order p^3 and summarise some results regarding the characteristic subgroups of these groups; see also [51] for an alternative discussion with more details. This information will be useful later.

TABLE 5.2: Proper nontrivial characteristic subgroups of groups of order p^3 using the relations of Table 5.1.

SOT ID	Nontrivial proper characteristic subgroups
$(p^3 : 1)$	$\langle a^p \rangle \cong C_{p^2}$, $\langle a^{p^2} \rangle \cong C_p$
$(p^3 : 2)$	$\langle a^p, b \rangle \cong C_p^2$, $\langle b \rangle \cong C_p$
$(p^3 : 3)$	–
$(p^3 : 4), p > 2$	$\langle c \rangle \cong C_p$
$(p^3 : 5), p > 2$	$\langle b, c \rangle \cong C_p^2$, $\langle c \rangle \cong C_p$
$(8 : 4)$	$\langle ab \rangle \cong C_4$, $\langle c \rangle \cong C_2$
$(8 : 5)$	$\langle a^2 \rangle \cong C_2$

5.1.3 An interlude: automorphism groups of extraspecial groups of order p^3

Both [46, Section 1.5.1] and [51, § 4] give detailed calculations regarding the automorphism groups of the groups of order p^3. We extract three results about the automorphism groups of extraspecial groups. Recall that the *Frattini subgroup* of a finite group G is the intersection of its maximal subgroups, denoted by $\Phi(G)$; if G is a p-group, then $\Phi(G) = [G, G]G^{[p]}$ (Theorem A.0.6), where $G^{[p]} = \langle \{g^p : g \in G\} \rangle$ is often called the *Agemo subgroup* of G, denoted by $\mho(G)$.

Proposition 5.1.9. *If p is an odd prime and $P \cong p_+^{1+2}$, then $\mathrm{Aut}(P/\Phi(P)) \cong \mathrm{GL}_2(p)$, and the natural projection $P \to P/\Phi(P)$ induces an epimorphism*

$$\pi \colon \mathrm{Aut}(P) \to \mathrm{Aut}(P/\Phi(P)),$$

where $\mathrm{Ker}\ \pi$ is a p-group. Moreover, $\mathrm{Aut}(P)$ is an extension of C_p^2 by $\mathrm{GL}_2(p)$, and so

$$|\mathrm{Aut}(P)| = p^3(p-1)^2(p+1).$$

Proof. The Frattini subgroup $\Phi(P)$ is characteristic in P, thus every $\alpha \in \mathrm{Aut}(P)$ induces automorphisms $\alpha|_{\Phi(P)} \in \mathrm{Aut}(\Phi(P))$ and $\alpha|_{P/\Phi(P)} \in \mathrm{Aut}(P/\Phi(P))$. For $\alpha \in \mathrm{Aut}(P)$ we abbreviate $\pi(\alpha) = \overline{\alpha}$ so that $\overline{\alpha}(g\Phi(P)) = \alpha(g)\Phi(P)$ for all $g \in P$. It follows from Theorem A.0.6 that $P/\Phi(P) \cong C_p^2$, and so $\mathrm{Aut}(P/\Phi(P)) \cong \mathrm{GL}_2(p)$. Thus, for any $\alpha, \beta \in \mathrm{Aut}(P)$ we have $\overline{\alpha}\overline{\beta}(g\Phi(P)) = \overline{\alpha\beta}(g\Phi(P))$ for all $g \in P$, showing π is a homomorphism. Consider

$$P = \langle a, b \mid a^p = b^p = [a,b]^p = 1 \rangle.^2$$

With respect to this presentation, we have that $\Phi(P) = \langle [a,b] \rangle$. Let $A = a\Phi(P)$ and $B = b\Phi(P)$. Then we can write $P/\Phi(P) = \mathrm{Pc}\langle A, B \mid A^p, B^p \rangle$. To see that π is surjective, it is sufficient to show that every $\theta \in \mathrm{Aut}(P/\Phi(P))$ lifts to an automorphism α of P such that $\pi(\alpha) = \theta$. Any $\theta \in \mathrm{Aut}(P/\Phi(P))$ acts on C_p^2 via an invertible matrix $\left(\begin{smallmatrix} x_1 & y_1 \\ x_2 & y_2 \end{smallmatrix}\right) \in \mathrm{GL}_2(p)$ with respect to the basis $\{A = (1\,0), B = (0\,1)\}$, where $x_1y_2 - x_2y_1 \not\equiv 0 \bmod p$; define $\alpha \colon P \to P$ via

$$\begin{cases} \alpha(a) & = a^{x_1}b^{y_1} \\ \alpha(b) & = a^{x_2}b^{y_2} \end{cases}.$$

We check by von Dyck's theorem (Theorem 3.1.1) that α is a homomorphism on P. Lastly, note that θ^{-1} lifts to the inverse of α, thus $\alpha \in \mathrm{Aut}(P)$ and π is surjective. To show that $\mathrm{Ker}\,\pi$ is a p-group, we show that automorphisms of order coprime to p are not in $\mathrm{Ker}\,\pi$. Let $\sigma \in \mathrm{Aut}(P)$ be an automorphism of prime order $q \neq p$. Suppose that $\overline{\sigma} = 1$. That is, σ acts on each coset $x\Phi(P)$ as a permutation of order 1 or q. It follows that σ leaves at least one element fixed in each base element of $P/\Phi(P)$, say $a_i \in a_i\Phi(P)$ is such an element for each i. By Burnside's basis theorem (Theorem A.0.6), the collection of these elements $\{a_1, \ldots, a_m\}$ forms a minimal generating set of P and it is fixed under σ. This forces that $\sigma = 1$, a contradiction. Hence, $\sigma \notin \mathrm{Ker}\,\pi$ and $\mathrm{Ker}\,\pi$ is a p-group. It remains to show that $\mathrm{Ker}\,\pi \cong C_p^2$, from which the claim follows. Let $S = \{\theta \colon \theta(a) = a[a,b]^s, \theta(b) = b[a,b]^t, \text{ where } s,t \in \mathbb{Z}_p\}$. It follows from Theorem 3.1.1 that for any $s,t \in \mathbb{Z}_p$ such a map θ extends to an automorphism of P. By abuse of notation, we write $\theta \in \mathrm{Aut}(P)$. Then a direct computation shows that $C_p^2 \cong S \leq \mathrm{Aut}(P)$. We now show that $\mathrm{Ker}\,\pi \subseteq S$: if $\alpha \in \mathrm{Ker}\,\pi$, then $\alpha(g)\Phi(P) = g\Phi(P)$ for all $g \in P$, which is equivalent to saying that $\alpha(g) = g[h,k]$ for some $[h,k] = [a,b]^r \in \Phi(P)$ and $r \in \mathbb{Z}_p$ (recall that $\Phi(P) \cong C_p$); in particular, this shows that $\alpha(a) = a[a,b]^s$ and $\alpha(b) = b[a,b]^t$ for some $s,t \in \mathbb{Z}_p$, and so $\alpha \in S$. Conversely, we show that $S \subseteq \mathrm{Ker}\,\pi$: let $\theta \in S$ with $\theta(a) = a[a,b]^s$ and $\theta(b) = b[a,b]^t$; since every element $g \in P$ can be expressed as $g = a^xb^y[a,b]^z$ for some $x,y,z \in \mathbb{Z}_p$, it follows that $g\Phi(P) = a^xb^y\Phi(P)$, but $\theta(g)\Phi(P) = a^xb^y[a,b]^{xs+yt+z}\Phi(P) = a^xb^y\Phi(P)$, thus $\theta \in \mathrm{Ker}\,\pi$. In conclusion, $\mathrm{Ker}\,\pi = S \cong C_p^2$ and $\mathrm{Aut}(P)$ is an extension of C_p^2 by $\mathrm{GL}_2(p)$. □

Proposition 5.1.10. *If p is an odd prime and $P \cong p_-^{1+2}$, then $\mathrm{Aut}(P) \cong C_{p-1} \ltimes p_+^{1+2}$.*

Proof. If $P = \mathrm{Pc}\langle a, b \mid a^p, b^{p^2}, b^a = b^{p+1} \rangle$, then each $\alpha \in \mathrm{Aut}(P)$ is defined by $\alpha(a) = a^ub^v$ and $\alpha(b) = a^xb^y$ for some $u,x \in \mathbb{Z}_p$ and $v,y \in \mathbb{Z}_{p^2}$. We have $b^ja^i = a^ib^{j(p+1)^i} = a^ib^{j(ip+1)}$ and $(a^ib^j)^n = a^{in}b^{jn+\frac{1}{2}ijpn(n-1)}$. For α to be an automorphism, it must preserve the order of a and b. Hence the values for u,v,x,y must satisfy that $(a^ub^v)^p = b^{vp} = 1$, and $(a^xb^y)^p = b^{yp} \neq 1$, forcing $y \in \mathbb{Z}_{p^2}^*$ and $v = mp$ for some $m \in \mathbb{Z}_p$. Moreover, for $\alpha(b^a) = \alpha(b)^{\alpha(a)}$ to hold true, or equivalently, $\alpha(b)\alpha(a) = \alpha(a)\alpha(b)^{1+p}$, it is required that $a^xb^ya^ub^v = a^ub^v(a^xb^y)^{1+p}$, which simplifies to $a^{x+u}b^{uyp+y+v} = a^{x+u}b^{v+yp+y}$, forcing $u = 1$. Conversely, any such triple of exponents $\{v,x,y\}$ defines an automorphism of P. That is, for any $v = mp \in \mathbb{Z}_p \backslash \mathbb{Z}_p^*$ and

[2] Note that P is isomorphic to $\mathrm{Pc}\langle a, b, c \mid a^p, b^p, c^p, b^a = bc \rangle$, as seen in Table 5.1, via an isomorphism α described by $\alpha(a) = a$, $\alpha(b) = b$, $\alpha([a,b]^{-1}) = c$.

$x \in \mathbb{Z}_p$ and $y \in \mathbb{Z}_{p^2}^*$, the map α defined by $\alpha(a) = ab^{mp}$ and $\alpha(b) = a^x b^y$ extends to an automorphism of P by Theorem 3.1.1. Since there are p options for v, x, and $p(p-1)$ options for y, we find $|\mathrm{Aut}(P)| = p^3(p-1)$. Theorem A.0.8 shows that the Sylow p-subgroup, denoted by N, is normal in $\mathrm{Aut}(P)$, and Theorem 2.4.1 shows that N has a complement of order $p-1$ in $\mathrm{Aut}(P)$. Thanks to the detailed calculation given in [46, Section 1.5.1] for an explicit formula of multiplication in $\mathrm{Aut}(P)$, we find that an automorphism of P has order p if and only if it is defined by the triple $(mp, x, 1+pr)$ for some $m, x, r \in \mathbb{Z}_p$ and m, x, r are not all zero. It follows these $p^3 - 1$ elements define precisely the nontrivial elements of N, and so N is nonabelian of exponent p. Thus, $N \cong p_+^{1+2}$ by Lemma 5.1.8. It remains to investigate the structure of the complement to N in $\mathrm{Aut}(P)$. If $r \in \mathbb{Z}_{p^2}^*$ has order $p-1$, then $\beta \in \mathrm{Aut}(P) \backslash N$ defined by the triple $(0, 0, r)$ has order $p-1$. Moreover, βN has order $(p-1)$ in $\mathrm{Aut}(P)/N$. It follows that $\mathrm{Aut}(P)/N \cong C_{p-1}$. □

5.2 Groups of odd order p^4

By Theorem A.0.12, there are five isomorphism types of abelian groups of order p^4, namely,

$$C_{p^4}, \quad C_p \times C_{p^3}, \quad C_{p^2}^2, \quad C_p^2 \times C_{p^2}, \quad C_p^4.$$

We are left with the nonabelian groups. To classify the nonabelian groups of order p^4 up to isomorphism, the following lemma from [1] shows that it suffices to classify the extensions of an abelian group of order p^3 by C_p; see also [15, pp. 140–144].

Lemma 5.2.1 ([1], Proposition 12)**.** *Every group of order p^4 has an abelian subgroup of order at least p^3.*

5.2.1 Summary of results

In this subsection, we consider odd primes p; we consider order 2^4 in the next subsection. The main approach used in this section is motivated by [1, 2, 15, 38, 46]; we collate some of the results in said sources and construct the groups using what we have established for p-groups and polycyclic extensions.

Theorem 5.2.2. *Let p be an odd prime. There are 15 isomorphism types of the groups of order p^4, five of which are abelian. Up to isomorphism, groups of odd order p^4 are the ones described in Table 5.3.*

5.2.2 Determination of groups of odd order p^4

To determine groups of odd order p^4, the following lemma of Burnside [15] asserts that it is sufficient to consider extensions of $C_{p^2} \times C_p$ and C_p^3 by C_p.

Lemma 5.2.3 ([15], § 109)**.** *Let p be an odd prime. If a nonabelian group G of order p^m contains a cyclic normal subgroup of order p^{m-1}, then it also contains a subgroup isomorphic to $C_{p^{m-2}} \times C_p$.*

By setting $m = 4$ in Lemma 5.2.3, we see that if G contains a cyclic normal subgroup of order p^3, then it also contains a normal subgroup isomorphic to $C_{p^2} \times C_p$. It remains to construct and

TABLE 5.3: Groups of odd order p^4, using Notation 4.1.1.

SOT ID	PC-relators	Structure	Centre	GAP ID
$(p^4:1)$	a^{p^4}	C_{p^4}	C_{p^4}	$(p^4, 1)$
$(p^4:2)$	a^{p^3}, b^p	$C_{p^3} \times C_p$	$C_{p^3} \times C_p$	$(p^4, 5)$
$(p^4:3)$	a^{p^2}, b^{p^2}	$C_{p^2}^2$	$C_{p^2}^2$	$(p^4, 2)$
$(p^4:4)$	a^{p^2}, b^p, c^p	$C_{p^2} \times C_p^2$	$C_{p^2} \times C_p^2$	$(p^4, 11)$
$(p^4:5)$	a^p, b^p, c^p, d^p	C_p^4	C_p^4	$(p^4, 15)$
$(p^4:6)$	$a^p, b^p, c^{p^2}, b^a/bc^p$	$C_p \ltimes (C_p \times C_{p^2})$	C_{p^2}	$(p^4, 14), (81, 14)$
$(p^4:7)$	$a^p/b, b^p, c^{p^2}, b^a/bc^p$	$C_p \ltimes C_{p^3}$	C_{p^2}	$(p^4, 6), (81, 6)$
$(p^4:8)$	$a^p, b^{p^2}, c^p, b^a/b^{1+p}$	$p_-^{1+2} \times C_p$	C_p^2	$(p^4, 13), (81, 13)$
$(p^4:9)$	$a^p, b^{p^2}, c^p, b^a/bc$	$C_p \ltimes (C_{p^2} \times C_p)$	C_p^2	$(p^4, 3), (81, 3)$
$(p^4:10)$	$a^p/c, b^{p^2}, c^p, b^a/b^{1+p}$	$C_{p^2} \ltimes C_{p^2}$	C_p^2	$(p^4, 4), (81, 4)$
$(p^4:11)$	$a^p, b^p, c^p, d^p, b^a/bc$	$p_+^{1+2} \times C_p$	C_p^2	$(p^4, 12), (81, 12)$
$(p^4:12)$	$a^p, b^{p^2}, c^p, b^a/bc, c^a/b^pc$	$C_p \ltimes (C_{p^2} \times C_p)$	C_p	$(p^4, 9), (81, 8)$
$(p^4:13)$	$a^p, b^{p^2}, c^p, b^a/bc, c^a/b^{rp}c$	$C_p \ltimes (C_{p^2} \times C_p)$	C_p	$(p^4, 10), (81, 9)$
$(p^4:14)$	$a^p, b^p, c^p, d^p, b^a/bc, c^a/cd$	$C_p \ltimes C_p^3$	C_p	$(p^4, 7), (81, 7)$
$(p^4:15)$, $p>3$	$a^p/d, b^p, c^p, d^p, b^a/bc, c^a/cd$	$C_p \ltimes (C_p \ltimes C_{p^2})$	C_p	$(p^4, 8)$
$(81:15)$	$a^3/d, b^3/d, c^3, d^3, b^a/bc, c^a/cd^2$	$C_3.3_+^{1+2}$	C_3	$(81, 10)$

classify the extensions of $C_{p^2} \times C_p$ and C_p^3 by C_p up to isomorphism. Before that, recall that a p-group G of order p^m is of maximal class if it has nilpotency class $m-1$; we now present a result on the groups of maximal class.

Lemma 5.2.4 ([3], Lemma 1.1, [38] Chapter 3)**.** *Let G be a nonabelian p-group that has an abelian subgroup of index p, then the upper and lower central series coincide and $|G| = p|G'||Z(G)|$, and the following are equivalent:*

(i) $|Z(G)| = p$,

(ii) $|G : G'| = p^2$,

(iii) *G is of maximal class.*

Proof. Since G is nonabelian, we can assume $|G| \geq p^3$. Berkovich [3, Lemma 1.1] showed that $|G| = p|G'||Z(G)|$. Leedham-Green and McKay [38, 52, Proposition 3.1.2] showed if G is of maximal class, then its upper and lower central series coincide and $G/G' \cong C_p^2$ and $Z(G) \cong C_p$. To show the equivalence of the statements, it is sufficient to show that (i) implies (ii) and (ii) implies (ii); this is left as an exercise in [3] and we include a sketch of the proof here for the sake of completeness.

(i) $\implies$ (ii): $|G : G'| = \frac{|G|}{|G'|} = p|Z(G)| = p^2$ since $|G| = p|G'||Z(G)|$.

(ii) $\implies$ (iii): Since $\frac{|G|}{p|G'|} = |Z(G)|$ by assumption, it follows that $|Z(G)| = p$. Since G is nilpotent, nontrivial normal subgroups intersect $Z(G)$ nontrivially ([45, Theorem 5.41]). This implies that $G' \cap Z(G) = Z(G)$; that is, $Z(G) \leq G'$. In particular, the third isomorphism theorem shows that $|G/Z(G) : G'/Z(G)| = p^2$. If $|G| = p^3$, then the claim follows trivially, which serves the base case for an induction to show that G is of maximal class: if $|G| = p^4$, then $G/Z(G)$ is of maximal class. Since $Z(G) \cong C_p$, by examining the upper central series, we see that G is also of maximal class. Inductively, this proves that G is of maximal class. □

We now prove Theorem 5.2.2 by a case distinction on the size of the centre of the group for the extensions of $C_{p^2} \times C_p$ and C_p^3 by C_p. Note that we often compute some invariant subgroups

in determining whether two groups are isomorphic. We now briefly recall that the *Omega subgroup* of a p-group G is the subgroup generated by $\{g \in G \colon g^p = 1\}$, denoted by $\Omega(G)$.

Proof of Theorem 5.2.2. Let G be a nonabelian group of order p^4, then G contains an abelian normal subgroup H of order p^3 by Lemma 5.2.1.

1. If $H \cong C_{p^2} \times C_p$ and $Z(G) = C_{p^2}$, then G has a pc-presentation of the form

$$G(t, e, f) = \mathrm{Pc}\langle a, b, c \mid a^p = t, b^p, c^{p^2}, b^a = b^e c^f \rangle,$$

where $t \in H = \langle b, c \rangle$, $e \in \mathbb{Z}_p$ and $f \in \mathbb{Z}_{p^2}$ cannot be both 0, and $Z(G) = \langle c \rangle$. We read $b^{(a^p)} = b^{(e^p)} c^{(f^p)} = b$ forces $e = 1$ and $f \equiv 0 \bmod p$. Note that $f \neq 0$ for otherwise $b \in Z(G)$, a contradiction. Thus $k \in \mathbb{Z}_p^*$. Since $t^a = t$ by Theorem 3.2.3 and $t \in H$, and H is abelian, it follows that $t \in Z(G) = \langle c \rangle$; that is, $t = c^k$ for some $k \in \mathbb{Z}_{p^2}^*$. Now, $G \cong (c^k, 1, xp)$ for some $k \in \mathbb{Z}_p$ and $x \in \mathbb{Z}_p^*$. However, we see that for any $x \in \mathbb{Z}_p^*$ the map $\{a \mapsto a^x, b \mapsto b, c \mapsto c\}$ extends to an isomorphism $G(c^{kx}, 1, xp) \to G(c^k, 1, p)$ by Theorem 3.1.1, thus it suffices to consider $x = 1$ and there is a unique isomorphism class of the split extension $C_p \ltimes H$ with cyclic centre of order p^2, isomorphic to

$$G(1, 1, p) = \mathrm{Pc}\langle a, b, c \mid a^p, b^p, c^{p^2}, b^a = bc^p \rangle \quad \text{(type } (p^4 : 6) \text{ in Table 5.3)}.$$

Moreover, observe that the map $\{a \mapsto a, b \mapsto b^k, c \mapsto c^k\}$ extends to an isomorphism $G(c, 1, p) \to G(c^k, 1, p)$ for all $k \in \mathbb{Z}_{p^2}^*$ and the map $\{a \mapsto abc^{p+1}, b \mapsto b, c \mapsto c\}$ extends to an isomorphism $G(c^{kp}, 1, p) \to G(1, 1, p)$ for all $k \in \mathbb{Z}_p^*$. This shows that $G(c^k, 1, p)$ is nonisomorphic to $G(1, 1, p)$ with SOT ID $(p^4 : 6)$ if and only if $k \in \mathbb{Z}_{p^2}^*$, and for any $k \in \mathbb{Z}_{p^2}^*$, such a group $G(c^k, 1, p)$ is isomorphic to

$$G(c, 1, p) = \mathrm{Pc}\langle a, b, c \mid a^p = c, b^p, c^{p^2}, b^a = bc^p \rangle \quad \text{(type } (p^4 : 7) \text{ in Table 5.3)},$$

which is equivalent to

$$\mathrm{Pc}\langle a, b, c, d \mid a^p = c, b^p, c^p = d, d^p, b^a = bd \rangle,$$

which allows us to see that such a group is isomorphic to

$$C_p \ltimes C_{p^3} = \mathrm{Pc}\langle x, y \mid x^p, y^{p^3}, y^x = x^{p^2+1} \rangle$$

via the isomorphism induced by $\{b \mapsto x, a \mapsto y, c \mapsto y^{p^2}, d \mapsto y^p\}$. Lastly, since the group with SOT ID $(p^4 : 6)$ contains no element of order p^3 while type $(p^4 : 7)$ does, they are not isomorphic.

2. Suppose that G contains a normal subgroup $H \cong C_{p^2} \times C_p$ and $Z(G) = C_p^2$. Then G has a presentation of the form

$$\mathrm{Pc}\langle a, b, c, d \mid a^p = t, b^p = c, c^p, d^p, b^a = b^{e_1} c^{e_2} d^{e_3} \rangle,$$

where $H = \langle b, c, d \rangle$, $t \in H$, $Z(G) = \langle c, d \rangle$, and $e_1, e_2, e_3 \in \mathbb{Z}_p$ are not all zero. Since $t^a = t$, and H is abelian, it follows that $t \in Z(G)$. Since

$$b^t = b^{(e_1^p)} c^{e_2(1+e_1+\cdots e_1^{p-1})} d^{e_3(1+e_1+\cdots e_1^{p-1})} = b,$$

it is required that $e_2 \sum_{i=0}^{p-1} e_1^i \equiv e_3 \sum_{i=0}^{p-1} e_1^i \equiv 0 \bmod p$ and $e_1^p \equiv 1 \bmod p$. Hence, $e_1 = 1$, and so e_2, e_3 cannot be both zero, for otherwise $b^a = b$ and G is abelian, a contradiction. Now we consider G of the form

$$G(t, e_2, e_3) = \mathrm{Pc}\langle a, b, c, d \mid a^p = t, b^p = c, c^p, d^p, b^a = bc^{e_2}d^{e_3}\rangle.$$

First note that the map $\{a \mapsto a, b \mapsto b, c \mapsto c, d \mapsto c^x d^x\}$ extends to an isomorphism $G(t, 0, 1) \to G(t, x, x)$, it suffices to consider $e_2 \neq e_3$. Observe that $\{a \mapsto a^k\}$[3] extends to an isomorphism $G(t, k, e_3) \to G(t, 1, k^{-1}e_3)$ for any $k \in \mathbb{Z}_p^*$, and $\{d \mapsto d^m\}$ extends to an isomorphism $G(t, e_2, 1) \to (t, e_2, m)$ for any $m \in \mathbb{Z}_p^*$. This shows that it is sufficient to consider $e_2, e_3 \in \{0, 1\}$, and so G is isomorphic to $G(t, 1, 0)$ or $G(t, 0, 1)$. Moreover, since $\{a \mapsto a^k\}$ extends to an automorphism of $C_p \cong G/H$ and $\{d \mapsto c^m d^n\}$ extends to an automorphism of H for any $k, m, n \in \mathbb{Z}_p^*$, Theorem 2.3.5 verifies that it is sufficient to consider $t \in \{1, c, d\}$.

If $t = 1$, then G is a split extension and G is isomorphic to one of the following:

$$G(1, 1, 0) = \mathrm{Pc}\langle a, b, c, d \mid a^p, b^p = c, c^p, d^p, b^a = bc\rangle \quad \text{(type } (p^4 : 8) \text{ in Table 5.3)},$$

$$G(1, 0, 1) = \mathrm{Pc}\langle a, b, c, d \mid a^p, b^p = c, c^p, d^p, b^a = bd\rangle \quad \text{(type } (p^4 : 9) \text{ in Table 5.3)}.$$

If $t = c$, then G is isomorphic to

$$G(c, 1, 0) = \mathrm{Pc}\langle a, b, c, d \mid a^p = c, b^p = c, c^p, d^p, b^a = bc\rangle,$$

or

$$G(c, 0, 1) = \mathrm{Pc}\langle a, b, c, d \mid a^p = c, b^p = c, c^p, d^p, b^a = bd\rangle.$$

Since $G/Z(G)$ is abelian, we know $[G, G] \leq Z(G)$ and Lemma 5.1.5 applies. In particular, we have $(ab^{-1})^p = a^p b^{-p} [b^{-1}, a]^{\frac{1}{2}p(p-1)} = 1$. Using this, we see that the map $\{a \mapsto ab^{-1}\}$ extends to isomorphisms $G(c, 1, 0) \to G(1, 1, 0)$ and $G(c, 0, 1) \to G(1, 0, 1)$. If $t = d$, then G is isomorphic to

$$\mathrm{Pc}\langle a, b, c, d \mid a^p = d, b^p = c, c^p, d^p, b^a = bc\rangle,$$

or

$$\mathrm{Pc}\langle a, b, c, d \mid a^p = d, b^p = c, c^p, d^p, b^a = bd\rangle.$$

However, both of them are isomorphic to

$$\mathrm{Pc}\langle a, b, c \mid a^p = c, b^{p^2}, c^p, b^a = b^{p+1}\rangle \quad \text{(type } (p^4 : 10) \text{ in Table 5.3)},$$

via isomorphisms described by

$$\{a \mapsto a, b \mapsto b, c \mapsto b^p, d \mapsto c\}$$

and

$$\{a \mapsto b, b \mapsto a^{-1}, c \mapsto c^{-1}, d \mapsto b^p\},$$

respectively. It remains to show that groups with SOT ID $(p^4 : 8)$, $(p^4 : 9)$, and $(p^4 : 10)$ are nonisomorphic. Note that every element in each of those groups can be written in its normal form, thus we compute the Agemo subgroup $\langle \{(a^x b^y c^u d^v)^p : x, y, u, v \in \mathbb{Z}_p\}\rangle$. In particular, we see that the Agemo subgroups of types $(p^4 : 8)$, $(p^4 : 9)$, and $(p^4 : 10)$ are $\langle c\rangle$, $\langle c\rangle$, and $\langle c, d\rangle$ respectively. This shows that type $(p^4 : 10)$ is not isomorphic to either of the others. On the other hand, we can also find that the derived subgroup of type

[3] Recall that we sometimes abbreviate the map on generators by omitting the fixed points.

$(p^4 : 8)$ coincides with its Agemo subgroup, whereas the derived subgroup of $(p^4 : 9)$ is $\langle d \rangle \not\leq \langle c \rangle$, from which we conclude that the groups with SOT ID $(p^4 : 8)$ and $(p^4 : 9)$ are nonisomorphic.

3. Suppose that G contains a normal subgroup $H \cong C_p^3$ and $Z(G) = C_p^2$. Then G has a pc-presentation of the form

$$\mathrm{Pc}\langle a, b, c, d \mid a^p = t, b^p, c^p, d^p, b^a = b^{e_1} c^{e_2} d^{e_3} \rangle,$$

where $t \in H = \langle b, c, d \rangle$ and $Z(G) = \langle c, d \rangle$. Since H is abelian and $t^a = t$, it follows that $t \in Z(G)$, namely, $t = c^e d^f$ for some $e, f \in \mathbb{Z}_p$. Theorem 3.2.3 shows that $e_1 = 1$ and e_2, e_3 are not both zero. Moreover, since $\{c \mapsto cd^k\}$ extends to an automorphism of H, we can consider $e_3 = 0$ without loss of generality. Thus, we know that G is isomorphic to

$$G(e, f, e_2) = \mathrm{Pc}\langle a, b, c, d \mid a^p = c^e d^f, b^p, c^p, d^p, b^a = bc^{e_2} \rangle,$$

for some $e_2 \in \mathbb{Z}_p^*$ and $e, f \in \mathbb{Z}_p$. Observe that the map $\{a \mapsto a^k\}$ extends to an isomorphism $G(ek, fk, k) \to G(e, f, 1)$ for any $k \in \mathbb{Z}_p^*$, thus it suffices to consider $e_2 = 1$ and there is a unique isomorphism class of split extensions $C_p \ltimes H$ isomorphic to $G(0, 0, 1)$, with a nontrivial C_p-action on $H = \langle b, c, d \rangle$ represented by $\langle \left(\begin{smallmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{smallmatrix}\right) \rangle$ with respect to the basis $\{b = (1\,0\,0), c = (0\,1\,0), d = (0\,0\,1)\}$. Thus there is a unique C_p-module structure on H up to equivalence, and it remains to consider nonsplit extensions $G(e, f, 1)$ with $c^e d^f \neq 1$. A similar computation as before shows that $G(e, 0, 1)$ has SOT ID $(p^4 : 8)$ for $e > 0$, and $G(0, f, 1)$ has SOT ID $(p^4 : 9)$ for $f > 0$; if $e \neq 0, f \neq 0$ then $G(e, f, 1)$ has SOT ID $(p^4 : 10)$. So we conclude that the extensions of this kind only add one new isomorphism class, which has a representative given by

$$\mathrm{Pc}\langle a, b, c, d \mid a^p, b^p, c^p, d^p, b^a = bc \rangle \quad \text{(type } (p^4 : 11) \text{ in Table 5.3)}.$$

4. Suppose that $Z(G) = C_p$. By Lemma 5.2.4, we know that G is of maximal class, and $|G'| = p^2$. Furthermore, Lemma 5.2.4 shows that $G/Z(G)$ is also of maximal class. In conjunction with [38, Theorem 3.3.2], which shows that both G' and $G/Z(G)$ have exponent p, implying $G/Z(G) \cong p_+^{1+2}$ and $G' \cong C_p^2$, we deduce that G has a presentation with pcgs $\{a, b, c, d\}$ whose upper central series has the following terms: $\zeta_1(G) = Z(G) = \langle d \rangle \cong C_p$, $\zeta_2(G) = \langle c, d \rangle = G' \cong C_p^2$, $\zeta_3(G) = G$. Moreover, $\langle a, b, c \rangle \cong p_+^{1+2}$. That is, any such maximal class group G of order p^4 is a central extension of C_p by p_+^{1+2} and has a presentation of the form

$$\mathrm{Pc}\langle a, b, c, d \mid a^p = t_1, b^p = t_2, c^p, d^p, b^a = bct_3, c^a = ct_4 \rangle,$$

where each $t_i \in \langle d \rangle = Z(G)$. Observe that $t_1, \ldots, t_4$ cannot all be zero, since otherwise the presentation defines a group with SOT ID $(p^4 : 11)$, which is already accounted for. Since $\{c \mapsto cd^k\}$ extends to an automorphism of $\langle c, d \rangle$ for all $k \in \mathbb{Z}_p$, we can fix $t_3 = 1$ without loss of generality. Now observe that if $t_4 = 1$, then for any choice of t_1 and t_2, the subgroup $\langle c, d \rangle$ lies in the centre, a contradiction. Hence, it suffices to consider the G of the form

$$G(x, y, z) = \mathrm{Pc}\langle a, b, c, d \mid a^p = d^x, b^p = d^y, c^p, d^p, b^a = bc, c^a = cd^z \rangle,$$

where $x, y \in \mathbb{Z}_p, z \in \mathbb{Z}_p^*$.

   (a) If $x = 0$, then independent of the choices of y, z, the extension G splits over a normal subgroup of order p^3: if $y = 0$, then $G \cong C_p \ltimes C_p^3$; if $y \neq 0$, then $G \cong C_p \ltimes (C_{p^2} \times C_p)$.

i. If $y = 0$ and $G \cong C_p \ltimes C_p^3$ with said setting, then the C_p-action on $H = \langle b, c, d \rangle$ can be represented by a matrix $a \mapsto \left(\begin{smallmatrix} 1 & 1 & 0 \\ 0 & 1 & z \\ 0 & 0 & 1 \end{smallmatrix}\right)$ acting on C_p^3 with respect to the basis $\{b = (1\,0\,0), c = (0\,1\,0), d = (0\,0\,1)\}$ for some $z \in \mathbb{Z}_p^*$. Since $\{b, c, d^z\}$ also forms a basis, any matrix of this form is conjugate to $\left(\begin{smallmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{smallmatrix}\right)$. By Corollary 2.4.2, this case adds a unique isomorphism class with representative $G(0, 0, 1)$

$$\mathrm{Pc}\langle a, b, c, d \mid a^p, b^p, c^p, d^p, b^a = bc, c^a = cd \rangle \quad \text{(type } (p^4 : 14) \text{ in Table 5.3).}$$

ii. If $y \in \mathbb{Z}_p^*$, then for any $z \in \mathbb{Z}_p^*$ map $\{d^y \mapsto d\}$ extends to an isomorphism $G(0, y, z) \to G(0, 1, y^{-1}z)$. Hence it is sufficient to fix $y = 1$, and it remains to investigate the pc-presentations corresponding to the $p - 1$ choices of z. Observe that for any $s \in \mathbb{Z}_p^*$, the map $\{a \mapsto a^s, c \mapsto c^s d^{\frac{1}{2}s(s-1)}\}$ extends to an isomorphism between $G(0, 1, z)$ and $G(0, 1, s^2 z)$. This shows that if z is a quadratic residue modulo p, then $G(0, 1, z)$ is isomorphic to

$$\mathrm{Pc}\langle a, b, c, d \mid a^p, b^p = d, c^p, d^p, b^a = bc, c^a = cd \rangle \quad \text{(type } (p^4 : 12) \text{ in Table 5.3);}$$

otherwise, $G(0, 1, z)$ is isomorphic to

$$\mathrm{Pc}\langle a, b, c, d \mid a^p, b^p = d, c^p, d^p, b^a = bc, c^a = cd^r \rangle \quad \text{(type } (p^4 : 13) \text{ in Table 5.3),}$$

where $r = \sigma_p$ (Notation 4.1.1), as $\{s^2 r \colon s \in \mathbb{Z}_p^*\}$ generates the complete set of the quadratic non-residues.

We are left to verify that types $(p^4 : 12)$, $(p^4 : 13)$, and $(p^4 : 14)$ are pairwise nonisomorphic. Since type $(p^4 : 14)$ has exponent p whereas the others have exponent p^2, it remains to show that types $(p^4 : 12)$ and $(p^4 : 13)$ are not isomorphic. Let G_1 have SOT ID $(p^4 : 12)$ and G_2 have SOT ID $(p^4 : 13)$, and both are defined by the presentations above. Suppose for contradiction that $\alpha \colon G_1 \to G_2$ is an isomorphism. Since derived subgroups are characteristic, $\alpha(\langle c, d \rangle) = \langle c, d \rangle = [G_2, G_2]$. Since b commutes with both c and d, it follows that $b \in \alpha(\langle b, c, d \rangle)$, thus $\alpha(\langle b, c, d \rangle) = \langle b, c, d \rangle$. Let $N = \langle a, b, c \rangle \lhd G_1$, this shows that $\alpha|_N \in \mathrm{Aut}(N)$, and $\alpha|_{\langle a \rangle} \in \mathrm{Aut}(\langle a \rangle)$. In particular, it shows that it suffices to consider $\alpha(a) = a^k$ for some $k \in \mathbb{Z}_p^*$, and $\alpha(b) = b^\ell c^m d^n$ where $\ell \in \mathbb{Z}_p^*, m, n \in \mathbb{Z}_p$. Since α is a homomorphism, we read that $\alpha([[b, a], a]) = [[b^\ell c^m d^n, a^k], a^k]$. However, the left-hand side equals $\alpha(d^r) = \alpha(b^{rp}) = b^{\ell rp} = d^{\ell r}$, while the right-hand side is $d^{(k^2)} = b^{(\ell k^2)}$. Since r is a quadratic non-residue, there exists no $k \in \mathbb{Z}_p^*$ such that $k^2 = r$, thus there exists no such an isomorphism α, that is, $G_1 \ncong G_2$.

(b) If $x > 0$, the the map $\{a \mapsto a^x, c \mapsto c^x, d \mapsto d^{(x^2)}\}$ extends to an isomorphism $G(1, y, z) \to G(x, y, z)$ for all $x \in \mathbb{Z}_p^*$, thus we can fix $x = 1$. A similar calculation with case distinction on $y = 0$ and $y > 0$ as seen in the preceding discussion shows that there are at most three new isomorphism types arising from such extensions, namely, $G(1, 0, 1)$, $G(1, 1, 1)$, and $G(1, 1, \sigma_p)$. However, considering each of these cases, we find that $G(1, 0, 1)$ has SOT ID $(81 : 14)$ if $p = 3$, and $G(1, 1, 1)$ has SOT ID $(p^4 : 12)$ for all $p > 2$, and $G(1, 1, \sigma_p)$ has SOT ID $(p^4 : 13)$ for all $p > 3$. Thus, in total these extensions adds at most one new isomorphism type, depending on whether $G(1, 0, 1)$ adds a new isomorphism type when $p > 3$ and whether $G(1, 1, \sigma_p)$ adds a new isomorphism type when $p = 3$. Now consider these two cases: for $p > 3$, the

group $G(1,0,1)$ is isomorphic to

$$\mathrm{Pc}\langle a,b,c,d \mid a^p = d, b^p, c^p, d^p, b^a = bc, c^a = cd\rangle \text{ (type } (p^4:15) \text{ in Table 5.3);}$$

for $p = 3$, the group $G(1,1,\sigma_p)$ is isomorphic to

$$\mathrm{Pc}\langle a,b,c,d \mid a^3 = b^3 = d, c^3, d^3, b^a = bc, c^a = cd^2\rangle \text{ (type } (81:15) \text{ in Table 5.3).}$$

In the former case, we calculate the Omega subgroup of the group in $G(1,0,1)$ to be

$$\{a^x b^y c^u d^v \colon (a^x b^y c^u d^v)^p = a^{xp} = d^x = 1, x, y, u, v \in \mathbb{Z}_p\} = \langle b, c, d\rangle,$$

which is abelian of order p^3 with $p > 3$, while type $(p^4:12)$ and $(p^4:13)$ both have nonabelian Omega subgroups (both have the form $\langle a,c,d\rangle \cong p_+^{1+2}$), and the Omega subgroup of type $(p^4:14)$ has order p^4 since it is of exponent p. Hence, if $p > 3$, then type $(p^4:15)$ is nonisomorphic to any of the other three.
For $p = 3$, the group $G(1,1,\sigma_p)$ is of exponent p^2, and so it is nonisomorphic to type $(3^4:14)$) and its Omega subgroup is isomorphic to C_3^2 (hence nonisomorphic to either of type $(3^4:12)$ or $(3^4:13)$. □

Remark 5.2.5. When $p > 3$, the groups $\mathrm{Pc}\langle a,b,c,d \mid a^p, b^p = d, c^p, b^a = bc, c^a = cd^r\rangle$ and $\mathrm{Pc}\langle a,b,c,d \mid a^p = d, b^p = d, c^p, b^a = bc, c^a = cd^r\rangle$ are isomorphic via the isomorphism induced by $\{a \mapsto abc\}$. When $p = 3$, the groups $\mathrm{Pc}\langle a,b,c,d \mid a^p, b^p, c^p, d^p, c^a = bc, d^a = cd\rangle$ and $\mathrm{Pc}\langle a,b,c,d \mid a^p = d, b^p, c^p, d^p, b^a = bc, c^a = cd\rangle$ are isomorphic via the isomorphism induced by $\{a \mapsto abcd\}$.

5.3 Groups of order sixteen

In this section, we comment on the special case of nonabelian groups of order 16.

TABLE 5.4: Nonabelian groups of order 16.

SOT ID	PC-relators	Structure	Centre	GAP ID
$(2^4:6)$	$a^2, b^4, c^2, b^a/b^3, c^a/b^2c$	$C_2 \ltimes (C_4 \times C_2)$	C_4	(16, 13)
$(2^4:7)$	$a^2, b^4, c^2, b^a/b^3$	$(C_2 \ltimes C_4) \times C_2$	$C_2 \times C_2$	(16, 11)
$(2^4:8)$	$a^2, b^4, c^2, b^a/bc$	$C_2 \ltimes (C_4 \times C_2)$	$C_2 \times C_2$	(16, 3)
$(2^4:9)$	$a^2/b^2, b^4, c^2, b^a/b^3$	$Q_8 \times C_2$	$C_2 \times C_2$	(16, 12)
$(2^4:10)$	$a^2/b^2, b^4, c^2, b^a/bc$	$C_4 \ltimes C_4$	$C_2 \times C_2$	(16, 4)
$(2^4:11)$	$a^2, b^8, b^a/b^5$	$C_2 \ltimes C_8$	C_4	(16, 6)
$(2^4:12)$	$a^2, b^8, b^a/b^3$	QD_{16}	C_2	(16, 8)
$(2^4:13)$	$a^2, b^8, b^a/b^7$	D_8	C_2	(16, 7)
$(2^4:14)$	$a^2/b^4, b^8, b^a/b^7$	Q_{16}	C_2	(16, 9)

Theorem 5.3.1. *There are 14 isomorphism types of the groups of order* 16*, five of which are abelian. A group of order* 16 *has a pc-presentation as encoded Table 5.4.*

We omit the details but provide only a sketch of the proof here. All fourteen groups can be constructed by cyclic extensions of the known groups of order 2^3 (see Table 5.1). However, the list can be reduced beforehand. Most of the results in the previous section still apply except for Lemma 5.2.3. Similar to the general case of p^4, we only need to consider abelian normal subgroups of order 2^3 in constructing the groups of order 2^4. The main difference lies in which

abelian normal subgroup we use, since Lemma 5.2.3 only applies to odd primes p. In particular, we know that any nonabelian group of order 16 contains a cyclic subgroup of order 4, thus we further deduce that the nonabelian extensions of C_2^3 by C_2 always contain a normal subgroup isomorphic to $C_4 \times C_2$. The discussion of such extensions for general primes p in the previous section still applies here, except that there are no extensions analogous to the types in Table 5.3 involving σ_p, since $\sigma_2 = 1$ is also a quadratic residue. For this reason, there are only three maximal class groups of order 16 up to isomorphism. All the nonabelian groups of order 16 containing no elements of order 8 can be constructed as extensions of $C_4 \times C_2$ by C_2. For the groups containing elements of order 8, it suffices to consider the extensions of C_8 by C_2. Since the group order is small, the construction and identification are trivial by exhaustion and we obtain the results in Table 5.4.

Chapter 6

Groups of order $p^a q^b$

Let p, q be distinct primes. In this chapter, we determine the isomorphism types of groups of order $p^a q^b$, where $1 \leq a, b$ and $a + b \leq 4$. Since the abelian groups are classified by the fundamental theorem of finitely generated abelian groups, we only discuss the proofs for the nonabelian ones. The determination of groups of order pq, p^2q, p^3q exists in the literature, for example, see [18], [32] and [51]. The enumeration is known for groups of order p^2q^2 (see [37] and [25]). Amongst the known results, some of the existing constructions are not efficient in practice. Our goal is to independingly describe explicit constructions for these groups using the results discussed in Chapter 2 to present an accessible proof and to derive an efficient algorithm for the construction and identification for these groups. As a direct result of our constructions, we obtain a counting formula for each order type. Our enumeration for groups of order p^2q^2 agrees with [37, Chapter V, § 1] and [24]; our enumeration for groups of order p^2q agrees with [32, § 21 - § 37] and [15, § 59]; our enumeration for groups of order p^3q agrees with [24] and [37].

In the rest of the chapter, let G be a group and let $P \in \mathrm{Syl}_p(G)$ and $Q \in \mathrm{Syl}_q(G)$ denote Sylow subgroups of G. Recall that we write $n_p(G) = |\mathrm{Syl}_p(G)|$ for each prime divisor p of $|G|$. Note that in the construction of non-nilpotent groups of order $p^a q^b$ with a normal Sylow subgroup, we make canonical choices as described in Notations 4.1.1, 4.2.1, and 4.2.6, which imposes a canonical order on the list of isomorphism representatives. This canonical ordering is crucial to the development of an identification function, which we exemplify in Chapter 8. In each table, we list the isomorphism types using said notation and include the enumeration result in the rightmost column; we highlight that if the expression in the column of "number of types" evaluates to 0 for a given order, then it means that the isomorphism type in the corresponding row does not exist. Recall again that Δ_u^v is the Kronecker delta function for divisibility of u by v.

6.1 Groups of order pq and p^2q

Recall that Theorem A.0.9 characterises finite nilpotent groups Corollary 3.2.5 gives a presentation for each nilpotent groups. Therefore, in the rest of the thesis we omit proofs of the determination of nilpotent groups.

TABLE 6.1: Groups of order pq and p^2q, using Notations 4.1.1, 4.2.1, and 4.2.6.

Order type	Pc-relators	Parameters	Number of types
$pq, p > q$	**Cluster 1**: abelian		
	a^{pq}		1
	Cluster 2: nonabelian		
	$a^p, b^p, b^a / b^{\rho(p,q)}$		Δ^q_{p-1}
p^2q	**Cluster 1**: nilpotent		
	a^{p^2q}		1
	a^{pq}, b^p		1
	Cluster 2: non-nilpotent, with $C_p^2 \cong P \trianglelefteq G$		
	$a^q, b^p, c^p, b^a / b^{\rho(p,q)}$		Δ^q_{p-1}
	$a^q, b^p, c^p, (b^a, c^a)/(b,c)^{M(p,q,\sigma_q^k)}$	$0 \le k \le \frac{1}{2}(q-1)$	$\frac{1}{2}(q+1-\Delta_q^2)\Delta^q_{p-1}$
	$a^q, b^p, c^p, (b^a, c^a)/(b,c)^{\mathrm{Irr}_2(p,q)}$		$(1-\Delta_q^2)\Delta^q_{p+1}$
	Cluster 3: non-nilpotent, with $C_{p^2} \cong P \trianglelefteq G$		
	$a^q, b^{p^2}, b^a / b^{\rho(p^2,q)}$		Δ^q_{p-1}
	Cluster 4: non-nilpotent, with $Q \trianglelefteq G$ and $P \cong C_p^2$		
	$a^p, b^p, c^q, c^a / c^{\rho(q,p)}$		Δ^p_{q-1}
	Cluster 5: non-nilpotent, with $Q \trianglelefteq G$ and $P \cong C_{p^2}$		
	$a^{p^2}, b^q, b^a / b^{\rho(q,p)}$		Δ^p_{q-1}
	$a^{p^2}, b^q, b^a / b^{\rho(q,p^2)}$		$\Delta^{p^2}_{q-1}$

Theorem 6.1.1. *Let p and q be distinct primes. Every group of order pq or p^2q has a normal Sylow subgroup. If $p > q$, then there are $1 + \Delta^q_{p-1}$ isomorphism types of groups of order pq. There are five isomorphism types of groups of $2p^2$ with $p > 2$; there are exactly*

$$2 + \Delta^q_{p+1} + \frac{1}{2}(q+5)\Delta^q_{p-1} + 2\Delta^p_{q-1} + \Delta^{p^2}_{q-1}$$

nonisomorphic groups of order p^2q with $q > 2$. A group of order pq or p^2q has a presentation as encoded Table 6.1 using notation defined in Notations 4.1.1, 4.2.1, and 4.2.6.

The following lemmas prove Theorem 6.1.1.

Lemma 6.1.2. *If G is a group of order p^nq with n a positive integer and $p > q$, then $P \lhd G$ and $G \cong C_q \ltimes P$.*

Proof. The order of P is p^n and $[G\colon P] = q$. Since $p > q$, the number of Sylow p-subgroups in G is 1 by Sylow theorems (see Theorem A.0.8), thus P is normal in G. On the other hand, since q is coprime to p, it follows from Theorem 2.4.1 that Q is a complement of P. Since Sylow q-subgroups of G have order q, this shows that $G = Q \ltimes P \cong C_q \ltimes P$. □

Applying Lemma 6.1.2 to the case where $n = 1$, we determine all groups of order pq.

Lemma 6.1.3. *Let $p > q$ be primes. Then there are $1 + \Delta^q_{p-1}$ isomorphism types of groups of order pq. In particular, a group G of order pq is abelian if and only if $G \cong C_{pq}$, and G is nonabelian if and only if $G \cong C_q \ltimes_\varphi C_p$ where with a faithful action φ.*

Proof. Let G be a group of order pq. By Theorem A.0.12, G is abelian if and only if $G \cong C_{pq}$. Lemma 6.1.2 shows that a nonabelian group G of such order is isomorphic to a split extension

$C_q \ltimes_\varphi C_p$, where $\varphi\colon C_q \to \mathrm{Aut}(C_p) \cong C_{p-1}$ is nontrivial. Since q is prime, such a nontrivial action must be faithful and exists only if $q \mid (p-1)$. Further, Corollary 2.4.3(ii) asserts that the isomorphism classes of such nontrivial split extension are in bijection with conjugacy classes of subgroups of order q in $\mathrm{Aut}(P) \cong \mathbb{Z}_p^*$. It follows immediately that there is a unique isomorphism type of nonabelian group $G \cong C_q \ltimes C_p$. In particular, as demonstrated in Example 4.0.1, such a nonabelian G is isomorphic to

$$\mathrm{Pc}\langle a, b \mid a^q, b^p, b^a = b^{\rho(p,q)}\rangle,$$

where $\rho(p,q)$ as defined in Notation 4.1.1. □

Let G be a group of order p^2q. If G is abelian, then G is isomorphic to C_{p^2q} or $C_{pq} \times C_p$ by Theorem A.0.12. Hence, it remains to consider the cases where G is nonabelian. We first show that G has a normal Sylow subgroup.

Lemma 6.1.4. *If G is a nonabelian group of order p^2q, then G contains a normal Sylow subgroup.*

Proof. Suppose for contradiction that G has no normal Sylow subgroup. By Theorem A.0.8, we deduce that $|\mathrm{Syl}_p(G)| = q$ and $q \equiv 1 \bmod p$. In particular, this implies that $q > p$. On the other hand, if $|\mathrm{Syl}_q(G)| = p^2$, then there are $p^2(q-1)$ elements of order q in G, leaving at most p^2 elements of order coprime to q, which implies that the Sylow p-subgroup is normal in G, a contradiction. It follows that $|\mathrm{Syl}_q(G)| = p$. However, this implies that $p > q$, a contradiction. Therefore G has a normal Sylow subgroup. □

We now apply Theorem 2.4.1 and Lemma 6.1.4 and see that a nonabelian group of order p^2q is isomorphic to $C_q \ltimes P$ or $P \ltimes C_q$, where $P \in \{C_{p^2}, C_p^2\}$. We look into these cases separately in the following lemmas.

Lemma 6.1.5. *A nonabelian group of order p^2q with a normal cyclic Sylow p-subgroup is unique up to isomorphism and exists if and only if $q \mid (p-1)$.*

Proof. By Theorem 2.4.1 such groups are isomorphic to $Q \ltimes P$, where $P \cong C_{p^2}$ and $Q \cong C_q$. On the other hand, a split extension $Q \ltimes P$ is nonabelian if and only Q acts faithfully on P. Since $\mathrm{Aut}(P) \cong \mathbb{Z}_{p^2}^*$, this requires that $q \mid (p-1)$. Uniqueness follows from Corollary 2.4.3. In particular, such groups are isomorphic to $\mathrm{Pc}\langle a, b \mid a^q, b^{p^2}, b^a = b^{\rho(p^2,q)}\rangle$, where $\rho(p^2,q) \in \mathrm{Aut}(P)$ is the canonical automorphism of order q in $\mathrm{Aut}(C_{p^2})$ as described in Notation 4.1.1. □

Lemma 6.1.6. *There are $\frac{1}{2}(q+3)\Delta_{p-1}^q + \Delta_{p+1}^p$ isomorphism types of the groups of order p^2q with a normal elementary abelian Sylow p-subgroup if $q > 2$, and two isomorphism types if $q = 2$. Each of them has a presentation as encoded in Table 6.1.*

Proof. The enumeration of such groups up to isomorphism follows from Corollary 2.4.3 and Theorem 4.2.7(i). To find an explicit construction of such groups, we note that if $Q = \langle a \rangle \cong C_q$ and $P = \langle b, c \rangle$, then any Q-module structure of P via $\varphi\colon G \to \mathrm{Aut}(P)$ can be described by the induced image of the generator a in $\mathrm{GL}_2(p)$, namely,

$$\varphi\colon Q \to \mathrm{GL}_2(p),\ a \mapsto \begin{pmatrix} i & j \\ e & f \end{pmatrix},$$

corresponding to

$$a \mapsto \begin{cases} b \mapsto & b^i c^e \\ c \mapsto & b^j c^f \end{cases},$$

for some $i, j, e, f \in \mathbb{Z}_p$ such that $fi - ej \not\equiv 0 \bmod p$. This in turn defines a pc-presentation of $G = Q \ltimes P$, namely,

$$\mathrm{Pc}\langle a, b, c \mid a^q, b^p, c^p, b^a = b^i c^e, c^a = b^j c^f \rangle.$$

In conjunction with canonical choices of automorphisms given in Chapter 4, we follow the proof of Theorem 4.2.7(i) to construct the (ordered) list of isomorphism types of nonabelian extensions $G \cong C_q \ltimes C_p^2$ as follows.

1. If $q > 2$ and $q \mid (p+1)$, then subgroups of order q are irreducible and lie in a single conjugacy class in $\mathrm{GL}_2(p)$. Thus, there is a unique isomorphism type of nonabelian split extensions $G = Q \ltimes_\varphi P$, with isomorphism class reprsentative

   $$\mathrm{Pc}\langle a, b, c \mid a^q, b^p, c^p, b^a = c, c^a = b^{-1}c^{i+i^p} \rangle,$$

   where $\varphi(a) = \mathrm{Irr}_2(p, q)$ (recall Notation 4.2.6).

2. If $q \mid (p-1)$, then C_q is diagonalisable in $\mathrm{GL}_2(p)$, implying that it acts diagonalisably on C_p^2. It follows from Theorem 4.2.7(i) and Corollary 2.4.3(ii) that there are $\frac{1}{2}(q + 3 - \Delta_q^2)$ isomorphism types of $G \cong C_q \ltimes C_p^2$, in one-to-one correspondence with the conjugacy classes of subgroups of order q in $\mathrm{GL}_2(p)$. In particular, if $Z(G) \cong C_p$, then G is isomorphic to

   $$\mathrm{Pc}\langle a, b, c \mid a^q, b^p, c^p, b^a = b^{\rho(p,q)} \rangle;$$

   if $Z(G) = 1$, then the isomorphism class representatives for such groups are parameterised by

   $$\mathrm{Pc}\langle a, b, c \mid a^q, b^p, c^p, (b, c)^a = (b, c)^{M(p,q,\sigma_q^k)} \rangle,$$

   where $0 \leq k \leq \frac{1}{2}(q-1)$ using notation explained in Notation 4.2.1. □

Lemma 6.1.7. *There are $2\Delta_{q-1}^p + \Delta_{q-1}^{p^2}$ isomorphism types of nonabelian groups of order p^2q with a normal Sylow q-subgroup. Each of them has a presentation as encoded in Table 6.1.*

Proof. Let G be a nonabelian group of order p^2q with a normal Sylow q-subgroup, then $G \cong P \ltimes_\varphi C_q$, where $|P| = p^2$. Since $\mathrm{Aut}(C_q) \cong \mathbb{Z}_q^*$ is cyclic, we apply Corollary 2.4.6 to construct and enumerate the isomorphism types of these nonabelian split extensions. Since P is abelian, we further deduce that $Z(G) = \mathrm{Ker}\,\varphi$. There are two cases to consider.

1. If $P \cong C_{p^2}$, then it has two proper normal subgroups with cyclic quotient. Moreover, such subgroups are characteristic in P. It follows that a P-action on C_q via φ is nontrivial if and only if $\mathrm{Ker}\,\varphi = 1$ or $\mathrm{Ker}\,\varphi \cong C_p$. In particular, if $\mathrm{Ker}\,\varphi = 1$, then $p^2 \mid (q-1)$; if $\mathrm{Ker}\,\varphi \cong C_p$, then $p \mid (q-1)$. Conversely, if $G \cong C_{p^2} \ltimes C_q$ has a trivial centre, then it is isomorphic to

   $$\mathrm{Pc}\langle a, b \mid a^{p^2}, b^q, b^a = b^{\rho(q,p^2)} \rangle;$$

   if G has nontrivial (proper) centre, then it is isomorphic to

   $$\mathrm{Pc}\langle a, b \mid a^{p^2}, b^q, b^a = b^{\rho(q,p)} \rangle.$$

2. If $P \cong C_p^2$, then it has a unique $\mathrm{Aut}(P)$-class of proper normal subgroups with cyclic quotients. Therefore, G is nonabelian if and only if $\varphi\colon P \to \mathrm{Aut}(C_q)$ is nontrivial, if and only if $\mathrm{Ker}\,\varphi \cong C_p$. By Corollary 2.4.6, such a split extension is unique up to isomorphism, and is isomorphic to
$$\mathrm{Pc}\langle a, b, c \mid a^p, b^p, c^q, c^a = c^{\rho(q,p)}\rangle.$$

Combing both cases, the enumeration follows; we obtain the presentations as encoded Table 6.1 accordingly. □

6.2 Groups of order p^3q

In this section, we discuss the groups of order p^3q. Western determined the isomorphism types of these groups in [51], where the proofs are detailed and in length. Here we provide a proof built on what we have established previously. We derived our results independent of Western's, but our main approaches are similar and our enumeration results agree.

6.2.1 Summary of results

Theorem 6.2.1. *Then there are*
$$5 + 7\Delta_p^2 + 2\Delta_{q-1}^4 + \Delta_{q-1}^8 + 3\Delta_p^2\Delta_q^3 + \Delta_p^2\Delta_q^7 + 10\Delta_q^2$$
isomorphism types of groups of even order p^3q; then there are
$$\begin{aligned} &5 + (5+p)\Delta_{q-1}^p + 2\Delta_{q-1}^{p^2} + \Delta_{q-1}^{p^3} + \frac{1}{6}(q^2 + 13q + 36 + 4\Delta_{q-1}^3)\Delta_{p-1}^q \\ &\quad + 2\Delta_{p+1}^q + (1 - \Delta_q^3)\Delta_{p^2+p+1}^q \end{aligned} \tag{6.2.1}$$
isomorphism types of groups of odd order p^3q. A group of order p^3q has a presentation as encoded Tables 6.2 and 6.3.

Note that $\Delta_{p+1}^q + (1 - \Delta_q^3)\Delta_{p^2+p+1}^q$ in (6.2.1) can be written as $(1 - \Delta_{p-1}^q)\Delta_{(p+1)(p^2+p+1)}^q$.

6.2.2 Determination of groups of order p^3q

From Burnside's pq-theorem we know that all groups of order p^3q are solvable. We also know that if $p > q$, then a group of such order always contains a normal Sylow p-subgroup by Lemma 6.1.2. In the following discussion, we will first show that a group of order p^3q always contains a normal Sylow subgroup except when it is isomorphic to Sym_4. Then we list all the isomorphism types of the nilpotent groups of this order type using the fact that a finite group is nilpotent if and only if all of its Sylow subgroups are normal. For the remaining non-nilpotent groups with a normal Sylow subgroup, we divide the determination into two cases depending on the existence of a normal Sylow q-subgroup, and for each case we further divide our discussions depending on the isomorphism types of the Sylow p-subgroups. In particular, there are only five possible isomorphism types of Sylow p-subgroups (with pc-presentations in Table 5.1) in a group of order p^3q.

TABLE 6.2: Groups of order p^3q with a normal Sylow q-subgroup, using Notations 4.1.1, 4.2.1, and 4.2.6.

Pc-relators	Parameters	Number of types
Cluster 1: nilpotent		
a^{p^3q}		1
a^{p^2}, b^{pq}		1
a^p, b^p, c^{pq}		1
$a^p, b^p, c^p, d^q, b^a/bc$		$1-\Delta_p^2$
$a^p/c, b^p, c^p, d^q, b^a/bc$		$1-\Delta_p^2$
$a^2, b^4, c^q, b^a/b^3$		Δ_p^2
$a^2/b^2, b^4, c^q, b^a/b^3$		Δ_p^2
Cluster 2: non-nilpotent, $P \cong C_{p^3}$		
$a^{p^3}, b^q, b^a/b^{\rho(q,p)}$		Δ_{q-1}^p
$a^{p^3}, b^q, b^a/b^{\rho(q,p^2)}$		$\Delta_{q-1}^{p^2}$
$a^{p^3}, b^q, b^a/b^{\rho(q,p^3)}$		$\Delta_{q-1}^{p^3}$
Cluster 3: non-nilpotent, $P \cong C_{p^2} \times C_p$		
$a^{p^2}, b^p, c^q, c^b/c^{\rho(q,p)}$		Δ_{q-1}^p
$a^{p^2}, b^p, c^q, c^a/c^{\rho(q,p)}$		Δ_{q-1}^p
$a^{p^2}, b^p, c^q, c^b/c^{\rho(q,p)}, c^a/c^{\rho(q,p^2)}$		$\Delta_{q-1}^{p^2}$
Cluster 4: non-nilpotent, $P \cong C_p^3$		
$a^p, b^p, c^p, d^q, d^a/d^{\rho(q,p)}$		Δ_{q-1}^p
Cluster 5: non-nilpotent, $P \cong p_+^{1+2}$ or $P \cong D_4$		
$a^p, b^p, c^p, d^q, c^a/bc, d^a/d^{\rho(q,p)}$		Δ_{q-1}^p
$a^2, b^4, c^q, b^a/b^3, c^a/c^{-1}$		Δ_p^2
Cluster 6: non-nilpotent, $P \cong p_-^{1+2}$ or $P \cong Q_8$		
$a^p, b^{p^2}, c^q, b^a/b^{p+1}, c^b/c^{\rho(q,p)}$		$(1-\Delta_p^2)\Delta_{q-1}^p$
$a^p, b^{p^2}, c^q, b^a/b^{p+1}, c^a/c^{\rho(q,p,k)}$	$k \in \mathbb{Z}_p^*$	$(p-1-\Delta_p^2)\Delta_{q-1}^p$
$a^2/b^2, b^4, b^a/b^3, c^q, c^a/c^{-1}$		Δ_p^2

Lemma 6.2.2. *Let G be a group of order p^3q. Then G has no normal Sylow subgroups if and only if $G \cong \mathrm{Sym}_4$.*

Proof. Since Sym_4 has 3 subgroups of order 8 and 4 subgroups of order 3, it follows from Theorem A.0.8 that G does not normalise a nontrivial Sylow subgroup. Conversely, if G has no normal Sylow p-subgroup, then Theorem A.0.8 shows that there are q Sylow p-subgroups in G as a direct consequence of . It follows that $q \equiv 1 \bmod p$, which implies that $p < q$. Similarly, $n_q(G) \equiv 1 \bmod q$ and $n_q(G) \mid p^3$, and it follows that $n_q(G) > q > p$. Also, since all q-subgroups of G intersect trivially, we deduce that $n_q(G) \neq p^3$, for otherwise there could be at most one subgroup of order p^3 in G, contradicting that $n_p(G) = q$. Therefore, $n_q(G) = p^2$, which implies that $q \mid (p^2-1) = (p-1)(p+1)$. Since $p < q$ as established, it follows that $q \mid (p+1)$, but $q \geq p+1$, thus $p = 2$ and $q = 3$. This affirms that G has order 24 and has 4 Sylow 3-subgroups. A direct computation (for example, carried out in GAP [27]) shows that $G \cong \mathrm{Sym}_4$. Alternatively, here we also include some theoretical arguments. Note that the conjugation action of G on $\mathrm{Syl}_q(G)$ gives rise to a homomorphism $f\colon G \to \mathrm{Sym}_4$. Since $K = \ker f \leq N_G(Q)$ and $|G|/|N_G(Q)| = 4$ for all $Q \in \mathrm{Syl}_3(G)$, implying $|N_G(Q)| = 6$, we know that $|K| \neq 3, 6$, for otherwise $K \lhd G$ contains a characteristic subgroup of order 3 that is normal in G. Also, observe that $|K| \neq 2$, for otherwise G/K has order 12 and contains a normal Sylow subgroup as seen in Lemma 6.1.4. In particular, if G/K contains a normal Sylow 3-subgroup, then $KQ/K = N_G(Q)/K$ is normal in G/K. This implies that $N_G(Q) \lhd G$ and

TABLE 6.3: Groups of order p^3q without normal Sylow q-subgroup, using Notations 4.1.1, 4.2.1, and 4.2.6.

Pc-relators	Parameters	Number of types
Cluster 7: $P \lhd G, P \cong C_{p^3}$		
$a^q, b^{p^3}, b^a/b^{\rho(p^3,q)}$		Δ_{p-1}^q
Cluster 8: $P \lhd G, P \cong C_{p^2} \times C_p$		
$a^q, b^{p^2}, c^p, c^a/c^{\rho(p,q)}$		Δ_{p-1}^q
$a^q, b^{p^2}, c^p, b^a/b^{\rho(p^2,q)}$		Δ_{p-1}^q
$a^q, b^{p^2}, c^p, b^a/b^{\rho(p^2,q)}, c^a/c^{\rho(p,q,k)}$	$k \in \mathcal{Z}_q^*$	$(q-1)\Delta_{p-1}^q$
Cluster 9: $P \lhd G, P \cong C_p^3$		
$a^q, b^p, c^p, d^p, b^a/b^{\rho(p,q)}$		Δ_{p-1}^q
$a^q, b^p, c^p, d^p, b^a/b^{\rho(p,q)}, c^a/c^{\rho(p,q,\sigma_q^k)}$	$0 \le k \le \frac{1}{2}(q-1)$	$\frac{1}{2}(q+1-\Delta_q^2)\Delta_{p-1}^q$
$a^q, b^p, c^p, d^p, b^a/b^{\rho(p,q)}, c^a/c^{\rho(p,q)}, d^a/d^{\rho(p,q,k)}$	$k \in \mathbb{Z}_q^*$	$(q-1)\Delta_{p-1}^q$
$a^q, b^p, c^p, d^p, b^a/b^{\rho(p,q)}, c^a/c^{\rho(p,q,\sigma_q^k)}, d^a/d^{\rho(p,q,\sigma_q^\ell)}$	$(k,\ell) \in \mathcal{P}$	$\frac{1}{6}(q^2-5q+6+4\Delta_{q-1}^3)\Delta_{p-1}^q$
$a^q, b^p, c^p, d^p, (b^a, c^a)/(b,c)^{\mathrm{Irr}_2(p,q)}$		$(1-\Delta_q^2)\Delta_{p+1}^q$
$a^q, b^p, c^p, d^p, (b^a, c^a, d^a)/(b,c,d)^{\mathrm{Irr}_3(p,q)}$		$(1-\Delta_q^2)(1-\Delta_q^3)\Delta_{p^2+p+1}^q$
Cluster 10: $P \lhd G, P \cong p_+^{1+2}$		
$a^q, b^p, c^p, d^p, c^b/cd, b^a/b^{\rho(p,q,q-1)}, c^a/c^{\rho(p,q)}$		Δ_{p-1}^q
$a^q, b^p, c^p, d^p, c^b/cd, b^a/b^{\rho(p,q)}, d^a/d^{\rho(p,q)}$		Δ_{p-1}^q
$a^q, b^p, c^p, d^p, c^b/cd, b^a/b^{\rho(p,q,k)}, c^a/c^{\rho(p,q,q+1-k)}, d^a/d^{\rho(p,q)}$	$2 \le k \le \frac{1}{2}(q+1)$	$\frac{1}{2}(q-1-\Delta_q^2)\Delta_{p-1}^q$
$a^q, b^p, c^p, d^p, c^b/cd, (b^a, c^a)/(b,c)^{\mathrm{Irr}_2(p,q)}$		$(1-\Delta_q^2)(1-\Delta_p^2)\Delta_{p+1}^q$
Cluster 11: $P \lhd G, P \cong p_-^{1+2}$ or Q_8		
$a^q, b^p, c^{p^2}, c^a/c^{\rho(p^2,q)}, c^b/c^{p+1}$.		Δ_{p-1}^q
$a^3, b^2/c^2, c^4, c^b/c^3, b^a/c, c^a/bc$		$\Delta_p^2\Delta_q^3$
Cluster 12: no normal Sylow subgroup		
$a^2, b^3, c^2, d^2, b^a/b^2, c^a/d, c^b/d, d^a/c, d^b/cd$		$\Delta_p^2\Delta_q^3$
Parameter sets		
$\mathcal{P} = \begin{cases} \{(x,y) \in \mathbb{Z}_{q-1}^2 \,:\, 1 \le x \le \frac{1}{3}(q-2),\ 2x \le y \le q-2-x\} & (q \equiv 2 \bmod 3) \\ \{(x,y) \in \mathbb{Z}_{q-1}^2 \,:\, 1 \le x \le \frac{1}{3}(q-1),\ 2x \le y \le q-2-x\} \cup \{(\frac{1}{3}(q-1), \frac{2}{3}(q-1))\} & (q \equiv 1 \bmod 3) \end{cases}$		

G contains a normal Sylow 3-subgroup; if G/K contains a normal Sylow 2-subgroup, then $S/K \lhd G/K$ for any $S \le G$ such that $K \lhd S$ and $|S/K| = 4$, and it follows that $S \in \mathrm{Syl}_2(G)$ and $S = P \lhd G$ by correspondence theorem (see [45, Theorem 2.28]), a contradiction. Therefore f is injective and G embeds into Sym_4; since $|G| = |\mathrm{Sym}_4|$, it follows that $G \cong \mathrm{Sym}_4$. □

The nilpotent groups of order p^3q are isomorphic to $P \times Q$, where $Q \cong C_q$ and the isomorphism types of P are listed in Table 5.1. We thus obtain the following result.

Lemma 6.2.3. *There are five isomorphism types of nilpotent groups of order p^3q, namely,*

$$C_{p^3q}, \quad C_{p^2q} \times C_p, \quad C_{pq} \times C_p^2, \quad p_+^{1+2} \times C_q, \quad p_-^{1+2} \times C_q.$$

It remains to consider the isomorphism types of non-nilpotent groups of order p^3q with a normal Sylow subgroup. Theorem 2.4.1 asserts that such groups are isomorphic to $P \ltimes Q$ or $Q \ltimes P$; Corollary 2.4.3(ii) and Corollary 2.4.6 classify these split extensions. In particular, Corollary 2.4.6(ii) shows that the isomorphism types of non-nilpotent split extensions $Q \ltimes P$ are in bijection with the conjugacy classes of subgroups of order q in $\mathrm{Aut}(P)$; using notation

from Definition 2.4.4, it follows that the number of isomorphism types of $P \ltimes Q$ is

$$\sum_{\ell \mid m} \sum_{K \in \mathcal{K}_\ell} \mathrm{ind}_K,$$

where $m = \gcd(p^3, q-1)$. We use these result in the following lemmas to explicitly determine the isomorphism types of non-nilpotent groups of order p^3q with a normal Sylow subgroup.

Lemma 6.2.4. *There are*

$$(5+p)\Delta_{q-1}^{p} + 2\Delta_{q-1}^{p^2} + \Delta_{q-1}^{p^3}$$

isomorphism types of non-nilpotent groups of order p^3q with a normal Sylow q-subgroup, each of which has a presentation as encoded Table 6.2.

Proof. By assumption, each such group has the form $G = P \ltimes_\varphi Q$, where P acts on Q nontrivially via $\varphi\colon P \to \mathrm{Aut}(Q)$. This requires that $|\varphi(P)|$ divides $|\mathrm{Aut}(Q)|$. Since $\mathrm{Aut}(Q) \cong \mathbb{Z}_q^*$, it follows that $\varphi(P)$ is normal in $\mathrm{Aut}(Q)$, and there are $\Delta_{q-1}^{p} + \Delta_{q-1}^{p^2} + \Delta_{q-1}^{p^3}$ nontrivial cyclic subgroups of order dividing p^3 in $\mathrm{Aut}(Q)$. In particular, we can apply Corollary 2.4.6 to construct and enumerate such split extensions $P \ltimes Q$. Following the notation in Corollary 2.4.6, we know it suffices to consider $\mathrm{Ker}\,\varphi = K$ for some representative $K \in \mathcal{K}_\ell$ with $\ell \mid \gcd(p^3, q-1)$. Since we only consider non-nilpotent $P \ltimes_\varphi Q$, it follows that $Z(G) \leq K$. Furthermore, since K acts trivially on Q, we know that $K \times Q$ is nilpotent. Let $F(G)$ be the largest nilpotent subgroup of G, namely, the Fitting subgroup. Then $K \times Q \leq F(G)$. Since such groups exist only if $|\varphi(P)|$ is greater than 1 and divides $\mathrm{Aut}(Q)$, in the following we consider $p \mid (q-1)$ throughout.

1. If $P \cong C_{p^3}$, then $Z(G) = \mathrm{Ker}\,\varphi = K$ for some $K \in \mathcal{K}_p \cup \mathcal{K}_{p^2} \cup \mathcal{K}_{p^3}$, and $\mathrm{ind}_K = 1$ for each such K. Let c_1 be the number of isomorphism types of groups $G \cong C_{p^3} \ltimes C_q$, then it follows from Corollary 2.4.6 that $c_1 = \Delta_{q-1}^{p} + \Delta_{q-1}^{p^2} + \Delta_{q-1}^{p^3}$. In particular, if $|Z(G)| = p^2$, then G is isomorphic to

   $$\mathrm{Pc}\langle a, b \mid a^{p^3}, b^q, b^a = b^{\rho(q,p)} \rangle;$$

   if $|Z(G)| = p$, then G is isomorphic to

   $$\mathrm{Pc}\langle a, b \mid a^{p^3}, b^q, b^a = b^{\rho(q,p^2)} \rangle;$$

   if $|Z(G)| = 1$, then G is isomorphic to

   $$\mathrm{Pc}\langle a, b \mid a^{p^3}, b^q, b^a = b^{\rho(q,p^3)} \rangle.$$

2. If $P \cong C_{p^2} \times C_p$, then $Z(G) = \mathrm{Ker}\,\varphi = K$ for some $K \in \mathcal{K}_p \cup \mathcal{K}_{p^2}$. For $K \in \mathcal{K}_p$, we have $|K| = p^2$; there are two $\mathrm{Aut}(P)$-classes of such subgroups, namely, $K \cong C_{p^2}$ or $K \cong C_p^2$. For $K \in \mathcal{K}_{p^2}$, we have $|K| = p$; such subgroups are isomorphic to C_{p^2} and lie in a single $\mathrm{Aut}(P)$-class. We determine $\mathrm{ind}_K = 1$ for all $K \in \mathcal{K}_p \cup \mathcal{K}_{p^2}$. Applying Corollary 2.4.6, we count in total $c_2 = 2\Delta_{q-1}^{p} + \Delta_{q-1}^{p^2}$ isomorphism types of such groups. In particular, if $Z(G) \cong C_{p^2}$, then G is isomorphic to

   $$\mathrm{Pc}\langle a, b, c \mid a^{p^2}, b^p, c^q, c^b = c^{\rho(p,q)} \rangle;$$

if $Z(G) \cong C_p^2$, then G is isomorphic to

$$\mathrm{Pc}\langle a, b, c \mid a^{p^2}, b^p, c^q, c^a = c^{\rho(p,q)}\rangle;$$

if $Z(G) \cong C_p$, then G is isomorphic to

$$\mathrm{Pc}\langle a, b, c \mid a^{p^2}, b^p, c^q, c^a = c^{\rho(q,p^2)}\rangle.$$

3. If $P \cong C_p^3$, then there is a unique $\mathrm{Aut}(P)$-class of normal subgroups with cyclic quotient and $Z(G) = \mathrm{Ker}\,\varphi = K$ for some $K \in \mathcal{K}_p$. Since $K \cong C_p^2$ and $\mathrm{ind}_K = 1$ for $K \in \mathcal{K}_p$, and $|\mathcal{K}_p| = 1$, it follows that there are $c_3 = \Delta_{q-1}^p$ isomorphism types of $P \ltimes_\varphi Q$ with representative $G \cong C_p^2 \times (C_p \ltimes C_q)$ given by

$$\mathrm{Pc}\langle a, b, c, d \mid a^p, b^p, c^p, d^q, d^a = d^{\rho(p,q)}\rangle.$$

4. If $P \cong p_+^{1+2}$ or $P \cong D_4$, then we can write $P = \mathrm{Pc}\langle a, b, c \mid a^p, b^p, c^p, b^a = bc\rangle$. If $p > 2$, then there is a unique $\mathrm{Aut}(P)$-class of normal subgroups K with cyclic quotient and $P/K \cong C_p$. In this case, it suffices to consider $G \cong P \ltimes_\varphi C_q$ with $\mathrm{Ker}\,\varphi = K = \langle b, c\rangle \cong C_p^2$ and we have $\mathrm{ind}_K = 1$. If $p = 2$ and $P \cong D_4$, then there are two $\mathrm{Aut}(D_4)$-classes of normal subgroups with a cyclic quotient; that is, $K \cong C_2$ or $K \cong C_4$. In each case, $\mathrm{ind}_K = 1$. In total, we count $c_4 = \Delta_{q-1}^p + \Delta_p^2$ isomorphism types of groups $G \cong p_+^{1+2} \ltimes_\varphi C_q$. Given such a group G, we can determine its isomorphism type by a case distinction on $F(G)$: if $F(G) \cong C_p \times C_{qp}$, then G is isomorphic to

$$\mathrm{Pc}\langle a, b, c, d \mid a^p, b^p, c^p, d^q, b^a = bc, d^a = d^{\rho(q,p)}\rangle;$$

if $F(G) \cong C_{4p}$, then G is isomorphic to

$$\mathrm{Pc}\langle a, b, c \mid a^2, b^4, c^q, b^a = b^3, c^a = c^{-1}\rangle.$$

5. If $P \cong p_-^{1+2}$ with $p > 2$, then we can write $P = \mathrm{Pc}\langle a, b \mid a^p, b^{p^2}, b^a = b^{p+1}\rangle$ for some $a, b \in G$. Observe that $\mathcal{K}_\ell \neq \varnothing$ if and only if $\ell = p$. Moreover, $K \in \mathcal{K}_p$ is either cyclic, generated by $a^k b$ for some $k \in \mathbb{Z}_p$, or elementary abelian, generated by $\{a, b^p\}$. Note that it is sufficient to consider $k = 0$: suppose $K = \langle a^k b\rangle$ for some $k \in \mathbb{Z}_p^*$, then the map $\{b_0 \mapsto a^k b, a_0 \mapsto a\}$ induces an isomorphism on P (Theorem 3.1.1). In other words, $\{\langle a^k b\rangle \mid k \in \mathbb{Z}_p\}$ lies in a single $\mathrm{Aut}(P)$-class. We see from Table 5.2 that $\langle a, b^p\rangle$ is characteristic in P. Thus, $\mathcal{K}_p = \{\langle b\rangle \cong C_{p^2}, \langle a, b^p\rangle \cong C_p^2\}$.
   (a) Suppose that $\mathrm{Ker}\,\varphi = K = \langle b\rangle$ and $Q = \langle c\rangle$. Then $G \cong C_p \ltimes (C_{p^2} \ltimes C_q)$, and we show that $\mathrm{ind}_K = p - 1$ by verifying that each of the possible value of $k \in \mathbb{Z}_p^*$ in

$$G(k) = \mathrm{Pc}\langle a, b, c \mid a^p, b^{p^2}, c^q, b^a = b^{p+1}, c^a = c^{\rho(q,p,k)}\rangle \tag{6.2.2}$$

   adds a new isomorphism type: Suppose, for a contradiction, that $G(1) \cong G(x)$ for some $1 < x \in \mathbb{Z}_p^*$, then there is an isomorphism $G(1) \to G(x)$ described by

$$\begin{cases} a & \mapsto a^{e_1} b^{e_2 p} \\ b & \mapsto a^{e_3} b^{e_4} \\ c & \mapsto c^f \end{cases},$$

where $e_i \in \mathbb{Z}_p$ with $e_1, e_4 > 0$. A direct calculation shows that such an isomorphism exists only if $e_1 = x$ and $e_4(p+1)^{e_1} \equiv e_4(p+1) \bmod p^2$. However, since $x \in \mathbb{Z}_p^*$, this forces that $x = 1$, a contradiction. Thus, there are $(p-1)\Delta_{q-1}^p$ new isomorphism types arising from the parametrised presentation (6.2.2).

(b) If $\operatorname{Ker}\varphi = K = \langle a, b^p\rangle$, then $G \cong C_p \ltimes (C_{p^2} \ltimes C_q)$ has a presentation of the form

$$\mathrm{Pc}\langle a, b, c \mid a^p, b^{p^2}, c^q, b^a = b^{p+1}, c^b = c^r\rangle,$$

where $r \in \mathbb{Z}_q^*$ has order p. Since $\varphi(P) = \langle\varphi(b)\rangle$ is uniquely determined as the normal subgroup of order p in $\operatorname{Aut}(Q)$, we have $\mathrm{ind}_K = 1$ and it suffices to consider $r = \rho(q, p)$ by Corollary 2.4.6.

If $P \cong Q_8$, then G has a presentation of the form

$$\mathrm{Pc}\langle a, b, c \mid a^2 = b^2, b^4, c^q, b^a = b^3, c^a = c^{r_1}, c^b = c^{r_2}\rangle,$$

where $r_i^2 \equiv 1 \bmod q$ for $i = 1, 2$. Since $|\mathcal{K}_4| = 1$ in Q_8, we deduce that $\operatorname{Ker}\varphi \cong C_4$ and $K = \langle b\rangle \in \mathcal{K}_4$ is characteristic in P. It follows that $r_2 = 1$ since $[b, Q] = 1$, and G is uniquely determined by the action of $\langle a\rangle$ on Q. In particular, G is isomorphic to

$$\mathrm{Pc}\langle a, b, c \mid a^2 = b^2, b^4, c^q, c^a = c^{-1}\rangle.$$

In total, there are $c_5 = (p - \Delta_p^2)\Delta_{q-1}^p$ isomorphism types of G if $p_-^{1+2} \cong P \in \mathrm{Syl}_p(G)$ with a normal Sylow q-subgroup.

Combing all of the above, we have the explicit isomorphism class representatives for all non-nilpotent groups of order p^3q with a normal Sylow q-subgroup; the enumeration follows from summing c_i over $i \in \{1, \ldots, 5\}$. In particular, we extract the results for the special case $|G| = 8q$ and count

$$7\Delta_p^2 + 2\Delta_{q-1}^4 + \Delta_{q-1}^8$$

such groups of order $8q$. □

Lemma 6.2.5. *If $q = 2$, then there are 10 isomorphism types of non-nilpotent groups of order p^3q with a normal Sylow p-subgroup; if $q = 3$, then there are $14\Delta_{p-1}^q + 2\Delta_{p+1}^q$ isomorphism types; if $q > 3$, then there are*

$$\frac{1}{6}(q^2 + 13q + 36 + 4\Delta_{q-1}^3)\Delta_{p-1}^q + 2\Delta_{p+1}^q + \Delta_{p^2+p+1}^q$$

isomorphism types.

Proof. Every such group has the form $G = Q \ltimes_\varphi P$, where $\varphi\colon Q \to \operatorname{Aut}(P)$ is nontrivial. Since Q is simple, $\varphi(Q) \cong C_q$ for any such nontrivial action φ. Since p is coprime to $|Q|$, every $P \in \mathrm{Syl}_p(G)$ is a strong Q-group and every Q-action fixes the characteristic subgroups of P setwise, as listed in Table 5.2. We apply Corollary 2.4.3 to enumerate and determine the isomorphism types of such split extensions by investigating the conjugacy classes of cyclic q-subgroups of $\operatorname{Aut}(P)$ for each isomorphism type of P. Similar to the preceding proof, we make canonical choices defined in Chapter 4 to find the isomorphism class representatives.

1. If $P \cong C_{p^3}$, then $\operatorname{Aut}(P) \cong \mathbb{Z}_{p^3}^*$ and $G \cong C_q \ltimes_\varphi C_{p_3}$ is a nonabelian metacyclic split extension. It follows that $q \mid (p-1)$. Since $C_q \cong \varphi(Q) \lhd \operatorname{Aut}(P)$, Corollary 2.4.3(ii) shows that there is a unique isomorphism type of such split extensions, namely,

$$\mathrm{Pc}\langle a, b \mid a^q, b^{p^3}, b^a = b^{\rho(p^3,q)}\rangle.$$

2. If $P \cong C_{p^2} \times C_p$, then $|\mathrm{Aut}(P)| = p^3(p-1)^2$. It follows that $q \mid (p-1)$. We further deduce that $\mathrm{Aut}(P)$ has a normal Sylow p-subgroup by Theorem A.0.8. On the other hand, studying the automorphisms of P we see that $\mathrm{Aut}(P)$ contains a subgroup isomorphic to C_{p-1}^2. It follows from Theorem 2.4.1 that this subgroup is unique up to conjugacy and complements the normal Sylow p-subgroup in $\mathrm{Aut}(P)$ Thus, we count $(q+1)\Delta_{p-1}^q$ conjugacy classes of cyclic subgroups C_q in $\mathrm{Aut}(P)$. Now we explicitly determine the isomorphism types. Write $P = \mathrm{Pc}\langle a, b \mid a^{p^2}, b^p\rangle$. Then from Table 5.2 we know that the subgroups $\langle a^p, b\rangle$ and $\langle b\rangle$ are characteristic in P. As a result, the characteristic subgroups of P are normal in every such extension. Thus, every such group $G \cong Q \ltimes P$ has a presentation of the form

$$G(x_1, x_2) = \mathrm{Pc}\langle a, b, c \mid a^q, b^{p^2}, c^p, b^a = b^{x_1}, c^a = c^{x_2}\rangle,$$

where $x_1 \in \mathbb{Z}_{p^2}^*, x_2 \in \mathbb{Z}_p^*$ and x_1, x_2 have order at most q. It remains to investigate the possibilities for x_i. If $x_1 = 1$, then $G(1, x_2) \cong (C_q \ltimes C_p) \times C_{p^2}$ is determined by the unique isomorphism type of the nonabelian group $C_q \ltimes C_p$ and G is isomorphic to

$$\mathrm{Pc}\langle a, b, c \mid a^q, b^{p^2}, c^p, c^a = c^{\rho(p,q)}\rangle.$$

Similarly, if $x_2 = 1$, then $G(x_1, 1) \cong (C_q \ltimes C_{p^2}) \times C_p$ is determined by the unique isomorphism type of the nonabelian group $C_q \ltimes C_{p^2}$ and has a presentation

$$\mathrm{Pc}\langle a, b, c \mid a^q, b^{p^2}, c^p, b^a = b^{\rho(p^2,q)}\rangle.$$

Now we are left with the case where both x_1, x_2 have order q. First we note that it is sufficient to fix $x_1 = \rho(p^2, q)$: a different choice of $x_1 \in \mathbb{Z}_{p^2}^*$ can be written as $\rho(p^2, q, k)$ for some $k \in \mathbb{Z}_q^*$, but we check that the map $\{a \mapsto a^k, b \mapsto b, c \mapsto c\}$ extends to an isomorphism $G(\rho(p^2, q, k), x_2^k) \to G(\rho(p^2, q), x_2)$. It remains to investigate the effect of choosing different values of x_2 in $G(\rho(p^2, q), x_2)$. By investigating the maps on the generators, we see that $G(\rho(p^2, q), k) \cong G(\rho(p^2, q), k')$ if and only if $k \equiv k' \bmod q$. We also know that there are precisely $q-1$ conjugacy classes of subgroups of order q in $\mathrm{Aut}(P)$ remained to be considered, accounting for the remaining $q-1$ isomorphism types, namely,

$$\mathrm{Pc}\langle a, b, c \mid a^q, b^{p^2}, c^p, b^a = b^{\rho(p^2,q)}, c^a = c^{\rho(p,q,k)}\rangle$$

parametrised by $k \in \mathbb{Z}_q^*$. In conclusion, there are in total $(q+1)\Delta_{p-1}^q$ isomorphism types of such non-nilpotent split extensions $C_q \ltimes (C_{p^2} \times C_p)$, agreeing with the number of conjugacy classes of subgroups of order q in $\mathrm{Aut}(P)$.

3. If $P \cong C_p^3$, then $\mathrm{Aut}(P) \cong \mathrm{GL}_3(p)$ with $|\mathrm{Aut}(P)| = p^3(p-1)^3(p^2+p+1)(p+1)$, and the nonabelian split extensions $G \cong Q \ltimes_\varphi P$ are in one-to-one correspondence with the conjugacy classes of cyclic subgroups C_q in $\mathrm{GL}_3(p)$ as counted in Theorem 4.2.7(iv). We look at the cases where q divides $(p-1)$, (p^2+p+1) or $(p+1)$, and determine the isomorphism types of $C_q \ltimes C_p^3$ in accordance with the conjugacy class representatives discussed in the proof of Theorem 4.2.7(iv).
   (a) If $q \mid (p-1)$, then Q acts diagonalisably on C_q^3. We see in the proof of Theorem 4.2.7 that, up to conjugacy, Q has a generating element represented by a diagonal matrix of the form $\mathrm{diag}(a, 1, 1)$, $\mathrm{diag}(a, a^{(\alpha^k)}, 1)$, and $\mathrm{diag}(a, a^{(\alpha^k)}, a^{(\alpha^\ell)})$, where $a = \rho(p, q)$, and $\alpha = \sigma_q$. In particular, if $|Z(G)| = p^2$, then Q acts (with our canonical choices of

automorphisms) on P via $\langle \mathrm{diag}(a,1,1)\rangle$, and G is isomorphic to

$$\mathrm{Pc}\langle a,b,c,d \mid a^q, b^p, c^p, d^p, b^a = b^{\rho(p,q)}\rangle.$$

On the other hand, if $|Z(G)| = p$, then Q acts via $\langle \mathrm{diag}(a, a^{(\alpha^k)}, 1)\rangle$, in which case $G \cong (C_q \ltimes C_p^2) \times C_p$. Such groups are fully determined by the isomorphism types of the centreless factor $C_q \ltimes C_p^2$, which are listed in Table 6.1. More specifically, there are $\frac{1}{2}(q+1-\Delta_q^2)$ isomorphism types of such groups in this case, namely,

$$\mathrm{Pc}\langle a,b,c,d \mid a^q, b^p, c^p, d^p, b^a = b^{\rho(p,q)}, c^a = c^{(\rho(p,q,\sigma_q^k)}\rangle$$

parametrised by $k \in \{0, \dots \lfloor \frac{1}{2}(q-1)\rfloor\}$. It remains to consider the cases where $Z(G) = 1$, in which case Q acts on P via $\langle \mathrm{diag}(a, a^{(\alpha^k)}, a^{(\alpha^\ell)})\rangle$. In this case, any such group is isomorphic to

$$G(x,y) = \mathrm{Pc}\langle a,b,c,d \mid a^q, b^p, c^p, d^p, b^a = b^{\rho(p,q)}, c^a = c^{\rho(p,q,\sigma_q^x)}, d^a = d^{\rho(p,q,\sigma_q^y)}\rangle,$$

for some $x, y \in \mathbb{Z}_q^*$ with $r \in \mathbb{Z}_p^*$ of order q. From Corollary 2.4.3(ii) and Theorem 4.2.7(iv) we know that two such groups $G(k,\ell)$ and $G(x,y)$ are isomorphic if and only if the cyclic groups $\langle \mathrm{diag}(r, r^{(\sigma_q^k)}, r^{(\sigma_q^\ell)})\rangle$ and $\langle \mathrm{diag}(r, r^{(\sigma_q^x)}, r^{(\sigma_q^y)})\rangle$ are conjugate in $\mathrm{GL}_3(p)$, if and only if $\{x,y\} \in \{\{k,\ell\}, \{-\ell, k-\ell\}, \{\ell-k, -k\}\}$. It follows that if $k = \ell$, then the pairs $(0,-k), (-k,0), (k,k)$ define the same isomorphism type, and there are $q-1$ isomorphism types of G parametrised by

$$\mathrm{Pc}\langle a,b,c,d \mid a^q, b^p, c^p, d^p, b^a = b^{\rho(p,q)}, c^a = c^{\rho(p,q)}, d^a = d^{\rho(p,q,k)}\rangle,$$

with $k \in \mathbb{Z}_q^*$. It remains to consider that $k \neq \ell$ and $k, \ell \in \{1, \dots, q-2\}$. To find the parameter sets $\{k,\ell\}$ that define nonisomorphic groups, it is equivalent to find the remaining $\frac{1}{6}(q^2 - 5q + 6 + 4\Delta_{q-1}^3)$ representatives for the Sym_3-orbits in $\mathbb{Z}_{q-1}^3$ (see Theorem 4.2.7(iv)). Without loss of generality, consider $k < \ell$, and define the representative of each orbit to be the ordered pair $(a,b) \in \{(k,\ell), (-k, \ell-k), (-\ell, k-\ell)\}$ such that $a = \min(k, -k, -\ell) \bmod (q-1)$. A direct computation shows that at least one of the ordered pairs $(k,\ell), (-k,\ell-k), (-\ell,k-\ell)$ contains an entry that is less than or equal to $\frac{1}{3}(q-1)$. Hence, it suffices to consider $1 \leq k \leq \frac{1}{3}(q-1)$. In particular, $k = \frac{1}{3}(q-1)$ is an integer if and only if $3 \mid (q-1)$. By our choice of the representatives, it follows that $2k \leq \ell \leq q-2-k$ for all pairs (k,ℓ) with an exception at $(\frac{1}{3}(q-1), \frac{2}{3}(q-1))$, which exists only if $3 \mid (q-1)$. In conclusion, there are $\frac{1}{6}(q^2 - 5q + 6 + 4\Delta_{q-1}^3)$ isomorphism types in this case, namely,

$$\mathrm{Pc}\langle a,b,c,d \mid a^q, b^p, c^p, d^p, b^a = b^{\rho(p,q)}, c^a = c^{\rho(p,q,\sigma_q^k)}, d^a = d^{\rho(p,q,\sigma_q^\ell)}\rangle,$$

parametrised by $(k,\ell) \in \mathbb{Z}_{q-1}^2$ with $k < \ell$, such that $(k,\ell) = (\frac{1}{3}(q-1), \frac{2}{3}(q-1))$, or $1 \leq k \leq \frac{1}{3}(q-1)$ and $2k \leq \ell \leq q-2-k$.

(b) If $q \nmid (p-1)$ and $q \mid (p^2+p+1)$, then $q > 3$ and Q acts irreducibly on C_p^3. Since there is a unique conjugacy class of irreducible subgroups C_q in $\mathrm{GL}_3(q)$, such extensions are isomorphic to

$$\mathrm{Pc}\langle a,b,c,d \mid a^q, b^p, c^p, d^p, (b^a, c^a, d^a) = (b,c,a)^{\mathrm{Irr}_3(p,q)}\rangle,$$

where $\mathrm{Irr}_3(p,q)$is the canonical irreducible automorphism of order q in $\mathrm{GL}_3(p)$ de-

scribed in Notation 4.2.6.

(c) Lastly, consider $q \nmid (p-1)$ and $q \mid (p+1)$. This implies that $q > 2$. Since q divides neither $|\mathrm{Aut}(C_p)|$ nor $|\mathrm{GF}(p^3)|$, the Q-action on P embeds into an irreducible subgroup of $\mathrm{GL}_2(p)$ and G is isomorphic to $(C_q \ltimes C_p^2) \times C_p$. In particular, G has a pc-presentation

$$\mathrm{Pc}\langle a, b, c, d \mid a^q, b^p, c^p, d^p, (b^a, c^a) = (b, c)^{\mathrm{Irr}_2(p,q)} \rangle,$$

where $\mathrm{Irr}_2(p, q)$as described in Notation 4.2.6.

4. If $P \cong D_4$, then $\mathrm{Aut}(P) \cong D_4$, in which case there exists no non-nilpotent split extension $C_q \ltimes D_4$. If $p > 2$ and $P \cong p_+^{1+2}$, then $|\mathrm{Aut}(P)| = p^3(p-1)^2(p+1)$ by Proposition 5.1.9. Moreover, Proposition 5.1.9 shows that $\mathrm{Aut}(P)$ is an extension of C_p^2 by $\mathrm{GL}_2(p)$, and it contains a normal Sylow p-subgroup. There are two cases to consider: either $q \mid (p-1)$ or $q \mid (p+1)$. For each case we make further distinctions on the centre of G. In particular, we know that the centre of G is characteristic in P, leaving only two possibilities: either $Z(G) \cong C_p$ or $Z(G)$ is trivial. Moreover, the conjugacy classes of cyclic groups of order q in $\mathrm{Aut}(P)$ are in one-to-one correspondence with those of $\mathrm{Aut}(P/\Phi(P)) \cong \mathrm{GL}_2(p)$ by Proposition 5.1.9. In conjunction with Lemma 4.2.8, it follows that the number of non-nilpotent isomorphism types of $C_q \ltimes p_+^{1+2}$ is counted by Theorem 4.2.7(i). To explicitly determine the isomorphism types arising from this case, we lift the Q-actions on the normal subgroup C_p^2 in P to determine the split extensions $Q \ltimes P$.

(a) If $q \mid (p-1)$ and $Z(G) \cong C_p$, then Q acts trivially on $Z(P)$ and G is isomorphic to

$$G(r_1, r_2) = \mathrm{Pc}\langle a, b, c, d \mid a^q, b^p, c^p, d^p, c^b = cd, b^a = b^{r_1}, c^a = c^{r_2} \rangle,$$

for some $r_1, r_2 \in \mathbb{Z}_p^*$ such that r_1, r_2 are of order at most q and not both 1. To determine the values of r_i, note that $(c^b)^a = (c^a)^{(b^{r_1})}$ is required for the pc-presentation to be consistent, but

$$(c^b)^a = (cd)^a = c^a d^a = c^{r_2} d \text{ and } (c^a)^{(b^{r_1})} = (c^{r_2})^{(b^{r_1})} = c^{r_2} d^{r_1 r_2},$$

which forces $r_2 \equiv r_1^{-1} \bmod p$ and both $r_1, r_2 \in \mathbb{Z}_p^*$ have order q. On the other hand, since $\{a \mapsto a^k\}$ extends to an isomorphism $G(r_1^k, r_1^{-k}) \to G(r_1, r_1^{-1})$ for any $k \in \mathbb{Z}_q^*$, it suffices to fix $r_1 = \rho(p, q)$. Hence, there is a unique isomorphism type of G:

$$\mathrm{Pc}\langle a, b, c, d \mid a^q, b^p, c^p, d^p, c^b = cd, b^a = b^{\rho(p,q)}, c^a = c^{\rho(p,q,q-1)} \rangle.$$

(b) If $q \mid (p-1)$ and $Z(G) = 1$. Then Q acts nontrivially on $Z(P) \lhd G$, and G is isomorphic to

$$G(r_1, r_2, r_3) = \mathrm{Pc}\langle a, b, c, d \mid a^q, b^p, c^p, d^p, c^b = cd, b^a = b^{r_1}, c^a = c^{r_2}, d^a = d^{r_3} \rangle,$$

where each $r_1, r_2 \in \mathbb{Z}_p^*$ has order at most q and $r_3 \in \mathbb{Z}_p^*$ has order q. Since $\{a \mapsto a^k\}$ extends to an isomorphism $G(r_1, r_2, r_3^k) \to G(r_1^{(k^{-1})}, r_2^{(k^{-1})}, r_3)$ for any $k \in \mathbb{Z}_q^*$, it suffices to fix $r_3 = \rho(p, q)$, denoted by r. Then we can write $r_1 = r^x$, $r_2 = r^y$ for some $x, y \in \mathbb{Z}_q$. For such a pc-presentation to be consistent it is required that

$$(c^b)^a = (c^a)^{(b^a)},$$

which is equivalent to

$$c^{(r^y)}d^r = c^{(r^y)}d^{(r^{x+y})};$$

that is,

$$x + y \equiv 1 \bmod q.$$

Hence, any such group G is isomorphic to

$$G(k)=\mathrm{Pc}\langle a,b,c,d \mid a^q, b^p, c^p, d^p, c^b = cd, b^a = b^{\rho(p,q,k)}, c^a = c^{\rho(p,q,q+1-k)}, d^a = d^{\rho(p,q)}\rangle,$$

for some $k \in \mathbb{Z}_q^*$. However, the map $\{b \mapsto c, c \mapsto b, d \mapsto d^{-1}\}$ extends to an isomorphism, hence the groups $G(k)$ and $G(q+1-k)$ are isomorphic for any $k \in \mathbb{Z}_q^*$. Therefore, there are $\frac{1}{2}(q-1-\Delta_q^2)$ new isomorphism types arising from this case, parametrised by $G(k)$ with $k \in \{2,\dots,\lfloor\frac{1}{2}(q+1)\rfloor\}$.

(c) If $q \mid (p+1)$, then Q acts trivially on $\langle d\rangle$. Since there is a unique conjugacy class of subgroups of order $p+1$ in $\mathrm{Aut}(P)$, there is a unique conjugacy class of irreducible cyclic subgroups of order q in $\mathrm{Aut}(P)$, corresponding to the unique isomorphism type of such extensions, namely,

$$\mathrm{Pc}\langle a,b,c,d \mid a^q, b^p, c^p, d^p, c^b = cd, (b^a, c^a) = (b,c)^{\mathrm{Irr}_2(p,q)}\rangle.$$

In total, there are $\frac{1}{2}(q+3-\Delta_q^2)\Delta_{p-1}^q + (1-\Delta_q^2)\Delta_{p+1}^q$ isomorphism types, in one-to-one correspondence with the conjugacy classes of reducible cyclic subgroups C_q in $\mathrm{GL}_2(p)$, with $p > 2$.

5. If $P \cong p_-^{1+2}$ and $p > 2$, then $\mathrm{Aut}(P) \cong C_{p-1} \ltimes p_+^{1+2}$ has size $p^3(p-1)$ by Proposition 5.1.10. From Theorem A.0.8 and Theorem 2.4.1 we know $\mathrm{Aut}(P)$ has a normal Sylow p-subgroup with a unique (up to conjugacy) complement isomorphic to C_{p-1}. It follows that $q \mid (p-1)$ and $\varphi(Q)$ is unique up to conjugacy in $\mathrm{Aut}(P)$, corresponding to the unique isomorphism type of such extensions, namely,

$$\mathrm{Pc}\langle a,b,c \mid a^q, b^p, c^{p^2}, c^b = c^{p+1}, c^a = c^{\rho(p^2,q)}\rangle.$$

On the other hand, if $P \cong Q_8$, then $\mathrm{Aut}(P) \cong \mathrm{Sym}_4$, and it follows that $q = 3$. Moreover, $\varphi(Q)$ is a Sylow q-subgroup of $\mathrm{Aut}(P) \cong \mathrm{Sym}_4$; Sylow q-subgroups are conjugate in $\mathrm{Aut}(P)$. By Corollary 2.4.3, this shows that there is a unique non-nilpotent split extension $C_3 \ltimes Q_8$, namely,

$$\mathrm{Pc}\langle a,b,c,d \mid a^3, b^2 = c^2 = d, d^2, c^b = cd, b^a = c, c^a = bc.\rangle \tag{6.2.3}$$

In particular, this group is isomorphic to $\mathrm{SL}_2(3)$.

Combining all of the cases above, the claimed result follows. In particular, there are 10 non-nilpotent isomorphism types of the groups of order $2p^3$, each of which contains a normal Sylow p-subgroup. □

TABLE 6.4: Isomorphism type of groups of order p^2q^2, using Notations 4.1.1, 4.2.1, and 4.2.6.

Pc-relators	Structure	Number of types
Cluster 1: nilpotent		
$a^{p^2q^2}$		1
a^p, b^{pq^2}		1
a^{p^2q}, b^q		1
a^{pq}, b^{pq}		1
Cluster 2: non-nilpotent, $C_{p^2} \cong P \lhd G$ with complement $Q \cong C_{q^2}$		
$a^{q^2}, b^{p^2}, b^a / b^{\rho(p^2,q)}$		Δ_{p-1}^q
$a^{q^2}, b^{p^2}, b^a / b^{\rho(p^2,q^2)}$		$\Delta_{p-1}^{q^2}$
Cluster 3: non-nilpotent, $C_{p^2} \cong P \lhd G$ with complement $Q \cong C_q^2$		
$a^q, b^q, c^{p^2}, c^a / c^{\rho(p^2,q)}$		Δ_{p-1}^q
Cluster 4: non-nilpotent, $C_p^2 \cong P \lhd G$ with complement $Q \cong C_{q^2}$, or $(p,q) = (3,2)$		
$a^{q^2}, b^p, c^p, b^a / b^{\rho(p,q)}$		Δ_{p-1}^q
$a^{q^2}, b^p, c^p, (b^a, c^a) / (b,c)^{M(p,q,\sigma_q^k)}$	$0 \le k \le \frac{1}{2}(q-1)$	$\frac{1}{2}(q+1-\Delta_q^2)\Delta_{p-1}^q$
$a^{q^2}, b^p, c^p, b^a / b^{\rho(p,q^2)}$		$\Delta_{p-1}^{q^2}$
$a^{q^2}, b^p, c^p, (b^a, c^a) / (b,c)^{M(p,q^2,\sigma_{q^2}^k)}$	$0 \le k \le \frac{1}{2}(q^2-q)$	$\frac{1}{2}(q^2-q+2)\Delta_{p-1}^{q^2}$
$a^{q^2}, b^p, c^p, (b^a, c^a) / (b,c)^{M(p,q^2,kq)}$	$k \in \mathbb{Z}_q^*$	$(q-1)\Delta_{p-1}^{q^2}$
$a^9, b^2, c^2, b^a / c, c^a / bc$		$\Delta_p^3\Delta_q^2$
$a^{q^2}, b^p, c^p, (b^a, c^a) / (b,c)^{\mathrm{Irr}_2(p,q)}$		$(1-\Delta_q^2)\Delta_{p+1}^q$
$a^{q^2}, b^p, c^p, (b^a, c^a) / (b,c)^{\mathrm{Irr}_2(p,q^2)}$		$\Delta_{p+1}^{q^2}$
Cluster 5: non-nilpotent, $C_p^2 \cong P \lhd G$ with complement $Q \cong C_q^2$, or $(p,q) = (3,2)$		
$a^q, b^q, c^p, d^p, c^a / c^{\rho(p,q)}$		Δ_{p-1}^q
$a^q, b^q, c^p, d^p, (c^a, d^a) / (c,d)^{M(p,q,\sigma_q^k)}$	$0 \le k \le \frac{1}{2}(q-1)$	$\frac{1}{2}(q+1-\Delta_q^2)\Delta_{p-1}^q$
$a^q, b^q, c^p, d^p, c^a / c^{\rho(p,q)}, d^b / d^{\rho(p,q)}$		Δ_{p-1}^q
$a^3, b^3, c^2, d^2, c^a / d, d^a / cd$		$\Delta_p^3\Delta_q^2$
$a^q, b^q, c^p, d^p, (c^a, d^a) / (c,d)^{\mathrm{Irr}_2(p,q)}$		$(1-\Delta_q^2)\Delta_{p+1}^q$

6.3 Groups of order p^2q^2

6.3.1 Summary of results

Theorem 6.3.1. *Let $p > q$ be primes. There are four abelian isomorphism types of abelian groups of order p^2q^2, namely,*

$$C_{p^2q^2}, \quad C_{p^2q} \times C_q, \quad C_p \times C_{pq^2}, \quad C_{pq} \times C_{pq}.$$

If $q = 2$ and $p = 3$, then there are 10 isomorphism types of nonabelian groups of order p^2q^2; if $q = 2$ and $p > 3$, then there are $7 + 5\Delta_{p-1}^4 + \Delta_{p+1}^4$ isomorphism types of nonabelian groups of order p^2q^2; if $p > q > 2$, then there are

$$(6+q)\Delta_{p-1}^q + \frac{1}{2}(4+q+q^2)\Delta_{p-1}^{q^2} + 2\Delta_{p+1}^q + \Delta_{p+1}^{q^2}$$

isomorphism types of nonabelian groups of order p^2q^2; Each isomorphism type has a presentation as encoded Table 6.4.

6.3.2 Determination of groups of order p^2q^2

Abelian groups of order p^2q^2 are determined by Theorem A.0.12. It remains to consider the nonabelian isomorphism types. Without loss of generality, assume $p > q$ throughout this section. Then Theorem A.0.8 implies that the number of Sylow p-subgroups in a group G of order p^2q^2 is either 1 or q^2. Let G be a group of order p^2q^2 and $P \in \mathrm{Syl}_p(G)$ and $Q \in \mathrm{Syl}_q(G)$. Since both P and Q are abelian, G is nonabelian if and only if it is non-nilpotent. If $n_p(G) = 1$, then P is normal in G, and $G \cong Q \ltimes P$. If $n_p(G) = q^2$, then p divides $(q+1)$ since $p > q$, implying that $p = 3$ and $q = 2$, in which case we will show that the Sylow 2-subgroup is normal. This allows us to apply Theorem 2.4.2(ii) to determine all non-nilpotent groups of order p^2q^2.

Lemma 6.3.2. *There are*

$$(6 + q - \Delta_q^2)\Delta_{p-1}^q + \frac{1}{2}(4 + q + q^2)\Delta_{p-1}^{q^2} + 2(1 - \Delta_q^2)\Delta_{p+1}^q + \Delta_{p+1}^{q^2}$$

isomorphism types of nonabelian groups of order p^2q^2 with a normal Sylow p-subgroup.

Proof. Any such group as described in the lemma is a split extension $G \cong Q \ltimes_\varphi P$, where $\varphi\colon Q \to \mathrm{Aut}(P)$ is a nontrivial action. Since both P and Q are abelian, $\mathrm{Ker}\,\varphi \leq Z(G)$. We make case distinction on the isomorphism types of P and Q to determine the isomorphism types of such extensions in the following.

1. If $P \cong C_{p^2}$ and $Q \cong C_{q^2}$, then $|\mathrm{Aut}(P)| = p(p-1)$ and $q \mid (p-1)$. Since Q, P, and $\mathrm{Aut}(P)$ are all cyclic, we apply Corollary 2.4.3(ii) and Corollary 2.4.6. In particular, we note that $\mathrm{Ker}\,\varphi = K$ for some $K \in \mathcal{K}_q \cup \mathcal{K}_{q^2}$; for each $K \in \mathcal{K}$, it is straightforward to check that $\mathrm{ind}_K = 1$. Also, $Z(G) = \mathrm{Ker}\,\varphi$. Therefore, there are $\Delta_{p-1}^q + \Delta_{p-1}^{q^2}$ isomorphism types of such groups, and we explicitly determine them as follows:
   - If $Z(G) \cong C_q$, then $K \in \mathcal{K}_q$ and $q \mid (p-1)$. Since $|\mathcal{K}_q| = 1$, there is a unique isomorphism type of such groups, namely,
   $$G \cong \mathrm{Pc}\langle a, b \mid a^{q^2}, b^{p^2}b^a = b^{\rho(p^2,q)}\rangle.$$
   - If $Z(G) = 1$, then $K \in \mathcal{K}_{q^2}$ and $q^2 \mid (p-1)$. Since $|\mathcal{K}_{q^2}| = 1$, there is a unique isomorphism type of such groups, namely,
   $$G \cong \mathrm{Pc}\langle a, b \mid a^{q^2}, b^{p^2}b^a = b^{\rho(p^2,q^2)}\rangle.$$
2. If $P \cong C_p^2$ and $Q \cong C_{q^2}$, then $\mathrm{Aut}(P) \cong \mathrm{GL}_2(p)$. It follows that $q \mid (p^2-1)$. Applying Corollary 2.4.3(ii), the enumeration of the isomorphism types of such groups follows from Theorem 4.2.7. To explicitly construct these groups, we first note that $\mathrm{Ker}\,\varphi = K$ for some $K \in \mathcal{K}_q \cup \mathcal{K}_{q^2}$. Since $K \leq Z(G)$, there are two cases to consider:
   - If $q \mid |Z(G)|$, then $K \in \mathcal{K}_q$. In this case, $q \mid (p^2-1)$, and G is uniquely determined by its nonabelian maximal normal subgroup of order p^2q that has a normal Sylow p-subgroups. The isomorphism types of such groups are in bijection with the conjugacy classes of subgroups of order q in $\mathrm{GL}_2(p)$; that is, there are $\frac{1}{2}(q + 3 - \Delta_q^2)\Delta_{p-1}^q + (1 - \Delta_q^2)\Delta_{p+1}^q$ isomorphism types in this case, counted in Theorem 4.2.7(i). Using Notations 4.1.1, 4.2.1, 4.2.6, we construct the isomorphism class

representatives for these groups as follows:

$$\begin{aligned}&\mathrm{Pc}\langle a,b,c \mid a^{q^2}, b^p, c^p, (b^a,c^a) = (b,c)^{\mathrm{Irr}_2(p,q)}\rangle,\\ &\mathrm{Pc}\langle a,b,c \mid a^{q^2}, b^p, c^p, b^a = b^{\rho(p,q)}\rangle,\\ &\mathrm{Pc}\langle a,b,c \mid a^{q^2}, b^p, c^p, (b^a,c^a) = (b,c)^{M(p,q,\sigma_q^k)}\rangle,\end{aligned}$$

with $k \in \{0,\dots,\lfloor \frac{1}{2}(q-1)\rfloor\}$.

- If $q \nmid |Z(G)|$, then $K \in \mathcal{K}_{q^2}$, and it follows that $q^2 \mid (p^2-1)$. The isomorphism types of such groups are in bijection with the conjugacy classes of cyclic subgroups C_{q^2} in $\mathrm{GL}_2(p)$ by Corollary 2.4.3(ii), which are counted in Theorem 4.2.7(ii). In conjunction with Corollary 2.4.3(ii), the proof of Theorem 4.2.7(ii) shows that each of the conjugacy class representative corresponds to a new isomorphism type. We thus follow the proof of Theorem 4.2.7(ii) to explicitly determine the isomorphism class representatives. If $q^2 \mid (p+1)$, then Q acts irreducibly on P and there is a unique isomorphism type of such split extensions, namely,

  $$\mathrm{Pc}\langle a,b,c \mid a^{q^2}, b^p, c^p, (b^a,c^a) = (b,c)^{\mathrm{Irr}_2(p,q^2)}\rangle.$$

  If $q^2 \mid (p-1)$, then Q acts diagonalisably on P. If $Z(G) = p$, then G is isomorphic to

  $$\mathrm{Pc}\langle a,b,c \mid a^{q^2}, b^p, c^p, b^a = b^{\rho(p,q^2)}\rangle.$$

  If $Z(G) = 1$, then there are $\frac{1}{2}(q^2-q+2)+q-1$ isomorphism types of such group, parametrised by

  $$\mathrm{Pc}\langle a,b,c \mid a^{q^2}, b^p, c^p, (b^a,c^a) = b^{M(p,q^2,\sigma_{q^2}^k)}\rangle,$$

  where $0 \le k \le \frac{1}{2}(q^2-q)$, and

  $$\mathrm{Pc}\langle a,b,c \mid a^{q^2}, b^p, c^p, (b^a,c^a) = b^{M(p,q^2,kq)}\rangle,$$

  where $k \in \mathbb{Z}_q^*$. In total, we find $\frac{1}{2}(q^2+q+2)$ isomorphism types in accordance with the conjugacy class representatives of cyclic groups of order q^2 in $\mathrm{GL}_2(p)$ (Theorem 4.2.7(ii)).

3. If $P \cong C_{p^2}$ and $Q \cong C_q^2$, then $\mathrm{Aut}(P) \cong \mathbb{Z}_{p^2}^*$ and it follows that $q \mid (p-1)$. Moreover, $\operatorname{Ker}\varphi \cong \varphi(Q) \cong C_q$. Thus, G is isomorphic to $C_q \times (C_q \ltimes C_{p^2})$. There are Δ_{p-1}^q isomorphism types of nonabelian extensions $C_q \ltimes C_{p^2}$ as seen in Theorem 6.1. Thus, G is isomorphic to

   $$\mathrm{Pc}\langle a,b,c \mid a^q, b^q, c^{p^2}, c^a = c^{\rho(p^2,q)}\rangle.$$

4. If $P \cong C_p^2$ and $Q \cong C_q^2$, then $\mathrm{Aut}(P) \cong \mathrm{GL}_2(p)$ and $q \mid (p^2-1)$. Observe that Q acts nonfaithfully on P if and only if $q \mid |Z(G)|$, in which case $G \cong C_q \times (C_q \ltimes C_p^2)$ is determined by the isomorphism types of nonabelian groups $C_q \ltimes C_p^2$, which are determined in Lemma 6.1.6. It follows that there are $\frac{1}{2}(q+3-\Delta_q^2)\Delta_{p-1}^q + (1-\Delta_q^2)\Delta_{p+1}^q$ isomorphism

types of such groups. In particular, G is isomorphic to one of the following:

$$\mathrm{Pc}\langle a,b,c,d \mid a^q, b^q, c^p, d^p, (c^a,d^a) = (c,d)^{\mathrm{Irr}_2(p,q)}\rangle,$$
$$\mathrm{Pc}\langle a,b,c,d \mid a^q, b^q, c^p, d^p, c^a = c^{\rho(p,q)}\rangle,$$
$$\mathrm{Pc}\langle a,b,c,d \mid a^q, b^q, c^p, d^p, (c^a,d^a) = (c,d)^{M(p,q,\sigma_q^k)}\rangle,$$

with $k \in \{0,\ldots,\lfloor \frac{1}{2}(q-1)\rfloor\}$. If Q acts faithfully on P, then $Z(G) = 1$ and $q \mid (p-1)$. Since there is a unique conjugacy class of elementary abelian subgroups C_q^2 in $\mathrm{GL}_2(p)$ as shown in Theorem 4.2.7(ii), it follows that G isomorphic to

$$\mathrm{Pc}\langle a,b,c,d \mid a^q, b^q, c^p, d^p, c^a = c^{\rho(p,q)}, d^b = d^{\rho(p,q)}\rangle.$$

Combining the results for each case, we obtain the claimed result. In particular, if $q = 2$, then the counting formula simplifies to $7 + 5\Delta_{p-1}^4 + \Delta_{p+1}^4$. □

It remains to consider the special case where G is non-nilpotent and contains no normal Sylow p-subgroup, in which case $p = 3, q = 2$ as a consequence of Theorem A.0.8 (as discussed at the start of this section).

Lemma 6.3.3. *If G is a non-nilpotent group of order 36 and contains no normal Sylow 3-subgroup, then G contains a normal Sylow 2-subgroup. There are two isomorphism types of such groups, namely,*

$$C_9 \ltimes C_2^2, \quad C_3^2 \ltimes C_2^2 \cong C_3 \times \mathrm{Alt}_4.$$

Proof. This can be shown by a direct computation in GAP [27]. Alternatively, we present a theoretical argument as follows: Since Sylow 3-subgroups of G are not normal, it follows from Theorem A.0.8 that there are 4 Sylow 3-subgroups. Let $P \in \mathrm{Syl}_p(G)$, then [35, Corollary 1.15] shows that $[G\colon N_G(P)] = n_p(G) = 4$. It follows that $|P| = |N_G(P)| = 9$. Since $P \leq N_G(P)$, we have $N_G(P) = P$. Consider the action of G on the set of all left cosets of $N_G(P)$ via left multiplication. This gives rise to a homomorphism $\varphi\colon G \to \mathrm{Sym}_4$. Since G does not embed into Sym_4, we know $\mathrm{Ker}\,\varphi \neq 1$. Also, $|\mathrm{Ker}\,\varphi| \leq |N_G(P)|$. Denote $K = \mathrm{Ker}\,\varphi$. Since P is not normal in G by assumption, it follows that $|K| = 3$. Since all Sylow 3-subgroups of G are abelian, and $K \lhd G$, it follows that the centraliser of K contains at least $4(9-3)+3 = 27$ elements. By Lagrange's Theorem, it forces that $C_G(K) = G$; that is, $K \leq Z(G)$, which implies that $3 \mid |Z(G)|$. Since G is nonabelian and contains no normal Sylow q-subgroup, we deduce immediately that $|Z(G)| \notin \{9, 36\}$. We also deduce that $|Z(G)| \neq 18$, since G has no normal subgroup of order 18 (any group of order $18 = 2{\cdot}3^2$ contains a characteristic Sylow 3-subgroup as shown in Lemma 6.1.2, which would be normal in G, a contradiction). Moreover, $|G/Z(G)| \neq 3$, for otherwise $G/Z(G)$ is cyclic and G would be abelian, a contradiction. Hence, $|Z(G)| \in \{3, 6\}$. However, if $|Z(G)| = 6$, then G is a nonabelian central extension of C_6 by D_3 (otherwise G would be abelian), which contains a normal Sylow 3-subgroup, a contradiction. Hence, $|Z(G)| = 3$ and $Z(G) = K$. This shows that G is a central extension of K by H, where $|H| = 12$. If H has a normal Sylow 3-subgroup, then G will also have a normal Sylow 3-subgroup, a contradiction. Thus H has a normal (unique) Sylow 2-subgroup, which is also normal in G. Therefore, G is isomorphic to $Q \ltimes P$, where $Q \in \mathrm{Syl}_q(G)$. Since $\mathrm{Aut}(C_4) \cong C_2$ and $\mathrm{Aut}(C_2^2) \cong \mathrm{GL}_2(2) \cong \mathrm{Sym}_3$, we see that G has a normal subgroup $P \cong C_2^2$ and Q acts irreducibly on P. Finally, we apply Corollary 2.4.3 and explicitly determine the isomorphism types of G. If $Q \cong C_9$, then G is isomorphic to $\mathrm{Pc}\langle a,b,c \mid a^9, b^2, c^2, b^a = c, c^a = bc\rangle$; if $Q \cong C_3^2$, then G is isomorphic to $\mathrm{Pc}\langle a,b,c,d \mid a^3, b^3, c^2, d^2, c^a = d, d^a = cd\rangle$. □

Chapter 7

Groups of orders pqr, $pqrs$, and p^2qr

Let p, q, r, s be distinct primes. Groups of order pqr, $pqrs$ and p^2qr are special cases of squarefree and cubefree orders, hence for more general algorithms to generate such groups we refer to [16], [19], and [21]. The C-Group generation algorithm in [21] is a complete generalisation of [16] that generates groups of a given order whose Sylow subgroups are cyclic (namely, *C-groups*); it also offers an identification function that determines the assigned C-group ID of a given group. While this covers the construction and identification functionality for groups of order pqr and $pqrs$, for the sake of completeness, we include a discussion here. For groups of order p^2qr, it is well-known that such a group is nonsolvable if and only if it is isomorphic to Alt_5 of order 60 and that Alt_5 is the smallest simple group ([35, p. 29]).

7.1 Groups whose Sylow subgroups are cyclic

In [32], Hölder gave a formula for the enumeration of isomorphism types of squarefree groups. We have seen a trivial example in the previous chapter of groups of order pq, here we describe a more general approach to construct and classify squarefree groups using results of Burnside, Hölder, and Zassenhaus ([43, (10.1.10)]) on the structure of finite groups whose Sylow subgroups are all cyclic.

Theorem 7.1.1 (Hölder, Burnside, Zassenhaus, [43], (10.1.10))**.** *If G is a finite group all of whose Sylow subgroups are cyclic, then G has a presentation*

$$G = \mathrm{Pc}\langle a, b \mid a^m, b^n, b^a = b^r \rangle,$$

where n is an odd integer, $r \in \mathbb{Z}_n$ and $r^m \equiv 1 \bmod n$, and $\gcd(n, m(r-1)) = 1$.

Note that Theorem 7.1.1 classifies the structure of C-groups, but it does not solve the isomorphism problem. The next theorem due to Hölder gives a counting formula for the isomorphism types of squarefree groups. Hölder's approach in the derivation of this result also motivates the main approach we use in this chapter for the determination of groups of order p^2qr.

Theorem 7.1.2 ([32], § 7)**.** *Let n be a squarefree natural number, $f(n)$ be the number of isomorphism*

types of groups of order n. Then

$$f(n) = \sum_{m|n} \prod_{p \in \pi(n/m)} \frac{p^{c_m(p)} - 1}{p - 1},$$

where $\pi(x) = \{p \text{ is a prime} : p \mid x\}$ denotes the set of prime factors of a positive integer $x \in \mathbb{N}$, and $c_x(p)$ is the number of prime divisors $q \in \pi(x)$ pf x such that $q \equiv 1 \bmod p$ for each prime p.

We recall that the Fitting subgroup of G, denoted by $F(G)$, is the largest normal nilpotent subgroup of G. We recall a few results regarding the Fitting subgroup that are useful to the investigation of solvable groups.

Theorem 7.1.3 ([35])**.** *Let G be a finite group. Then*

(i) *$F(G)$ is unique and characteristic in G;*

(ii) *$F(G)/\Phi(G) = F(G/\Phi(G))$;*

(iii) *if $N \trianglelefteq G$ is nontrivial, then $N \cap F(G) = F(N)$.*

Proof. For (i), we refer to [35, Corollary 1.28], the proof of which shows that $F(G)$ is a direct product of its Sylow subgroups, each of which is precisely the p-core of G for each prime p dividing $|G|$. For (ii), we refer to [35, (1D.15)]. To see (iii), note that it follows from (i) that $F(N)$ is characteristic in N, and so $F(N)$ is normal in G and $F(N) \leq N \cap F(G)$. On the other hand, since $F(G)$ is normal in both N and G, the intersection $N \cap F(G)$ is nilpotent and normal in N, hence contained in $F(N)$. □

Theorem 7.1.4 ([43], Lemma 5.4.4)**.** *If G is a nontrivial finite solvable group, then $F = F(G)$ is nontrivial and $C_G(F) = Z(F)$.*

%beginproof

We are now ready to prove a useful result that we use later for our determination of solvable cubefree groups.

Lemma 7.1.5. *If G is a finite solvable group with abelian Fitting subgroup $F = F(G)$, then G/F acts faithfully on F.*

Proof. Since G is solvable, F is nontrivial and normal in G. Thus, there is a well-defined G-action on F via conjugation, and the kernel of such action is $C_G(F)$, which is contained in F by Theorem 7.1.4. Given F is abelian, it follows that $F = C_G(F)$. Thus, there is an induced well-defined action of G/F on F via $\varphi\colon G/F \to \mathrm{Aut}(F)$ via $x^{\varphi(gF)} \mapsto x^g$ for $gF \in G/F$. If gF acts trivially on F, then g centralises F by definition, which implies that $g \in C_G(G) \leq F$ and $gF = F$. Hence, Ker φ is trivial and G/F acts faithfully. □

In the case where G is squarefree, $F(G)$ and G/F are also squarefree, we thus have the following result.

Lemma 7.1.6. *If G is a finite group of squarefree order, then G decomposes into $G = (A \ltimes B) \times C$, where $A \cong G/F(G)$, $F(G) = B \times C$, and $C = Z(G)$; the groups A, B, C are cyclic of pairwise coprime orders.*

Proof. Since G is squarefree, $F = F(G)$ is cyclic and has a complement $A \cong G/F$ in G. The group A is cyclic by Lemma 7.1.5. We know that $Z(G)$ is contained in F and it has an abelian complement in F, thus we can write $F = B \times Z(G)$, where $B \leq F$ is a complement of $Z(G)$ in F and $F/Z(G) \cong B \leq F$, and B is cyclic since it is squarefree. □

In particular, observe that the subgroup B in Lemma 7.1.6 is a normal Hall subgroup of F, thus characteristic in F and normal in G. Moreover, since G is squarefree, $G/B \cong A \times C$ is cyclic and B contains $[G, G]$. The following theorem shows that such a subgroup B coincides with $[G, G]$.

Theorem 7.1.7 ([35], Lemma 4.6)**.** *Let G be a finite group. If A is an abelian normal subgroup of G such that G/B is cyclic. Then $[G, G] = [B, G]$ and $|[G, G]| = |B|/|B \cap Z(G)|$.*

7.1.1 Groups of order pqr

TABLE 7.1: Groups of order pqr with $p < q < r$, using Notation 4.1.1.

Pc-relators	Parameters	Number of types
Cluster 1: abelian		
a^{pqr}		1
Cluster 2: $\lvert Z(G)\rvert \in \{p, q, r\}$		
$a^p, b^q, c^r, b^a / b^{\rho(q,p)}$		Δ^p_{q-1}
$a^p, b^q, c^r, c^a / c^{\rho(r,p)}$		Δ^p_{r-1}
$a^p, b^q, c^r, c^b / c^{\rho(r,q)}$		Δ^q_{r-1}
Cluster 3: $\lvert Z(G)\rvert = 1$		
$a^p, b^q, c^r, b^a / b^{\rho(q,p)}, c^a / c^{\rho(r,p,k)}$	$k \in \mathbb{Z}_p^*$	$(p-1)\Delta^p_{r-1}\Delta^p_{q-1}$
$a^p, b^q, c^r, c^a / c^{\rho(r,p)}, c^b / c^{\rho(r,q)}$		Δ^{qp}_{r-1}

Theorem 7.1.8. *There are $1 + \Delta^p_{q-1} + \Delta^p_{r-1}(1 + (p-1)\Delta^p_{q-1} + \Delta^q_{r-1}) + \Delta^q_{r-1}$ isomorphism types of groups of order pqr with $p < q < r$, each of which has a presentation as encoded in Table 7.1.*

Proof. Theorem A.0.12 shows that an abelian group of order pqr is isomorphic to C_{pqr}, thus it remains to consider the isomorphism types of nonabelian groups of such order. By Lemma 7.1.6 and Theorem 7.1.7, we know that such a group admits a decomposition $G = (A \ltimes B) \times C$, where $C = Z(G)$, $B = [G, G]$, $B \times C = F(G)$, and $A \cong G/F(G)$. In particular, since A acts faithfully on F via conjugation (Lemma 7.1.5), it must also act faithfully on B as it acts trivially on C. Moreover, for any $g \in F(G)$, if $[g, A] = 1$ then $g \in Z(G)$. That is, the split extension $A \ltimes B$ has trivial centre. A squarefree group G is abelian if and only if $C = F(G) = G$. In this case, $G \cong C_{pqr}$. It remains to consider the nonabelian isomorphism types of G. Since G/C is noncyclic for any nonabelian group G, we deduce that $|C| \in \{1, p, q, r\}$. We make a case distinction on the order of C. In the following, we apply Corollary 2.4.3(ii) and Corollary 2.4.6 to explicitly determine the isomorphism types of G.

- If $|C| \in \{p, q, r\}$, then G is uniquely determined by the nonabelian subgroup $H = A \ltimes B$ whose order is a product of two primes, say $H = ab$ where $a < b$ are primes. Lemma 6.1.3 shows that $a \mid (b-1)$ for such a nonabelian H of order ab to exist, and it is unique up to

isomorphism. It follows that G is isomorphic to one of the nonabelian groups:

$$(C_q \ltimes C_r) \times C_p, \quad (C_p \ltimes C_r) \times C_q, \quad (C_p \ltimes C_q) \times C_r,$$

each of which is unique up to isomorphism if it exists, and so there are $\Delta^q_{r-1} + \Delta^p_{r-1} + \Delta^p_{q-1}$ isomorphism types of such groups with cyclic centre of prime order.

- If $|C| = 1$, then $G = A \ltimes B$ with $B = F(G)$. Since $A \cong G/F$ acts faithfully on B, it follows that $A \mid |\mathrm{Aut}(B)|$, and we deduce that $|B| \in \{qr, pr, p, q\}$.
  1. If $B \cong C_{qr}$, then $G \cong A \ltimes C_{qr}$ where $A \cong C_p$ acts nontrivially on both the normal Sylow q- and r-subgroups of G, for otherwise $Z(A \ltimes B) \neq 1$. There are $(p-1)\Delta^p_{r-1}\Delta^p_{q-1}$ normal subgroups of order p in $\mathbb{Z}_q^* \times \mathbb{Z}_r^*$, each of which corresponds to a unique isomorphism type of G by Corollary 2.4.3(ii).
  2. If $B \cong C_{pr}$, then $A \cong C_q$ acts trivially on the Sylow p-subgroup of G since $q > p$, but this implies that $|Z(A \ltimes B)| \geq p$, a contradiction. Thus, this case does not occur.
  3. If $B \cong C_r$, then $A \cong C_{pq}$ and A embeds into $\mathrm{Aut}(B) \cong \mathbb{Z}_r^*$. Such a nonabelian group $G \cong C_{pq} \ltimes C_r$ exists if and only if $\Delta^{pq}_{r-1} = 1$, and is unique up to isomorphism.
  4. If $|B| = q$, then $A \cong C_{pr}$, but there is no faithful action of A on B via conjugation since $r > q$. Thus, such case does not exist.

  In conclusion, there are $(p-1)\Delta^p_{r-1}\Delta^p_{q-1} + \Delta_{r-1}pq$ isomorphism types of nonabelian groups of order pqr such that $Z(G) = 1$.

Combining all cases, the counting formula for the isomorphism types of groups of order pqr follows. For each of the nonabelian isomorphism types (if it exists) we construct a canonical presentation using Notation 4.1.1, the claimed result follows. □

7.1.2 Groups of order $pqrs$

Let G be a group of order $pqrs$. We can apply Lemma 7.1.6 to construct the isomorphism types of G by a case distinction on the sizes of $Z(G)$ and $F(G)$.

Theorem 7.1.9. *Let $p < q < r < s$ be primes. There are*

$$\begin{aligned}
&1+\Delta^s_{r-1} + \Delta^q_{s-1} + \Delta^q_{r-1} + \Delta^p_{s-1} + \Delta^p_{r-1} + \Delta^p_{q-1}\\
&+(q-1)\Delta^q_{s-1}\Delta^q_{r-1} + \Delta^{qr}_{s-1} + (p-1)\Delta^p_{s-1}\Delta^p_{r-1} + \Delta^{pr}_{s-1}\\
&+(p-1)\Delta^p_{s-1}\Delta^p_{q-1} + \Delta^{pq}_{s-1} + (p-1)\Delta^p_{r-1}\Delta^p_{q-1} + \Delta^{pq}_{r-1}\\
&+(p-1)((q-1)\Delta^{pq}_{r-1}\Delta^{pq}_{s-1} + \Delta^{pq}_{r-1}\Delta^p_{s-1} + \Delta^p_{r-1}\Delta^{pq}_{s-1})\\
&+(q-1)(\Delta^{pq}_{r-1}\Delta^q_{s-1} + (q-1)\Delta^q_{r-1}\Delta^{pq}_{s-1}) + \Delta^p_{r-1}\Delta^q_{s-1}\\
&+\Delta^q_{r-1}\Delta^p_{s-1} + \Delta^p_{q-1}\Delta^r_{s-1}(1 + (p-1)\Delta^p_{s-1} + \Delta^{pqr}_{s-1}
\end{aligned}$$

isomorphism types of groups of order $pqrs$, each of which has a presentation as encoded in Table 7.2.

Proof. Theorem A.0.12 shows that an abelian group of order $pqrs$ is isomorphic to C_{pqrs}, thus it remains to consider the isomorphism types of the nonabelian groups of such order. By Lemma 7.1.6 and Theorem 7.1.7 we know that such a group admits a decomposition $G = (A \ltimes B) \times C$, where $C = Z(G)$, $B = [G, G]$, $B \times C = F(G)$, and $A \cong G/F(G)$; this shows that G is determined by the centreless nonabelian direct factor $A \ltimes B$. Since G/C is noncyclic and

TABLE 7.2: Groups of order $pqrs$ with $p < q < r < s$, using Notation 4.1.1.

Pc-relators	Parameters	Number of types
Cluster 1: abelian		
a^{pqrs}		1
Cluster 2: $\lvert Z(G)\rvert \in \{pq, pr, ps, qr, qs, rs\}$		
$a^r, b^s, c^{pq}, b^a / b^{\rho(s,r)}$		Δ^r_{s-1}
$a^q, b^s, c^{pr}, b^a / b^{\rho(s,q)}$		Δ^q_{s-1}
$a^q, b^r, c^{ps}, b^a / b^{\rho(r,q)}$		Δ^q_{r-1}
$a^p, b^s, c^{qr}, b^a / b^{\rho(s,p)}$		Δ^p_{s-1}
$a^p, b^r, c^{qs}, b^a / b^{\rho(r,p)}$		Δ^p_{r-1}
$a^p, b^q, c^{rs}, b^a / b^{\rho(q,p)}$		Δ^p_{q-1}
Cluster 3: $\lvert Z(G)\rvert \in \{p, q, r, s\}$		
$a^{qr}, b^s, c^p, b^a / b^{\rho(s,qr)}$		Δ^{qr}_{s-1}
$a^q, b^r, c^s, d^p, b^a / b^{\rho(r,q)}, c^a / c^{\rho(s,q,k)}$	$k \in \mathbb{Z}_q^*$	$(q-1)\Delta^q_{r-1}\Delta^q_{s-1}$
$a^{pr}, b^s, c^q, b^a / b^{\rho(s,pr)}$		Δ^{pr}_{s-1}
$a^p, b^r, c^s, d^q, b^a / b^{\rho(r,p)}, c^a / c^{\rho(s,p,k)}$	$k \in \mathbb{Z}_p^*$	$(p-1)\Delta^p_{r-1}\Delta^p_{s-1}$
$a^{pq}, b^s, c^r, b^a / b^{\rho(s,pq)}$		Δ^{pq}_{s-1}
$a^p, b^q, c^s, d^r, b^a / b^{\rho(q,p)}, c^a / c^{\rho(s,p,k)}$	$k \in \mathbb{Z}_p^*$	$(p-1)\Delta^p_{q-1}\Delta^p_{s-1}$
$a^{pq}, b^r, c^s, b^a / b^{\rho(r,pq)}$		Δ^{pq}_{r-1}
$a^p, b^q, c^r, d^s, b^a / b^{\rho(q,p)}, c^a / c^{\rho(r,p,k)}$	$k \in \mathbb{Z}_p^*$	$(p-1)\Delta^p_{q-1}\Delta^p_{r-1}$
Cluster 4: $\lvert Z(G)\rvert = 1$		
$a^p, b^q, c^r, d^s, b^a / b^{\rho(q,p)}, c^a / c^{\rho(r,p,k)}, d^a / d^{\rho(s,p,\ell)}$	$(k,\ell) \in \mathbb{Z}_p^{*2}$	$(p-1)^2\Delta^p_{q-1}\Delta^p_{r-1}\Delta^p_{s-1}$
$a^p, b^q, c^r, d^s, c^a / c^{\rho(r,p)}, c^b / c^{\rho(r,q)}, d^a / d^{\rho(s,p,k)}, d^b / d^{\rho(s,q,\ell)}$	$(k,\ell) \in \mathbb{Z}_p^* \times \mathbb{Z}_q^*$	$(p-1)(q-1)\Delta^{pq}_{r-1}\Delta^{pq}_{s-1}$
$a^p, b^q, c^r, d^s, c^a / c^{\rho(r,p,k)}, d^a / d^{\rho(s,p)}, d^b / d^{\rho(s,q)}$	$k \in \mathbb{Z}_p^*$	$(p-1)\Delta^p_{r-1}\Delta^{pq}_{s-1}$
$a^p, b^q, c^r, d^s, c^b / c^{\rho(r,q,k)}, d^a / d^{\rho(s,p)}, d^b / d^{\rho(s,q)}$	$k \in \mathbb{Z}_q^*$	$(q-1)\Delta^q_{r-1}\Delta^{pq}_{s-1}$
$a^p, b^q, c^r, d^s, c^a / c^{\rho(r,p)}, c^b / c^{\rho(r,q)}, d^a / d^{\rho(s,p,k)}$	$k \in \mathbb{Z}_p^*$	$(p-1)\Delta^{pq}_{r-1}\Delta^p_{s-1}$
$a^p, b^q, c^r, d^s, c^a / c^{\rho(r,p)}, c^b / c^{\rho(r,q)}, d^a / d^{\rho(s,q,k)}$	$k \in \mathbb{Z}_q^*$	$(q-1)\Delta^{pq}_{r-1}\Delta^q_{s-1}$
$a^p, b^q, c^r, d^s, c^a / c^{\rho(r,p)}, d^b / d^{\rho(s,q)}$		$\Delta^p_{r-1}\Delta^q_{s-1}$
$a^p, b^q, c^r, d^s, c^b = c^{\rho(r,p)}, d^a = d^{\rho(s,p)}$		$\Delta^q_{r-1}\Delta^p_{s-1}$
$a^p, b^q, c^r, d^s, b^a = b^{\rho(q,p)}, d^c = d^{\rho(s,r)}$		$\Delta^p_{q-1}\Delta^r_{s-1}$
$a^p, b^q, c^r, d^s, b^a / b^{\rho(q,p,k)}, d^a / d^{\rho(s,p)}, d^c / d^{\rho(s,r)}$	$k \in \mathbb{Z}_p^*$	$(p-1)\Delta^{pr}_{s-1}\Delta^p_{q-1}$
$a^{pqr}, b^s, b^a = b^{\rho(s,pqr)}$		Δ^{pqr}_{s-1}

$C < F(G) < G$, it follows that $|C| \in \{1, p, q, r, s, pq, pr, ps, qr, qs, rs\}$. We make a case distinction on the order of C in the determination of isomorphism types of G. Moreover, since A and B are both cyclic and have coprime orders, we apply Corollary 2.4.3(ii) and Corollary 2.4.6 upon construction of such groups.

- If $|C| \in \{pq, pr, ps, qr, qs, rs\}$, then $G \cong (A \ltimes B) \times C$ is uniquely determined by the nonabelian subgroup whose order is a product of two distinct primes. It follows by Lemma 6.1.3 that there is a unique isomorphism type for each of the following nonabelian isomorphism types (if they exist) of G:

$$(C_r \ltimes C_s) \times C_{pq}, \quad (C_q \ltimes C_s) \times C_{pr}, \quad (C_q \ltimes C_r) \times C_{ps},$$

$$(C_p \ltimes C_s) \times C_{qr}, \quad (C_p \ltimes C_r) \times C_{qs}, \quad (C_p \ltimes C_q) \times C_{rs}.$$

  In other words, there are $\Delta^s_{r-1} + \Delta^q_{s-1} + \Delta^q_{r-1} + \Delta^p_{s-1} + \Delta^p_{r-1} + \Delta^p_{q-1}$ isomorphism types of G such that $|Z(G)|$ is a product of two distinct primes.

- If $|C| \in \{p, q, r, s\}$, then $G = H \times C$ is uniquely determined by the centreless direct factor $H = A \ltimes B$ whose order is a product of three distinct primes. In particular, such groups

are determined in Lemma 7.1.8. Therefore, there are

$$\begin{aligned}&(q-1)\Delta^q_{s-1}\Delta^q_{r-1}+\Delta^{qr}_{s-1}\\+&(p-1)\Delta^p_{s-1}\Delta^p_{r-1}+\Delta^{pr}_{s-1}\\+&(p-1)\Delta^p_{s-1}\Delta^p_{q-1}+\Delta^{pq}_{s-1}\\+&(p-1)\Delta^p_{r-1}\Delta^p_{q-1}+\Delta^{pq}_{r-1}\end{aligned}$$

isomorphism types of G such that $Z(G)$ is cyclic of prime order, each of which is of the form $H \times Z(G)$, where H has a pc-presentation whose pc-relators are listed in Cluster 3 in Table 7.1 with appropriate relative orders.

- If $|C| = 1$, then $G \cong A \ltimes B$, where A acts faithfully on $B = F(G)$, which implies that $|B| \notin \{1, p, q, r, pq, pr, qr, pqr\}$, for otherwise $|A| \nmid |\mathrm{Aut}(B)|$ and there are no faithful A-actions on B. On the other hand, A must act nontrivially on all nontrivial Sylow subgroups of B, for otherwise $A \ltimes B$ has a nontrivial centre, hence $|B| \notin \{ps, pqs, prs\}$. We consider $|B| \in \{s, qs, rs, qrs\}$.
  1. If $|B| = qrs$, then $G \cong C_p \ltimes C_{qrs}$. Since $A \cong C_p$ acts nontrivially on all nontrivial Sylow subgroups of $B \cong C_{qrs}$, it follows that p divides each of $(q-1)$, $(r-1)$, and $(s-1)$. In particular, there are $(p-1)^2\Delta^p_{q-1}\Delta^p_{r-1}\Delta^p_{s-1}$ isomorphism types of such G in one-to-one correspondence with the cyclic normal subgroups of order p in $\mathrm{Aut}(B) \cong \mathbb{Z}_q^* \times \mathbb{Z}_r^* \times \mathbb{Z}_s^*$.
  2. If $|B| = rs$, then $G \cong C_{pq} \ltimes C_{rs}$ and $A \cong C_{pq}$ embeds into $\mathrm{Aut}(B)$. Then by Corollary 2.4.3(ii), the isomorphism types of such split extensions are in bijection with the cyclic normal subgroups of order pq in $\mathrm{Aut}(B) \cong \mathbb{Z}_r^* \times \mathbb{Z}_s*$: there are

$$\begin{aligned}&(p-1)(q-1)\Delta^{pq}_{r-1}\Delta^{pq}_{s-1}\\+&(p-1)\Delta^{pq}_{r-1}\Delta^{p}_{s-1}\\+&(p-1)\Delta^{p}_{r-1}\Delta^{pq}_{s-1}\\+&(q-1)\Delta^{pq}_{r-1}\Delta^{q}_{s-1}\\+&(q-1)\Delta^{q}_{r-1}\Delta^{pq}_{s-1}\\+&\Delta^{p}_{r-1}\Delta^{q}_{s-1}+\Delta^{q}_{r-1}\Delta^{p}_{s-1}\end{aligned}$$

     isomorphism types in this case.
  3. If $|B| = qs$, then $A \cong C_{pr}$. Since $r > q$, the Sylow r-subgroup acts trivially on the normal Sylow q-subgroup of B, thus it acts nontrivially on the normal Sylow s-subgroup of B, for otherwise the action of A is nonfaithful. On the other hand, the Sylow p-subgroup of A must act nontrivially on the Sylow q-subgroup of B, for otherwise the centre of $A \ltimes B$ has nontrivial centre. It follows that $r \mid (s-1)$ and $p \mid (q-1)$. Now there are two cases dependent on whether the Sylow p-subgroup acts nontrivially on the Sylow r subgroup of B:
     (a) If the Sylow p-subgroup of A acts trivially on the Sylow r-subgroup of B, then $G \cong (C_p \ltimes C_q) \times (C_r \ltimes C_s)$, which is determined by the nonabelian direct factors $C_p \ltimes C_q$ and $C_r \ltimes C_s$. By Lemma 6.1.3, there are $\Delta^p_{q-1}\Delta^r_{s-1}$ isomorphism types in this case.
     (b) If the Sylow p-subgroup of A acts nontrivially on the Sylow r-subgroup of B, then $p \mid (r-1)$, and $G \cong C_{pr} \ltimes C_{qs}$. Corollary 2.4.3(ii) shows that the isomorphism types of such split extensions are in bijection with the cyclic nor-

mal subgroups of order pr in $\mathrm{Aut}(B) \cong \mathbb{Z}_q^* \times \mathbb{Z}_s^*$. In particular, there are $(p-1)\Delta_{s-1}^{pr}\Delta_{q-1}^{p}$ such isomorphism types.

In total, we find $\Delta_{q-1}^{p}\Delta_{s-1}^{r}(1+(p-1)\Delta_{s-1}^{p})$ isomorphism types of such groups with trivial centre and cyclic Fitting subgroup of order qs.

4. If $|B| = s$, then $G \cong C_{pqr} \ltimes C_s$. A faithful action of $A \cong C_{pqr}$ on $B \cong C_s$ requires that $pqr \mid (s-1)$, in which case there is a unique normal subgroup of order pqr in $\mathbb{Z}_s^*$. Therefore, there are Δ_{s-1}^{pqr} isomorphism types of such groups in this case.

Combining all of the cases above, the number of isomorphism types of groups of order $pqrs$ follows. For each of the nonabelian isomorphism types, if it exists, we determine a presentation using the canonical automorphisms defined in Notation 4.1.1, the claimed result follows. □

7.2 Groups of order p^2qr

Without loss of generality, let $q < r$. The enumeration of isomorphism types of the groups of order p^2qr is given in [24] and discussed in [37]. Such groups can be constructed by applying the algorithm in [19] since they are of cubefree order. In this section, we explicitly determine the isomorphism class representatives of these groups, which leads to an identification function that is not covered by [19]. Our explicit construction directly results in a counting formula, which agrees with the results in [24].

Note that all nilpotent groups of such order are classified by Theorem A.0.12, since all Sylow subgroups of a group of order p^2qr are abelian. We are left to determine all the isomorphism types of non-nilpotent groups. In particular, all groups of order p^2qr are solvable with only one exception, namely, Alt_5. Thus, it remains to classify the solvable non-nilpotent groups. Inspired by the approach adopted in [24], we explicitly construct the isomorphism types by making a case distinction on the structure of the Fitting subgroup.

From now on, let G exclusively denote a nonabelian group of order p^2qr with $q < r$. If G is solvable, then it has a nontrivial Fitting subgroup F. Moreover, since F is cubefree and nilpotent, it is abelian. Then Lemma 7.1.5 shows that G/F embeds into $\mathrm{Aut}(F)$. We construct and classify all isomorphism types of groups of order p^2qr accordingly.

7.2.1 Summary of results

TABLE 7.3: Groups of order p^2qr with $r > q$, using Notations 4.1.1, 4.2.1, and 4.2.6.

PC-relators	Parameters	Number of groups
Cluster 1: $F = G$		
a^{p^2qr}		1
a^p, b^{pqr}		1
Cluster 2: $\lvert F\rvert = r$		
$a^{p^2q}, b^r, b^a / b^{\rho(r,p^2q)}$		$\Delta_{r-1}^{p^2q}$
Cluster 3: $\lvert F\rvert = qr$		
$a^{p^2}, b^q, c^r, b^a / b^{\rho(q,p^2)}$		$\Delta_{q-1}^{p^2}$
$a^{p^2}, b^q, c^r, b^a / b^{\rho(q,p^2)}, c^a / c^{\rho(r,p,k)}$	$k \in \mathbb{Z}_p^*$	$(p-1)\Delta_{q-1}^{p^2}\Delta_{r-1}^{p}$
$a^{p^2}, b^q, c^r, b^a / b^{\rho(q,p^2)}, c^a / c^{\rho(r,p^2,k)}$	$k \in \mathbb{Z}_{p^2}^*$	$(p^2-p)\Delta_{r-1}^{p^2}\Delta_{q-1}^{p^2}$

$a^{p^2}, b^q, c^r, c^a/c^{\rho(r,p^2)}$		$\Delta_{r-1}^{p^2}$
$a^{p^2}, b^q, c^r, b^a/b^{\rho(q,p)}, c^a/c^{\rho(r,p^2,k)}$,	$k \in \mathbb{Z}_p^*$	$(p-1)\Delta_{r-1}^{p^2}\Delta_{q-1}^{p}$
$a^p, b^p, c^q, d^r, c^a/c^{\rho(q,p)}, d^b/d^{\rho(r,p)}$		$\Delta_{q-1}^{p}\Delta_{r-1}^{p}$
Cluster 4: $\lvert F\rvert = p^2$		
$a^{qr}, b^{p^2}, b^a/b^{\rho(p^2,qr)}$		Δ_{p-1}^{qr}
$a^q, b^r, c^p, d^p, c^a/c^{\rho(p,q)}, d^b/d^{\rho(p,r)}$		Δ_{p-1}^{qr}
$a^q, b^r, c^p, d^p, c^a/c^{\rho(p,q)}, c^b/c^{\rho(p,r)}$		Δ_{p-1}^{qr}
$a^q, b^r, c^p, d^p, (c^a, d^a)/(c,d)^{M(p,q,k)}, c^b/c^{\rho(p,r)}$	$k \in \mathbb{Z}_q^*$	$(q-1)\Delta_{p-1}^{qr}$
$a^q, b^r, c^p, d^p, c^a/c^{\rho(p,q)}, (c^b, d^b)/(c,d)^{M(p,r,k)}$	$k \in \mathbb{Z}_r^*$	$(r-1)\Delta_{p-1}^{qr}$
$a^q, b^r, c^p, d^p, (c^a, d^a)/(c,d)^{M(p,q,\sigma_q^k)}, (c^b, d^b)/(c,d)^{M(p,r,\sigma_r^\ell)}$	$(k,\ell) \in \mathcal{P}_1$	$\frac{1}{2}(qr-q-r+5-2\Delta_q^2)\Delta_{p-1}^{qr}$
$a^2, b^r, c^p, d^p, b^a/b^{-1}, (c^a, d^a)/(d,c), (c^b, d^b)/(c,d)^{M(p,r,r-1)}$		$\Delta_q^2\Delta_{p-1}^{r}$
$a^{qr}, b^p, c^p, (b^a, c^a)/(b,c)^{\mathrm{Irr}_2(p,qr)}$		$(1-\Delta_q^2)\Delta_{p+1}^{qr}$
$a^q, b^r, c^p, d^p, (c^a, d^a)/(c,d)^{M(p,q)}, (c^b, d^b)/(c,d)^{\mathrm{Irr}_2(p,r)}$		$\Delta_{p-1}^{q}\Delta_{p+1}^{r}$
$a^2, b^r, c^p, d^p, b^a/b^{-1}, (c^a, d^a)/(d,c), (c^b, d^b)/(c,d)^{\mathrm{Irr}_2(p,r)}$		$\Delta_q^2\Delta_{p+1}^{r}$
$a^q, b^r, c^p, d^p, (c^a, d^a)/(c,d)^{\mathrm{Irr}_2(p,q)}, (c^b, d^b)/(c,d)^{M(p,r)}$		$(1-\Delta_q^2)\Delta_{p+1}^{q}\Delta_{p-1}^{r}$
Cluster 5: $\lvert F\rvert = p^2q$		
$a^r, b^{p^2}, c^q, b^a/b^{\rho(p^2,r)}$		Δ_{p-1}^{r}
$a^r, b^p, c^p, d^q, b^a/b^{\rho(p,r)}$		Δ_{p-1}^{r}
$a^r, b^p, c^p, d^q, (b^a, c^a)/(b,c)^{M(p,r,\sigma_r^k)}$	$0 \le k \le \frac{1}{2}(r-1)$	$\frac{1}{2}(r+1)\Delta_{p-1}^{r}$
$a^r, b^p, c^p, d^q, (b^a, c^a)/(b,c)^{\mathrm{Irr}_2(p,r)}$		Δ_{p+1}^{r}
Cluster 6: $\lvert F\rvert = p^2r$		
$a^q, b^r, c^{p^2}, b^a/b^{\rho(r,q)}$		Δ_{r-1}^{q}
$a^q, b^r, c^{p^2}, c^a/c^{\rho(p^2,q)}$		Δ_{p-1}^{q}
$a^q, b^r, c^{p^2}, b^a/b^{\rho(r,q,k)}, c^a/c^{\rho(p^2,q)}$	$k \in \mathbb{Z}_q^*$	$(q-1)\Delta_{r-1}^{q}\Delta_{p-1}^{q}$
$a^q, b^r, c^p, d^p, c^a/c^{\rho(p,q)}$		Δ_{p-1}^{q}
$a^q, b^r, c^p, d^p, (c^a, d^a)/(c,d)^{M(p,q,\sigma_q^k)}$	$0 \le k \le \frac{1}{2}(q-1)$	$\frac{1}{2}(q+1-\Delta_q^2)\Delta_{p-1}^{q}$
$a^q, b^r, c^p, d^p, (c^a, d^a)/(c,d)^{\mathrm{Irr}_2(p,q)}$		Δ_{p+1}^{q}
$a^q, b^r, c^p, d^p, b^a/b^{\rho(r,q)}$		Δ_{r-1}^{q}
$a^q, b^r, c^p, d^p, b^a/b^{\rho(r,q)}, c^a/c^{\rho(p,q,k)}$	$k \in \mathbb{Z}_q^*$	$(q-1)\Delta_{r-1}^{q}\Delta_{p-1}^{q}$
$a^q, b^r, c^p, d^p, b^a/b^{\rho(r,q,\sigma_q^\ell)}, (c^a, d^a)/(c,d)^{M(p,q,\sigma_q^k)}$	$(k,\ell) \in \mathcal{P}_2$	$\frac{1}{2}q(q-1-\Delta_q^2)\Delta_{r-1}^{q}\Delta_{p-1}^{q}$
$a^2, b^r, c^p, d^p, b^a/b^{-1}, c^a/c^{-1}, d^a/d^{-1}$		Δ_q^2
$a^q, b^r, c^p, d^p, b^a/b^{\rho(r,q)}, (c^a, d^a)/(c,d)^{(\mathrm{Irr}_2(p,q)^k)}$	$1 \le k \le \frac{1}{2}(q-1)$	$\frac{1}{2}(q-1-\Delta_q^2)\Delta_{r-1}^{q}\Delta_{p+1}^{q}$
Cluster 7: $\lvert F\rvert = pr$		
$a^q, b^p, c^p, d^r, d^a/d^{\rho(r,q)}, d^b/d^{\rho(r,p)}$		Δ_{r-1}^{pq}
$a^q, b^{p^2}, c^r, c^a/c^{\rho(r,q)}, c^b/c^{\rho(r,p)}$		Δ_{r-1}^{pq}
$a^q, b^p, c^p, d^r, c^a/d^{\rho(p,q)}, d^b/d^{\rho(r,p)}$		$\Delta_{r-1}^{p}\Delta_{p-1}^{q}$
$a^q, b^p, c^p, d^r, c^a/d^{\rho(p,q,k)}, d^a/d^{\rho(r,q)}, d^b/d^{\rho(r,p)}$	$k \in \mathbb{Z}_q^*$	$(q-1)\Delta_{r-1}^{pq}\Delta_{p-1}^{q}$
Cluster 8: $\lvert F\rvert = pqr$		
$a^{p^2}, b^q, c^r, c^a/c^{\rho(r,p)}$		Δ_{r-1}^{p}
$a^{p^2}, b^q, c^r, b^a/b^{\rho(q,p)}$		Δ_{q-1}^{p}
$a^{p^2}, b^q, c^r, b^a/b^{\rho(q,p)}, c^a/c^{\rho(r,p,k)}$	$k \in \mathbb{Z}_p^*$	$(p-1)\Delta_{r-1}^{p}\Delta_{q-1}^{p}$
$a^p, b^p, c^q, d^r, d^a/d^{\rho(r,p)}$		Δ_{r-1}^{p}
$a^p, b^p, c^q, d^r, c^a/c^{\rho(q,p)}$		Δ_{q-1}^{p}
$a^p, b^p, c^q, d^r, c^a/c^{\rho(q,p)}, d^a/d^{\rho(r,p,k)}$	$k \in \mathbb{Z}_p^*$	$(p-1)\Delta_{r-1}^{p}\Delta_{q-1}^{p}$
Cluster 9: $F = 1$		
Alt_5 (not solvable)		$\Delta_p^2\Delta_q^3\Delta_r^5$

Parameter sets

$\mathcal{P}_1 = \{(x,y)\colon 0 \le x \le \frac{1}{2}(q-1),\ 0 \le y \le \frac{1}{2}(r-1)\} \cup \{(x,y)\colon 1 \le x \le \frac{1}{2}(q-3),\ \frac{1}{2}(r+1) \le y \le r-2\}$

$\mathcal{P}_2 = \{(x,0)\colon 0 \le x \le \frac{1}{2}(q-3)\} \cup \{(x,y)\colon 0 \le x \le \frac{1}{2}(q-1),\ 1 \le y \le \frac{1}{2}(q-3)\} \cup \{(\frac{1}{2}(q-1), \frac{1}{2}(q-1))\}$
$\cup \{(x,y)\colon 0 \le x \le \frac{1}{2}(q-3),\ \frac{1}{2}(q-1) \le y \le q-2\}$

Theorem 7.2.1. *Let p, q, r be distinct primes and $r > q$. Then there are*

$$\begin{aligned}
&2 + \Delta_{r-1}^{p^2q} + \Delta_{q-1}^{p^2}(1 + (p-1)\Delta_{r-1}^{p} + (p^2-p)\Delta_{r-1}^{p^2}) \\
&\quad + \Delta_{r-1}^{p^2}(1 + (p-1)\Delta_{q-1}^{p}) + \Delta_{r-1}^{p}\Delta_{q-1}^{p} \\
&\quad + \frac{1}{2}(qr+q+r+7)\Delta_{p-1}^{qr} + (1-\Delta_{p-1}^{qr})(1-\Delta_q^2)\Delta_{p^2-1}^{qr} \\
&\quad + 2\Delta_{p+1}^{r}\Delta_q^2 + \frac{1}{2}(r+5)\Delta_{p-1}^{r} + \Delta_{p+1}^{r} + 8\Delta_q^2 \\
&\quad + (1-\Delta_q^2)(\frac{1}{2}(q-1)(q+4)\Delta_{p-1}^{q}\Delta_{r-1}^{q} + \frac{1}{2}(q-1)\Delta_{p+1}^{q}\Delta_{r-1}^{q} \\
&\quad + \frac{1}{2}(q+5)\Delta_{p-1}^{q} + 2\Delta_{r-1}^{q} + \Delta_{p+1}^{q}) \\
&\quad + \Delta_{r-1}^{p}(\Delta_{p-1}^{q}(1 + (q-1)\Delta_{r-1}^{q}) + 2\Delta_{r-1}^{q}) \\
&\quad + 2(\Delta_{q-1}^{p} + \Delta_{r-1}^{p} + (p-1)\Delta_{q-1}^{p}\Delta_{r-1}^{p}) + \Delta_p^2\Delta_q^3\Delta_r^5
\end{aligned}$$

isomorphism types of groups of order p^2qr, and each of the solvable ones has a presentation as encoded in Table 7.3; a group of such order is nonsolvable if and only if it is isomorphic to Alt_5.

7.2.2 Determination of groups of order p^2qr

Firstly, note that there is a unique isomorphism type of nonsolvable groups of order p^2qr.

Lemma 7.2.2. *If G is a nonsolvable group of order p^2qr, then $G \cong \mathrm{Alt}_5$.*

Proof. If G is a nonsolvable group of order p^2qr, then G is simple. To see this, suppose N is a proper nontrivial normal subgroup of G. Since all squarefree groups and groups of order p^aq^b are solvable, N and G/N are solvable, which implies that G is solvable, a contradiction. Recall that we assume $r > q$. As a consequence of [15, Theorem II, §243] (also known as *Burnside's normal p-complement theorem* or *Burnside's transfer theorem*), if $q < p$, then G has a normal q-complement, a contradiction. Thus, we deduce that $p < qr$. Further, let $P \in \mathrm{Syl}_p(G)$, then P is abelian of order p^2. Since P is not normal in G and $P \leq C_G(P) \leq N_G(P)$, we deduce that $|N_G(P)| = p^2q$: if $|N_G(P)| = p^2qr$ then it implies that $P \lhd G$; if $|N_G(P)| = p^2$ then $N_G(P) = P = C_G(P)$, and it follows from Burnside's transfer theorem that G has a normal p-complement. Let $C = C_G(P), N = N_G(P)$, and $Q \in \mathrm{Syl}_q(G)$. Then $Q \in \mathrm{Syl}_q(N)$, since $|Q| = q$. Since $|N\colon C| > 1$, for otherwise G has a normal p-complement by Burnside's theorem, it follows that $|N\colon C| = q$, but we also know that N/C embeds into $\mathrm{Aut}(P)$, which has order $p(p-1)$ if P is cyclic, or $p(p-1)^2(p+1)$ if P is elementary abelian. This implies that $q \mid (p+1)$ or $q \mid (p-1)$. Since $p < q$, in particular, $q > 2$, we have that $q \mid (p+1)$, which forces that $q = 3$ and $p = 2$. Applying Sylow theorems, we deduce that the number of Sylow r-subgroups is 6, and $r = 5$. In other words, $|G| = 60$. It remains to show that $G \cong \mathrm{Alt}_5$, which can be directly verified using the SmallGroups Library of GAP [27]. Alternatively, we include a brief theoretical argument here: note that $PQ \leq G$ has order 12, and it does not contain a normal 3-subgroup. Lemma 6.1.4 shows that this group is isomorphic to Alt_4. That is, G contains a subgroup $PQ \cong \mathrm{Alt}_4$ with index $[G : PQ] = 5$. Since G is simple, G acts on the set of cosets of PQ faithfully, implying that G embeds into Sym_5. Let $A = \mathrm{Alt}_5$ and $S = \mathrm{Sym}_5$. Then $A \lhd S$, if

$G \cong H \leq S$, then $A \cap H \lhd H$. It follows that $A \cap H \in \{1, H\}$ as H is simple. However, since $H/(A \cap H) \cong HA/A \leq S/A \cong C_2$, it follows that $HA/A = 1$ and $A \cap H = H$, which implies that $G \cong H = A \cong \mathrm{Alt}_5$. □

We now prove Theorem 7.2.1.

Proof of Theorem 7.2.1. Lemma 7.2.2 shows that a group of order p^2qr is nonsolvable if and only if it is isomorphic to Alt_5. Thus, we are left to determine the isomorphism types nonabelian solvable groups of such order. Such a group G has nontrivial Fitting subgroup. Thus we make a case distinction on the order of $F = F(G)$ in the following discussion. In particular, $|F| = |G|$ if and only if G is abelian, and the isomorphism types of F is determined by the Sylow subgroup; if $\gcd(|F|, |G/F|) = 1$, then $G \cong G/F \ltimes F$ is a split extension where G/F acts faithfully on F by Lemma 7.1.5. This implies that if $|F| \in \{q, r, qr, p^2, p^2q, p^2r\}$, then G is isomorphic to a nonabelian semidirect product $G/F \ltimes F$. In this case, we apply Theorem 2.4.2(ii) and the subsequent corollaries discussed in Section 2.4 to determine the isomorphism types. The cases where $|F| \in \{p, pq, pr, pqr\}$ are dealt with separately. Together, we obtain the claimed result in Theorem 7.2.1 as follows.

1. If $|F| = q$, then G/F is cyclic of order p^2r since $\mathrm{Aut}(F) \cong \mathbb{Z}_q^*$ is cyclic. It follows that $G \cong C_{p^2r} \ltimes C_q$ and $p^2r \mid (q-1)$, which is impossible since $q < r$. Thus, there exists no such group.

2. If $|F| = r$, then G/F is cyclic of order p^2q since $\mathrm{Aut}(F) \cong \mathbb{Z}_r^*$ is cyclic. It follows that $G \cong C_{p^2q} \ltimes C_r$ and $p^2q \mid (r-1)$. Since the isomorphism types of such metacyclic extensions are enumerated by the number of conjugacy classes of groups of order p^2q in $\mathbb{Z}_r^*$ (Corollary 2.4.3(ii)) and there are $\Delta_{r-1}^{p^2q}$ isomorphism types of such groups. In particular, G is isomorphic to
$$\mathrm{Pc}\langle a, b \mid a^{p^2q}, b^r, b^a = b^{\rho(r, p^2q)}\rangle.$$

3. If $|F| = qr$, then $F \cong C_q \times C_r$ and $\mathrm{Aut}(F) \cong \mathbb{Z}_q^* \times \mathbb{Z}_r^*$. It follows that G/F is abelian of order p^2 and $p^2 \mid (q-1)(r-1)$. There are two cases to consider.
   (a) If $G/F \cong C_{p^2}$, then $p^2 \mid (q-1)$ or $p^2 \mid (r-1)$, for otherwise there is no faithful action of G/F on F. Moreover, from Corollary 2.4.3(ii) it follows that the number of isomorphism types of G coincides with the number of normal subgroups of order p^2 in $\mathrm{Aut}(F) \cong \mathbb{Z}_q^* \times \mathbb{Z}_r^*$. Note that if p^2 divides both $q-1$ and $r-1$, then there are $p^2 + p$ normal cyclic subgroups of order p^2 in $\mathrm{Aut}(F)$; if $\Delta_{q-1}^{p^2}\Delta_{r-1}^{p} = 1$ and $\Delta_{r-1}^{p^2} = 0$ then there are p such subgroups in $\mathrm{Aut}(F)$. Dual to the preceding case, if $\Delta_{r-1}^{p^2}\Delta_{q-1}^{p} = 1$ and $\Delta_{q-1}^{p^2} = 0$, then there are also p such subgroups in $\mathrm{Aut}(F)$. Also, if $\Delta_{q-1}^{p}\Delta_{r-1}^{p} = 0$ but $\Delta_{q-1}^{p^2} = 1$ or $\Delta_{r-1}^{p^2} = 1$, then there is a unique normal subgroup of order p^2 in $\mathrm{Aut}(F)$. Lastly, note that since F is abelian and characteristic in G, all Sylow q- and r-subgroups of G are normal. Upon the construction of such nonabelian metacyclic split extensions $G \cong C_{p^2} \ltimes C_{qr}$ by exhausting all possible canonical C_{p^2}-actions on C_{qr} as described in Notation 4.1.1, we apply Corollary 2.4.3 and obtain a complete and irredundent list of isomorphism types of G as follows:
      - If $p^2 \mid (q-1)$, then there are
$$\Delta_{q-1}^{p^2}(1 + (p-1)\Delta_{r-1}^{p} + (p^2-p)\Delta_{r-1}^{p^2})$$

isomorphism types of such groups with isomorphism class representatives

$$\begin{aligned}&\mathrm{Pc}\langle a,b,c \mid a^{p^2}, b^q, c^r, b^a = b^{\rho(q,p^2)}\rangle,\\ &\mathrm{Pc}\langle a,b,c \mid a^{p^2}, b^q, c^r, b^a = b^{\rho(q,p^2)}, c^a = c^{\rho(r,p,k)}\rangle,\\ &\mathrm{Pc}\langle a,b,c \mid a^{p^2}, b^q, c^r, b^a = b^{\rho(q,p^2)}, c^a = c^{\rho(r,p^2,\ell)}\rangle,\end{aligned}$$

where $k \in \mathbb{Z}_p^*$ and $\ell \in \mathbb{Z}_{p^2}^*$.

- If $p^2 \nmid (q-1)$, then $p^2 \mid (r-1)$ and there are $\Delta_{r-1}^{p^2}(1+(p-1)\Delta_{q-1}^{p})$ isomorphism types of such groups with isomorphism class representatives

$$\begin{aligned}&\mathrm{Pc}\langle a,b,c \mid a^{p^2}, b^r, c^q, b^a = b^{\rho(r,p^2)}\rangle,\\ &\mathrm{Pc}\langle a,b,c \mid a^{p^2}, b^q, c^r, b^a = b^{\rho(q,p,k)}, c^a = c^{\rho(r,p^2)}\rangle,\end{aligned}$$

where $k \in \mathbb{Z}_p^*$.

(b) If $G/F \cong C_p^2$, then $p \mid (q-1)$ and $p \mid (r-1)$ since there are $\Delta_{q-1}^{p}\Delta_{r-1}^{p}$ normal elementary abelian subgroups of order p^2 in $\mathrm{Aut}(F)$. Thus, there is a unique non-abelian isomorphism type $(C_p \ltimes C_q) \times (C_p \ltimes C_r)$ with presentation

$$\mathrm{Pc}\langle a,b,c,d \mid a^p, b^p, c^q, d^r, c^a = c^{\rho(q,p)}, d^b = d^{\rho(r,p)}\rangle.$$

4. If $|F| = p^2$, then G/F is of order qr.

(a) If $F \cong C_{p^2}$, then $\mathrm{Aut}(F)$ is cyclic of order $p(p-1)$. It follows that $qr \mid (p-1)$. Since there are Δ_{p-1}^{qr} normal cyclic subgroups of order p^2 in $\mathrm{Aut}(F)$, Corollary 2.4.3(ii) implies that there is a unique isomorphism type in this case, namely,

$$\mathrm{Pc}\langle a,b \mid a^{qr}, b^{p^2}, b^a = b^{\rho(p^2,qr)}\rangle.$$

(b) If $F \cong C_p^2$, then G/F embeds into $\mathrm{Aut}(F) \cong \mathrm{GL}_2(p)$ and $qr \mid (p^2-1)$. If $q > 2$, then either $q \mid (p-1)$ or $q \mid (p+1)$, likewise either $r \mid (p-1)$ or $r \mid (p+1)$. If $q = 2$, then $2r \mid (p^2-1)$ and $2r \nmid (p-1)$ if and only if $r \mid (p+1)$.

- If $qr \mid (p-1)$ and $q > 2$, then $q \nmid (p+1), r \nmid (p+1)$. We claim that there exists no faithful action of a nonabelian group of order qr on C_p^2, then it will be sufficed to consider $G/F \cong C_{qr}$. Suppose for contradiction that $G/F \cong C_q \ltimes C_r$ is nonabelian, in which case G is isomorphic to $(C_q \ltimes C_r) \ltimes C_p^2$, with a Sylow q-subgroup that acts nontrivially on a Sylow r-subgroup. Since a subgroup of order $qr \mid (p-1)$ is reducible in $\mathrm{GL}_2(p)$, it suffices to consider the presentation of G of the following form:

$$\mathrm{Pc}\langle a,b,c,d \mid a^q, b^r, c^p, d^p, b^a = b^\delta, c^a = c^{s_1}, d^a = d^{s_2}, c^b = c^{t_1}, d^b = d^{t_2}\rangle,$$

where $\delta \in \mathbb{Z}_r^*$ has order q, and for each $i \in \{1,2\}$ we have $s_i^q \equiv t_i^r \equiv 1 \bmod p$. For such a pc-presentation to be consistent, it is required that $c^{(b^a)} = c^{(b^\delta)}$: the left-hand side collects to c^{s_2}, and the right-hand side collects to $c^{(s_2^\delta)}$, forcing $\delta = 1$, which contradicts the assumption that $\langle a,b\rangle$ is nonabelian. Therefore, if $q > 2$ and $qr \mid (p-1)$, the isomorphism types of such G are split extensions $C_{qr} \ltimes C_p^2$.
By Corollary 2.4.3, the isomorphism types of such groups are characterised by the conjugacy class representatives of reducible cyclic subgroups of order qr

in $\mathrm{Aut}(P) \cong \mathrm{GL}_2(p)$. Proceeding from the proof of Theorem 4.2.7(iii), we explicitly construct the isomorphism class representatives of such groups. Let $P \in \mathrm{Syl}_p(G), Q \in \mathrm{Syl}_q(G)$, and $R \in \mathrm{Syl}_r(G)$ be Sylow subgroups of G. Since P is normal in G, we know PQ and PR are subgroups of G. If $Z(PQ) \cong Z(PR) \cong C_p$, then $G \cong (C_q \ltimes C_p) \times (C_r \ltimes C_p)$, which is unique up to isomorphism and exists if and only if $\Delta^p_{q-1}\Delta^p_{r-1} = 1$. If $Z(PQ) = 1$ and $Z(PR) \cong C_p$, then R acts trivially on a nontrivial subgroup of P whereas Q acts nontrivially on all nontrivial subgroups of P. That is, G/F acts on one of the nontrivial subgroups C_p in F via an automorphism of order q. There are $(q-1)\Delta^p_{q-1}\Delta^p_{r-1}$ isomorphism types with presentations

$$\mathrm{Pc}\langle a,b,c,d \mid a^q, b^r, c^p, d^p, c^a = c^{\rho(p,q)}, c^b = c^{\rho(p,r)}, d^a = d^{\rho(p,q,k)}\rangle,$$

parametrised by $k \in \mathbb{Z}_q^*$. Dual to the preceding case, if $Z(PQ) \cong C_p$ and $Z(PR) = 1$, then G/F acts on one generator of F via an automorphism of order r. There are $(r-1)\Delta^p_{q-1}\Delta^p_{r-1}$ isomorphism types of such groups, with presentations

$$\mathrm{Pc}\langle a,b,c,d \mid a^q, b^r, c^p, d^p, c^a = c^{\rho(p,q)}, c^b = c^{\rho(p,r)}, d^b = d^{\rho(p,r,\ell)}\rangle,$$

parametrised by $\ell \in \mathbb{Z}_r^*$.
If G/F acts on all nontrivial subgroups of F via an automorphism of order qr, then the isomorphism types of these groups are constructed using the conjugacy class representatives of cyclic diagonalisable subgroups of order qr in $\mathrm{GL}_2(p)$ as discussed in Theorem 4.2.7(ii). In particular, there are $\frac{1}{2}(qr-q-r+5)\Delta_{q-1}\Delta_{r-1}$ isomorphism types in this case, with presentations

$$\begin{aligned}\mathrm{Pc}\langle a,b,c,d \mid a^q, b^r, c^p, d^p, c^a = c^{\rho(p,q)}, c^b = c^{\rho(p,r)},\\ d^a = d^{\rho(p,q,\sigma_q^k)}, d^b = d^{\rho(p,r,\sigma_r^\ell)}\rangle,\end{aligned}$$

parametrised by

$$\begin{aligned}(k,\ell) \in &\{(x,y)\colon 0 \le x \le \frac{1}{2}(q-1),\ 0 \le y \le \frac{1}{2}(r-1)\}\\ &\cup\{(x,y)\colon 1 \le x \le \frac{1}{2}(q-3),\ \frac{1}{2}(r+1) \le y \le r-2\}.\end{aligned}$$

In total, if $q > 2$ then there are $\frac{1}{2}(qr+q+r+5)\Delta^{qr}_{p-1}$ isomorphism types of such groups. In the case where $q = 2$, the isomorphism types of groups that are isomorphic to $C_{2r} \ltimes C_p^2$, which are determined analogously, except that parameter set $\{(x,y)\colon 1 \le x \le \frac{1}{2}(q-3), \frac{1}{2}(r+1) \le y \le r-2\}$ is empty and there are in total $\frac{1}{2}(3r+5)$ isomorphism types. It remains to consider the case $G/F \cong D_r$. The proof of Theorem 4.2.7(iii) shows that groups are diagonalisable in $\mathrm{GL}_2(p)$, exist only if $r \mid (p-1)$, and are conjugate to the subgroup generated by $\left(\begin{smallmatrix}0&1\\1&0\end{smallmatrix}\right)$ and $\left(\begin{smallmatrix}t&0\\0&t^{-1}\end{smallmatrix}\right)$ with $t = \rho(p,r)$ of order r in $\mathbb{Z}_p$. In particular, such groups are isomorphic to

$$\begin{aligned}\mathrm{Pc}\langle a,b,c,d \mid a^2, b^r, c^p, d^p, b^a = b^{-1}, c^a = d, c^b = c^{\rho(p,r)},\\ d^a = c, d^b = d^{\rho(p,r,r-1)}\rangle.\end{aligned}$$

- If $qr \mid (p+1)$ and $q > 2$, then $qr \nmid (p-1)$, and it follows from Theorem 4.2.2 that any cyclic subgroup of order qr is conjugate to a normal subgroup of the Singer cycle of $\mathrm{GL}_2(p)$ and is irreducible. By Corollary 2.4.3(ii) and Theorem 4.2.7(iii), there is a unique isomorphism type in this case, namely,

$$\mathrm{Pc}\langle a, b, c \mid a^{qr}, b^p, c^p, (b^a, c^a) = (b, c)^{\mathrm{Irr}_2(p,qr)} \rangle,$$

using Notation 4.2.6. If $qr \mid (p+1)$ and $q = 2$, then the construction of $C_{2r} \ltimes C_p^2$ follows analogously and there is a unique isomorphism type of such groups, corresponding to the unique conjugacy class of the cyclic subgroup of $2r$ in $\mathrm{GL}_2(p)$.
It remains to consider the case where $G \cong D_r \ltimes C_p^2$. Since any subgroup of order $r \mid (p+1)$ is irreducible and conjugate to a Singer cycle of $\mathrm{GL}_2(p)$ by Theorem 4.2.2, such group G has a presentation of the form

$$G(k) = \mathrm{Pc}\langle a, b, c, d \mid a^2, b^r, b^a = b^{-1}, (c, d)^a = (c, d)^M, (c^b, d^b)^{\mathrm{Irr}_2(p,r,k)} \rangle,$$

for some $M \in \mathrm{GL}_2(p)$ of order 2 and $k \in \mathbb{Z}_r^*$. For the presentation to be consistent, it is required that $M = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$. On the other hand, since the map $\{b \mapsto b^k\}$ extends to an isomorphism $G(k) \to G(1)$ for any $k \in \mathbb{Z}_r^*$, the isomorphism type of $G(k)$ is independent of the choice of k. Therefore, there is a unique isomorphism type in this case, namely,

$$\mathrm{Pc}\langle a, b, c, d \mid a^2, b^r, b^a = b^{-1}, c^a = d, d^a = c, (c^b, d^b)^{\mathrm{Irr}_2(p,r)} \rangle.$$

- If $qr \mid (p^2-1)$, $qr \nmid (p-1)$, and $qr \nmid (p+1)$, then $q > 2$ and either $\Delta_{p-1}^q \Delta_{p+1}^r = 1$ or $\Delta_{p+1}^q \Delta_{p-1}^r = 1$. We claim that in both cases the subgroup of order qr is cyclic. Suppose for contradiction that $Q \in \mathrm{Syl}_q(G/F)$ acts nontrivially on the normal subgroup $R \in \mathrm{Syl}_r(G/F)$. If $\Delta_{p-1}^q \Delta_{p+1}^r = 1$, then Q is reducible and R irreducible in $\mathrm{GL}_2(p)$, and $G \cong (Q \ltimes R) \ltimes C_p^2$ has a presentation of the form

$$\mathrm{Pc}\langle a, b, c, d \mid a^q, b^r, c^p, d^p, b^a = b^\delta, (c^a, d^a) = (c, d)^M, (c^b, d^b) = (c, d)^A \rangle,$$

where $\delta = \rho(r, q)$, $M = M(p, q, k)$, and $A = \mathrm{Irr}_2(p, r, \ell)$ are the canonical automorphisms desribed in Notations 4.1.1, 4.2.1, and 4.2.6, with $k, \ell \in \mathbb{Z}_q^*$. For the pc-presentation to be consistent, it is required that $((c, d)^b)^a = ((c, d)^a)^{(b^a)}$, while the left-hand side is equivalent to $(c, d)^{AM}$ and the right-hand side equals $(c, d)^{MA^\delta}$, forcing the matrices AM and $M^\delta A$ to be equal. Since M is diagonal, we have $AM = MA = M^\delta A$, forcing that $\delta = 1$, a contradiction. Analogous arguments apply to the case where $\Delta_{p+1}^q \Delta_{p-1}^r = 1$. Hence, if $q > 2$, then it is sufficient to consider $G/F \cong C_{qr}$. Applying Corollary 2.4.3(ii), we find $\Delta_{p-1}^q \Delta_{p+1}^r + \Delta_{p-1}^r \Delta_{p+1}^q$ isomorphism types in this case, in correspondence with the unique conjugacy class of the irreducible cyclic groups of order qr in $\mathrm{GL}_2(p)$. In particular, if $\Delta_{p-1}^q \Delta_{p+1}^r = 1$, then G is isomorphic to

$$\mathrm{Pc}\langle a, b, c, d \mid a^q, b^r, c^p, d^p, (c, d)^a = (c, d)^{M(p,q)}, (c, d)^b = (c, d)^{\mathrm{Irr}_2(p,r)} \rangle;$$

if $\Delta_{p+1}^q \Delta_{p-1}^r = 1$, then G is isomorphic to

$$\mathrm{Pc}\langle a, b, c, d \mid a^q, b^r, c^p, d^p, (c, d)^a = (c, d)^{\mathrm{Irr}_2(p,q)}, (c, d)^b = (c, d)^{M(p,r)} \rangle.$$

5. If $|F| = p^2q$, then $G/F \cong C_r$ and G splits over F. Since $r > q$, we know G/F acts trivially on the Sylow q-subgroup of F. There are two isomorphism types of F, namely, $C_{p^2} \times C_q$ and $C_p^2 \times C_q$.
   (a) If $F \cong C_{p^2} \times C_q$, then $G \cong (C_r \ltimes C_{p^2}) \times C_q$ is uniquely determined by the nonabelian metacyclic extensions $C_r \ltimes C_{p^2}$, in one-to-one correspondence with the Δ^r_{p-1} normal subgroups of order r in $\mathrm{Aut}(F)$. In particular, G is isomorphic to
   $$\mathrm{Pc}\langle a, b, c \mid a^r, b^{p^2}, c^q, b^a = b^{\rho(p^2,r)}\rangle.$$
   (b) If $F \cong C_p^2 \times C_q$, then $\mathrm{Aut}(F) \cong \mathrm{GL}_2(p) \times \mathbb{Z}_q^*$. It follows that $r \mid (p^2-1)$, and $G \cong (C_r \ltimes C_p^2) \times C_q$. There are two cases to consider.
      - If $r \mid (p-1)$, then $r \nmid (q+1)$ and $G \cong (C_r \ltimes C_p^2) \times C_q$ is determined by the nonabelian factor $C_r \ltimes C_p^2$. Such groups of order p^2q are classified in Theorem 6.1.1. Thus, there are $\frac{1}{2}(r+3)\Delta^r_{p-1}$ isomorphism types in this case. In particular, if $Z(G) \cong C_{pq}$, then G is isomorphic to
      $$\mathrm{Pc}\langle a, b, c, d \mid a^r, b^p, c^p, d^q, b^a = b^{\rho(p,r)}\rangle;$$
      if $Z(G) \cong C_q$, then G is isomorphic to one of the following $\frac{1}{2}(r-1)$ groups
      $$\mathrm{Pc}\langle a, b, c, d \mid a^r, b^p, c^p, d^q, (b^a, c^a) = (b, a)^{M(p,r,\sigma_r^k)}\rangle,$$
      parametrised by $k \in \{0, \ldots, \frac{1}{2}(r-1)\}$.
      - If $r \mid (p+1)$, then $r \nmid (p-1)$ and $G \cong (C_r \ltimes C_p^2) \times C_q$ is determined by the nonabelian direct factor $C_r \ltimes C_p^2$ in this case. In particular, such a group exists only if $\Delta^r_{p+1} = 1$, and is unique up to isomorphism, and so G is isomorphic to
      $$\mathrm{Pc}\langle a, b, c, d \mid a^r, b^p, c^p, d^q, (c^a, d^a) = (c, d)^{\mathrm{Irr}_2(p,r)}\rangle.$$

6. If $|F| = p^2r$, then $G/F \cong C_q$. There are two isomorphism types of F, namely, $F \cong C_{p^2} \times C_r$ or $C_p^2 \times C_r$.
   (a) If $F \cong C_{p^2} \times C_r$, then $G \cong C_q \ltimes C_{p^2r}$ is a nonabelian metacyclic split extension. In particular, there are $\Delta^q_{r-1} + \Delta^q_{p-1} + (q-1)\Delta^q_{r-1}\Delta^q_{p-1}$ isomorphism types of such groups, in one-to-one correspondence with the cyclic normal subgroups of order q in $\mathrm{Aut}(F) \cong \mathbb{Z}_{p^2}^* \times \mathbb{Z}_r^*$. Using Notation 4.1.1, these groups have presentations
   $$\mathrm{Pc}\langle a, b, c \mid a^q, b^r, c^{p^2}, b^a = b^{\rho(r,q)}\rangle,$$
   $$\mathrm{Pc}\langle a, b, c \mid a^q, b^{p^2}, c^r, b^a = b^{\rho(p^2,q)}\rangle,$$
   $$\mathrm{Pc}\langle a, b, c \mid a^q, b^{p^2}, c^r, b^a = b^{\rho(p^2,q)}, c^a = c^{\rho(r,q,k)}\rangle,$$
   where $k \in \mathbb{Z}_q^*$.
   (b) If $F \cong C_p^2 \times C_r$, then $\mathrm{Aut}(F) \cong \mathrm{GL}_2(p) \times \mathbb{Z}_r^*$. It follows that $q \mid (p^2-1)(r-1)$.
      - If $q \nmid (r-1)$, then $q \mid (p-1)$ or $q \mid (p+1)$ and $G \cong (C_q \ltimes C_p^2) \times C_r$. If $q > 2$, then there are $\Delta^q_{p+1} + \frac{1}{2}(q+5)\Delta^q_{p-1}$ isomorphism types of such G parametrised by the conjugacy class representatives of cyclic subgroups of order q in $\mathrm{GL}_2(p)$.

In particular, if $q \mid (p+1)$, then G is isomorphic to

$$\mathrm{Pc}\langle a,b,c,d \mid a^q, b^p, c^p, d^r, (b^a, c^a) = (b,c)^{\mathrm{Irr}_2(p,q)}\rangle;$$

if $q \mid (p-1)$ and $Z(G) \cong C_{pr}$, then G is isomorphic to

$$\mathrm{Pc}\langle a,b,c,d \mid a^q, b^p, c^p, d^r, b^a = b^{\rho(p,q)}\rangle$$

if $q \mid (p-1)$ and $Z(G) \cong C_r$, then G is isomorphic to one of the $\frac{1}{2}(q+1)$ groups

$$\mathrm{Pc}\langle a,b,c,d \mid a^q, b^p, c^p, d^r, b^a = b^{\rho(p,q)}, c^a = c^{\rho(p,q,k)}\rangle,$$

parametrised by $k \in \{0,\dots,\frac{1}{2}(q-1)\}$.
Analogously, if $q = 2$, there are 2 isomorphism types of $G \cong (C_2 \ltimes C_p^2) \times C_r$. More specifically, if $Z(G) \cong C_{pr}$, then G is isomorphic to

$$\mathrm{Pc}\langle a,b,c,d \mid a^2, b^p, c^p, d^r, b^a = b^{-1}\rangle;$$

otherwise, G is isomorphic to

$$\mathrm{Pc}\langle a,b,c,d \mid a^2, b^p, c^p, d^r, b^a = b^{-1}, c^a = c^{-1}\rangle.$$

- If $q \nmid (p^2-1)$, then $q \mid (r-1)$ and $G \cong (C_q \ltimes C_r) \times C_p^2$, which is uniquely determined by the nonabelian direct factor $C_q \ltimes C_r$, which is unique up to isomorphism and exists only if $\Delta_{r-1}^q = 1$. Hence in this case, G is isomorphic to

$$\mathrm{Pc}\langle a,b,c,d \mid a^q, b^r, c^p, d^p, b^a = b^{\rho(r,q)}\rangle.$$

- It remains to consider the cases where $G/F \cong C_q$ acts nontrivially on both Sylow p- and r-subgroups of F. This requires that $q \mid (p^2-1)$ and $q \mid (r-1)$. From Corollary 2.4.3(ii) we know each conjugacy class of cyclic subgroups of order q in $\mathrm{Aut}(F) \cong \mathbb{Z}_r^* \times \mathrm{GL}_2(p)$ corresponds to precisely one isomorphism type of such split extensions. If $q \mid (p-1)$, then subgroups of order q are reducible in $\mathrm{GL}_2(p) < \mathrm{Aut}(F)$. Write $\mathrm{diag}(a,b,c)$ for an element $\left(\begin{smallmatrix} a & 0 & 0 \\ 0 & b & 0 \\ 0 & 0 & c \end{smallmatrix}\right) \in \mathrm{Aut}(F)$, where the first row is evaluated modulo r and the second and third rows modulo p. Using Notations 4.1.1 and 4.2.1, then a reducible subgroup C_q in $\mathrm{Aut}(F)$ is conjugate to $\langle \mathrm{diag}(s^\delta, t, t^\mu)\rangle$ with $s = \rho(r,q)$, $t = \rho(p,q)$, $\delta \in \mathbb{Z}_p^*$, and $\mu \in \mathbb{Z}_p$. In particular, a direct calculation shows that for $\mu, \nu \in \mathbb{Z}_p$ and $\delta \in \mathbb{Z}_p^*$, two subgroups generated by $\mathrm{diag}(s,t,t^\mu)$ and $\mathrm{diag}(s^\delta,t,t^\nu)$ are conjugate in $\mathrm{Aut}(F)$ if and only if there exists some $x \in \mathbb{Z}_q^*$ such that $\mathrm{diag}(s,t,1)^x$ is conjugate to $\mathrm{diag}(s^\delta,t,1)$, if and only if $s^x = s^\delta$ and $\mathrm{diag}(t^x,1)$ is conjugate to $\mathrm{diag}(t,1)$ in $\mathrm{GL}_2(p)$, if and only if $\delta = 1$. Similarly, for $\gamma, \delta \in ZZ_p^*$ and $\mu, \nu \in \mathbb{Z}_p$, the subgroups $\langle \mathrm{diag}(s^\gamma, t, t^\mu)\rangle$ and $\langle \mathrm{diag}(s^\delta, t, t^\nu)\rangle$ are conjugate if and only if there exists some $x \in \mathbb{Z}_q^*$ such that $\mathrm{diag}(s^\gamma, t, t^\mu)^x$ is conjugate to $\mathrm{diag}(s^\delta, t, t^\nu)$, if and only if $s^{x\gamma} = s^\delta$, and $\mathrm{diag}(t^x, t^{x\mu})$ is conjugate to $\mathrm{diag}(t, t^\nu)$ in $\mathrm{GL}_2(p)$, if and only if $\delta \equiv \gamma\nu$ and $\nu\mu \equiv 1 \bmod q$. This implies that if $\delta = \nu$, then $\langle \mathrm{diag}(s^\delta, t, t^\nu)\rangle$ is conjugate to $\langle \mathrm{diag}(s, t, t^{\nu^{-1}})\rangle$. Together, this shows that the conjugacy class representatives for these cyclic subgroups of order q in $\mathrm{Aut}(F)$ are of the form $\langle \rho(r,q), \rho(p,q,k), 1\rangle$ with $k \in \mathbb{Z}_q^*$, $\langle \rho(r,q), M(p,q,\sigma_q^k)\rangle$ with $0 \le k \le \lfloor \frac{1}{2}(q-3)\rfloor$,

or $\langle \rho(r,q,\sigma_q^\ell), M(p,q,\sigma_q^k)\rangle$, with

$$\begin{aligned}(k,\ell) \in &\{(x,y) \in \mathbb{Z}_{q-1}^2 \colon 0 \le x \le \frac{1}{2}(q-1),\ 1 \le y \le \frac{1}{2}(q-3)\}\\ &\cup\{(x,y) \in \mathbb{Z}_{q-1}^2 \colon 0 \le x \le \frac{1}{2}(q-3),\ \frac{1}{2}(q-1) \le y \le q-2\}\\ &\cup\{(\frac{1}{2}(q-1),\frac{1}{2}(q-1)) \in \mathbb{Z}_{q-1}^2\}.\end{aligned}$$

Accordingly, we find the $(q-1+\frac{1}{2}q(q-1))\Delta_{r-1}^q\Delta_{p-1}^q$ isomorphism types in this case, with presentations

$$\mathrm{Pc}\langle a,b,c,d \mid a^q, b^r, c^p, d^p, b^a = b^{\rho(r,q)}, c^a = c^{\rho(p,q,k)}\rangle$$

parametrised by $k \in \mathbb{Z}_q^*$, and

$$\mathrm{Pc}\langle a,b,c,d \mid a^q, b^r, c^p, d^p, b^a = b^{\rho(r,q,\sigma_q^\ell)}, (c^a,d^a) = (c,d)^{M(p,q,\sigma_q^k)}\rangle,$$

parametrised by $(k,\ell) \in P \subseteq \mathbb{Z}_{q-1}^2$, where

$$\begin{aligned}P =&\{(x,0) \colon 0 \le x \le \frac{1}{2}(q-3)\}\\ &\cup\{(x,y) \in \mathbb{Z}_{q-1}^2 \colon 0 \le x \le \frac{1}{2}(q-1),\ 1 \le y \le \frac{1}{2}(q-3)\}\\ &\cup\{(x,y) \in \mathbb{Z}_{q-1}^2 \colon 0 \le x \le \frac{1}{2}(q-3),\ \frac{1}{2}(q-1) \le y \le q-2\}\\ &\cup\{(\frac{1}{2}(q-1),\frac{1}{2}(q-1))\}.\end{aligned}$$

Note that in the special cases $q = 2$, there are two conjugacy classes of groups of order 2 in $\mathrm{Aut}(F)$, and the above discussion simplifies. In particular, the conjugacy class representatives are $\langle \mathrm{diag}(-1,-1,1)\rangle$ and $\langle \mathrm{diag}(-1,-1,-1)\rangle$, and the corresponding two isomorphism types are $D_{rp} \times C_p$ and$C_2 \ltimes (C_r \times C_p^2)$. If $q \mid (p+1)$ and $q \mid (r-1)$, then, up to conjugacy, there is a unique subgroup of order q in $\mathrm{GL}_2(p)$, and there is a unique normal subgroup of order q in $\mathbb{Z}_r^*$. Since the Sylow r-subgroup is normal in both F and G, it suffices to consider G with a presentation

$$G(k,\ell) = \mathrm{Pc}\langle a,b,c,d \mid a^q, b^r, c^p, d^p, b^a = b^{\rho(r,q,k)}, (c^a,d^a) = (c,d)^{\mathrm{Irr}_2(p,q,\ell)}\rangle,$$

for some $k,\ell \in \mathbb{Z}_q^*$. For any such k,ℓ, since the map $\{a \mapsto a^k\}$ extends to an isomorphism $G(k,\ell) \to G(1,k^{-1}\ell)$, it suffices to consider $k = 1$. It remains to investigate the isomorphism types of $G(1,\ell)$ with $\ell \in \mathbb{Z}_q^*$. Following from Corollary 2.4.3, we know $G(1,\ell) \cong G(1,\ell')$ if and only if the cyclic subgroups $\langle s, \mathrm{Irr}_2(p,q,\ell)\rangle$ and $\langle s, \mathrm{Irr}_2(p,q,\ell')\rangle$ are conjugate in $\mathrm{Aut}(F)$. Using Notation 4.2.6, with a fixed q-th root of unity $i \in GF(p^2)$, the block matrix $\mathrm{Irr}_2(p,q,\ell)$ is conjugate to $\begin{pmatrix} 0 & -1 \\ 1 & i^{\ell p}+i^\ell \end{pmatrix}$ in $\mathrm{GL}_2(p) < \mathrm{Aut}(F)$ for any $\ell \in \mathbb{Z}_q^*$, and so $\langle s, \mathrm{Irr}_2(p,q,\ell)\rangle$ is conjugate to

$$\langle \begin{pmatrix} s & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & i^{\ell p}+i^\ell \end{pmatrix}\rangle$$

for any $\ell \in \mathbb{Z}_q^*$. A direct calculation shows that for $\ell, \ell' \in \mathbb{Z}_q*$, the subgroups $\langle s, \mathrm{Irr}_2(p,q,\ell)\rangle$ and $\langle s, \mathrm{Irr}_2(p,q,\ell')\rangle$ are conjugate if and only if

$$i^{\ell p} + i^{\ell} = i^{\ell' p} + i^{\ell'},$$

if and only if $\ell' \in \{\ell, -\ell\}$ (since $i^{\ell p} = i^{-\ell^{-1}}$ for any $\ell \in \mathbb{Z}_q^*$). Therefore, there are $\frac{1}{2}(q-1)\Delta^q_{r-1}\Delta^q_{p+1}$ isomorphism types in this case, with presentations

$$\mathrm{Pc}\langle a,b,c,d \mid a^q, b^r, c^p, d^p, b^a = b^{\rho(r,q)}, (c^a, d^a) = (c,d)^{\mathrm{Irr}_2(p,q,\sigma_q^k)}\rangle,$$

parametrised by $k \in \{1, \dots, \frac{1}{2}(q-1)\}$.

We are left with the cases where $\gcd(|F|, |G/F|) > 1$, namely, $|F| \in \{p, pq, pr, pqr\}$.

1. If $|F| = p$, then $G/F \cong C_{pqr}$ since $\mathrm{Aut}(F) \cong C_{q-1}$. Hence, G/F has a normal Sylow p-subgroup, whose preimage under the natural projection $G \to G/F$ in G is also a normal Sylow subgroup and is of order p^2, which contradicts the assumption that $|F| = p$. Therefore, there exists no such group.

2. If $|F| = pq$, then $G/F \cong C_{pr}$ since $\mathrm{Aut}(F) \cong C_{p-1} \times C_{r-1}$. It follows that $p \mid (q-1)$ and $r \mid (p-1)$ for there to be a faithful G/F-action on F. But this implies that $r < p < q$, which contradicts the assumption that $r > q$. Therefore, there exists no such group.

3. If $|F| = pr$, then $G/F \cong C_{pq}$ since $\mathrm{Aut}(F) \cong C_{p-1} \times C_{r-1}$. It follows that $p \mid (r-1)$ and $q \mid (p-1)(r-1)$. Let $Q \in \mathrm{Syl}_q(G/F)$. There are two cases to consider.
   (a) If Q acts trivially on the Sylow p-subgroup of F, then Q acts nontrivially on the Sylow r-subgroup R for the G/F-action on F to be faithful. It follows that $q \mid (r-1)$. Moreover, $R \lhd G$ is characteristic and has a complement in G, denoted by H. Up to conjugacy, such H is unique by Theorem 2.4.1. In particular, $G \cong H \ltimes R$, where $|H| = p^2q$ and H acts on $R \cong C_r$ via an automorphism of order pq. Also, H is abelian by assumption. Thus $H \cong C_{p^2q}$ or $C_p^2 \times C_q$. For each case, there is a unique isomorphism type by Corollary 2.4.3; namely,

   $$\mathrm{Pc}\langle a,b,c,d \mid a^p, b^p, c^q, d^r, d^a = d^{\rho(r,p)}, d^c = d^{\rho(r,q)}\rangle,$$

   and

   $$\mathrm{Pc}\langle a,b,c,d \mid a^p = b, b^p, c^q, d^r, d^a = d^{\rho(r,p)}, d^c = d^{\rho(r,q)}\rangle,$$

   respectively, accounting for $2\Delta^q_{r-1}\Delta^p_{r-1}$ isomorphism types in this case.
   (b) If Q acts nontrivially on the Sylow p-subgroup of F, then $q \mid (p-1)$. Theorem 2.3.5 and Theorem 2.4.3 show that, up to equivalence, there are $\Delta^q_{p-1} + (q-1)\Delta^q_{p-1}\Delta^q_{r-1}$ such nonequivalent G/F-module structures on F, in bijection with the conjugacy classes with the cyclic normal subgroup of order q in $\mathrm{Aut}(F) \cong \mathbb{Z}_p^* \times \mathbb{Z}_r^*$. Thus it suffices to consider a pc-presentation of G parametrised by

   $$G(t_1, t_2, k) = \mathrm{Pc}\langle a,b,c,d \mid a^p = t_1, b^q = t_2, c^r, d^p, c^a = c^\nu, c^b = c^s, d^b = d^\mu\rangle,$$

   where $\nu = \rho(r,p)$ and $\mu = \rho(p,q)$, and $s = \rho(r,q,k)$ for some $k \in \mathbb{Z}_q$ with $k > 0$ only when $q \mid (r-1)$. Suppose that $t_1 = c^{x_1}d^{y_1}$ and $t_2 = c^{x_2}d^{y_2}$. Theorem 3.2.3 implies that $t_1^a = t_1$ and $t_2^b = t_2$, that $c^{\nu x_1} = c^{x_1}$ and $c^{sx_2}d^{\mu x_2} = c^{x_2}d^{y_2}$; this implies that $x_1 = 0 = y_2$. Moreover, if $k \neq 0$, then $x_2 = 0$; if $k = 0$, then $q \mid (r-1)$ and we might have $a^p = d^{y_1}$ and $b^q = c^{x_2}$. However, $(d^{y_1})^b = d^{\mu y_1} = (a^p)^b = a^p = b^{y_1}$ and

$(c^{x_2})^a = c^{\nu x_2} = (b^q)^a = b^q = c^{x_2}$, which forces $x_2 = 0 = y_1$. Hence, we conclude that any such extension of F by G/F splits. In particular, if Q acts trivially on the Sylow r-subgroup of F, then $G \cong (C_p \ltimes C_r) \times (C_q \ltimes C_p)$ is uniquely determined by the isomorphism types of the nonabelian factors $C_p \ltimes C_r$ and $C_q \ltimes C_p$, in which case G is isomorphic to

$$\mathrm{Pc}\langle a, b, c, d \mid a^p, b^q, c^r, d^p, c^a = c^{\rho(r,p)}, d^b = d^{\rho(p,q)} \rangle.$$

On the other hand, if Q acts nontrivially on the Sylow r-subgroup, then $q \mid (r-1)$, and there are $q-1$ isomorphism types of $(C_p \times C_q) \ltimes (C_r \times C_p)$ with presentations

$$\mathrm{Pc}\langle a, b, c, d \mid a^p, b^q, c^r, d^p, c^a = c^{\rho(r,p)}, c^b = c^{\rho(r,q)}, d^b = d^{\rho(p,q,k)} \rangle,$$

parametrised by $k \in \mathbb{Z}_q^*$.

4. If $F = pqr$, then $G/F \cong C_p$ and the subgroup $N \lhd F$ of order qr is characteristic in G. Theorem 2.4.1 shows that N has a complement $P \in \mathrm{Syl}_p(G)$ and $G = P \ltimes N$. In particular, P acts on N via *depending* $\in \mathrm{Aut}(N)$ such that α has order p. It follows that p divides at least one of $(q-1)$ and $(r-1)$. There are two cases to consider, namely, $P \cong C_{p^2}$ or C_p^2. For each case, there are $\Delta_{r-1}^p + \Delta_{q-1}^p + (p-1)\Delta_{r-1}^p\Delta_{q-1}^p$ isomorphism types of G, in one-to-one correspondence with subgroups of order p in $\mathrm{Aut}(N) \cong \mathbb{Z}_q^* \times \mathbb{Z}_r^*$. Since the Sylow q- and r-subgroups are both normal in G, it suffices to consider the isomorphism types

$$\mathrm{Pc}\langle a, b, c, d \mid a^p = t, b^p, c^q, d^r, c^a = c^\nu, d^a = d^\mu \rangle,$$

where $t = 1$ or b, corresponding to the cases where $P \cong C_p^2$ or C_{p^2} respectively, and $\mu \in \mathbb{Z}_q^*$ and $\nu \in \mathbb{Z}_r^*$ have order at most p, at least one of which has order p. In particular, these groups have isomorphism class representatives

$$\begin{aligned}
&\mathrm{Pc}\langle a, b, c, d \mid a^p = b, b^p, c^q, d^r, c^a = c^{\rho(q,p)} \rangle,\\
&\mathrm{Pc}\langle a, b, c, d \mid a^p = b, b^p, c^q, d^r, d^a = d^{\rho(r,p)} \rangle,\\
&\mathrm{Pc}\langle a, b, c, d \mid a^p = b, b^p, c^q, d^r, c^a = c^{\rho(q,p)}, d^a = d^{\rho(r,p,k)} \rangle,\\
&\mathrm{Pc}\langle a, b, c, d \mid a^p, b^p, c^q, d^r, c^a = c^{\rho(q,p)} \rangle,\\
&\mathrm{Pc}\langle a, b, c, d \mid a^p, b^p, c^q, d^r, d^a = d^{\rho(r,p)} \rangle,\\
&\mathrm{Pc}\langle a, b, c, d \mid a^p, b^p, c^q, d^r, c^a = c^{\rho(q,p)}, d^a = d^{\rho(r,p,k)} \rangle,
\end{aligned}$$

where $k \in \mathbb{Z}_p^*$. □

Part III

Generalisations and implementations

Chapter 8

Outlook and computational remarks

We have explicitly constructed all groups whose orders are products of at most four prime factors; this and the resulting GAP implementations are the main results of this thesis. In this final chapter, we briefly discuss possible generalisations. We also comment on the implementation of our algorithms.

8.1 Further order types

Let p, q be distinct primes. In [4], Besche and Eick gave an algorithmic description for the construction of groups of order $p^n q$ (assuming complete classification of groups of order p^n). The so-called *upwards cyclic extension method* [4, Figure 4] and the *downwards cyclic extension method* [4, Figure 3] are constructive and reflect the applications of Corollary 2.4.3 and Corollary 2.4.6 to groups of order $p^n q$. Our discussion in Chapter 6 is motivated by these cyclic extension methods. Moreover, we note that these methods are not confined to groups of order $p^n q$. For example, the downwards extension method also applies to groups of order $p^a q^b$ with a normal cyclic Sylow subgroup S such that $\mathrm{Aut}(S)$ is cyclic, and the upwards extension method applies to groups of order $p^a q^b$ with a normal Sylow subgroup and a cyclic complement. More generally, Theorem 2.4.2(ii) applies to the classification of groups with a normal Sylow subgroup. However, the generalisation of this approach to groups of order $p^a q^b$ faces a number of challenges since many of the results depend on the existence of a normal Sylow subgroup. Nevertheless, for "small" order types, groups without normal Sylow subgroup rarely appear and many of them can be constructed and identified by exhaustion. For example, Laue [37, Theorem 1.11] showed that if there exists a group of order $m = p^a q^b$ with $a + b \leq 6$ that has no normal Sylow subgroup, then

$$m \in \{2^3{\cdot}3,\ 2^3{\cdot}3^2,\ 2^3{\cdot}3^3,\ 2^4{\cdot}3,\ 2^4{\cdot}7,\ 2^4{\cdot}3^2,\ 2^4{\cdot}7^2,\ 2^4{\cdot}3,\ 2^5{\cdot}5,\ 2^5{\cdot}7,\ 3^4{\cdot}13,\ 3^4{\cdot}2^2,\ 3^4{\cdot}13^2,\ 3^5{\cdot}13\}$$

$$\text{or } m \in \{p^4q^2 \colon p, q \text{ are primes such that } q = p^2 + p + 1\}.$$

Note that the converse is not true. For example, we see later in Theorem 8.1.2 that every group of order $2^4{\cdot}7$ contains a normal Sylow subgroup (see also [37, Theorem 2.1]). If we restrict our attention to the groups of order $p^n q$, then the following theorem due to Eick and Moede [25] affirms that there is a strict condition on the primes p and q for there to exist a group of order $p^n q$ without normal Sylow subgroup.

Theorem 8.1.1 ([25], Theorem 25)**.** *Let p, q be distinct primes and n be a positive integer. If there exists a group of order $p^n q$ without normal Sylow subgroup, then there exist positive integers m, ℓ with $m\ell \leq n$ such that $p \mid \gcd(m^\ell \ell!, q-1)$ and $q \mid (p^m - 1)$.*

On the other hand, a group of order $p^n q$ is nilpotent if and only if all of its Sylow subgroups are normal. Such groups are isomorphic to direct products of C_q and p-groups of order p^n, thus are fully classified by the isomorphism types of such p-groups. Let $\mathcal{N}(x)$ be the number of isomorphism types of nilpotent groups of order x and denote the total number of isomorphism types of groups of order x by $\mathcal{G}(x)$. It follows that $\mathcal{N}(p^n q) = \mathcal{G}(p^n)$. The remaining groups are non-nilpotent and can be partitioned into three cases. Let $\mathcal{N}_p(x)$ be the number of non-nilpotent groups of order x that have a normal Sylow p-subgroup, let $\mathcal{N}_q(x)$ be its counterpart with a normal Sylow q-subgroup, and let $\mathcal{R}(x)$ be the number of isomorphism types of groups of order x without normal Sylow subgroups. Then the total number of isomorphism types of groups of order $p^n q$ is given by

$$\mathcal{G}(p^n q) = \mathcal{G}(p^n) + \mathcal{N}_p(p^n q) + \mathcal{N}_q(p^n q) + \mathcal{R}(p^n q). \tag{8.1.1}$$

The groups of order $p^n q^2$ can be studied in a similar manner, noting that there are two isomorphism types of groups of order q^2, namely, C_{q^2} and C_q^2. Thus, the total number of isomorphism types of groups of order $p^n q^2$ is given by

$$\mathcal{G}(p^n q^2) = 2\mathcal{G}(p^n) + \mathcal{N}_p(p^n q^2) + \mathcal{N}_q(p^n q^2) + \mathcal{R}(p^n q^2). \tag{8.1.2}$$

For $n \leq 5$, Eick and Moede [25] enumerated groups of order $p^n q$, where they gave an explicit formula for each summand in (8.1.1). For $n \leq 3$, we have constructed these groups explicitly in Chapter 6. Assuming a complete list of isomorphism class representatives for groups of order p^n, we can generalise the proofs of Lemma 6.2.5 and Lemma 6.2.4 to $n > 3$. For example, with the list of groups of order p^4 in Table 5.3, we apply the cyclic extension methods to explicitly construct all non-nilpotent groups (up to isomorphism) of order $p^4 q$ with a normal Sylow subgroup. For the remaining groups without normal Sylow subgroup, we first apply Theorem 8.1.1 to exhaust the finite list of possible orders, and then construct these groups and find $\mathcal{R}(p^4 q)$ accordingly.

This way, we find a list of isomorphism class representatives for groups of order $p^4 q$; we present the results in this section as a demonstration for the generalisation of Chapter 6. Due to the large number and complexity of the isomorphism types of these groups, the construction of groups of order $p^4 q$ contains more involving and technical manipulations of the pc-presentations. We omit detailed proofs in this section, but include a sketch of the proof in Appendix B (see Lemmas B.0.3, B.0.4, and B.0.2). Recall that in each table if the counting formula in the right column gives 0, then it means the groups listed in the respective row do not exist. Moreover, for each group of order p^4, we use our SOT ID (see Tables 5.3 and 5.4) to encode the isomorphism type. Unless otherwise specified, notations in Tables 8.1 and 8.2 are consistent with Notations 4.1.1, 4.2.1, and 4.2.6.

Theorem 8.1.2. *Let $\mathcal{G}(p^4q)$ be the number of isomorphism types of groups of order p^4q. Then*

$$\begin{aligned}\mathcal{G}(p^4q) &= 15 - \Delta_p^2 + (5p + 19 - \Delta_p^2)\Delta_{q-1}^p \\ &\quad + (5 + 2p)\Delta_{q-1}^{p^2} + 2\Delta_{q-1}^{p^3} + \Delta_{q-1}^{p^4} \\ &\quad + \frac{1}{24}(q^3 + 31q^2 + 189q + 423 + 16\Delta_{q-1}^3 + 12\Delta_{q-1}^4 + 27\Delta_q^2)\Delta_{p-1}^q \\ &\quad + \frac{1}{4}(q + 21 + 2\Delta_{q-1}^4)(1 - \Delta_q^2)\Delta_{p+1}^q + (1 - \Delta_q^3)(1 - \Delta_q^2)\Delta_{p^2+p+1}^q \\ &\quad + (1 - \Delta_q^2)\Delta_{p^2+1}^q + \Delta_p^{13}\Delta_q^3 + 4\Delta_p^2\Delta_q^3.\end{aligned}$$

In particular, we have $\mathcal{N}(p^4q) = 15 - \Delta_q^2$ and $\mathcal{R}(p^4q) = \Delta_p^{13}\Delta_q^3 + 4\Delta_p^2\Delta_q^3$. A non-nilpotent group of order p^4q with a normal Sylow subgroup has a presentation as listed in Tables 8.1 and 8.2; groups of such order without normal Sylow subgroup are listed in Table 8.3.

TABLE 8.1: Non-nilpotent groups of order p^4q with a normal Sylow q-subgroup with complement P (the isomorphism types and SOT IDs of P are listed in Table 5.3 and 8.2).

Pc-relators	Parameters	Number of groups
Cluster 1: $P \cong C_{p^4}$		
$a^{p^4}, b^q, b^a / b^{\rho(q,p)}$		Δ_{q-1}^{p}
$a^{p^4}, b^q, b^a / b^{\rho(q,p^2)}$		$\Delta_{q-1}^{p^2}$
$a^{p^4}, b^q, b^a / b^{\rho(q,p^3)}$		$\Delta_{q-1}^{p^3}$
$a^{p^4}, b^q, b^a / b^{\rho(q,p^4)}$		$\Delta_{q-1}^{p^4}$
Cluster 2: $P \cong C_{p^3} \times C_p$		
$a^{p^3}, b^p, c^q, c^b / c^{\rho(q,p)}$		Δ_{q-1}^{p}
$a^{p^3}, b^p, c^q, c^a / c^{\rho(q,p)}$		Δ_{q-1}^{p}
$a^{p^2} / c, b^p / c, c^p, d^q, d^a / d^{\rho(q,p^2)}$		$\Delta_{q-1}^{p^2}$
$a^{p^3}, b^p, c^q, c^a / c^{\rho(q,p^2)}$		$\Delta_{q-1}^{p^2}$
$a^{p^3}, b^p, c^q, c^a / c^{\rho(q,p^3)}$		$\Delta_{q-1}^{p^3}$
Cluster 3: $P \cong C_{p^2} \times C_{p^2}$		
$a^{p^2}, b^{p^2}, c^q, c^b / c^{\rho(q,p)}$		Δ_{q-1}^{p}
$a^{p^2}, b^{p^2}, c^q, c^b / c^{\rho(q,p^2)}$		$\Delta_{q-1}^{p^2}$
Cluster 4: $P \cong C_{p^2} \times C_p^2$		
$a^{p^2}, b^p, c^p, d^q, d^b / d^{\rho(q,p)}$		Δ_{q-1}^{p}
$a^{p^2}, b^p, c^p, d^q, d^a / d^{\rho(q,p)}$		Δ_{q-1}^{p}
$a^{p^2}, b^p, c^p, d^q, d^a / d^{\rho(q,p^2)}$		$\Delta_{q-1}^{p^2}$
Cluster 5: $P \cong C_p^4$		
$a^p, b^p, c^p, d^p, e^q, e^a / e^{\rho(q,p)}$		Δ_{q-1}^{p}
Cluster 6: P has SOT ID $(p^4 : 6)$		
$a^p, b^p / c, c^p, d^p, e^q, d^a / cd, e^a / e^{\rho(q,p)}$		$(1 - \Delta_p^2)\Delta_{q-1}^{p}$
$a^p, b^p / c, c^p, d^p, e^q, d^a / cd, e^b / e^{\rho(q,p)}$		$(1 - \Delta_p^2)\Delta_{q-1}^{p}$
$a^p, b^p / c, c^p, d^p, e^q, d^a / cd, d^b / cd, e^a / e^{\rho(q,p)}$		$(1 - \Delta_p^2)\Delta_{q-1}^{p}$
$a^2, b^2 / c, c^2, d^2, e^q, b^a / bc, d^a / cd, e^a / e^{-1}$		Δ_p^2
$a^2, b^2 / c, c^2, d^2, e^q, b^a / bc, d^a / cd, e^b / e^{-1}$		Δ_p^2

$a^2, b^2/d, c^2/d, d^2, e^q, c^a/cd, c^b/cd, e^a/e^{-1}$		Δ_p^2
Cluster 7: P has SOT ID $(p^4:7)$		
$a^p/b, b^p/c, c^p, d^p, e^q, d^a/cd, e^d/e^{\rho(q,p,k)}$	$k \in \mathbb{Z}_p^*$	$(p-1)(1-\Delta_p^2)\Delta_{q-1}^p$
$a^p/b, b^p/c, c^p, d^p, e^q, d^a/cd, e^a/e^{\rho(q,p)}$		$(1-\Delta_p^2)\Delta_{q-1}^p$
$a^p/b, b^p/d, c^p/d, d^p, e^q, c^a/cd, e^a/e^{\rho(q,p^2,k)}, e^b/e^{\rho(q,p,k)}$	$k \in \mathbb{Z}_p^*$	$(p-1)(1-\Delta_p^2)\Delta_{q-1}^{p^2}$
$a^p/b, b^p/c, c^p, d^p, e^q, d^a/cd, e^a/e^{\rho(q,p^2)}, e^b/e^{\rho(q,p)}$		$(1-\Delta_p^2)\Delta_{q-1}^{p^2}$
$a^2, b^2/c, c^2, d^2, e^q, b^a/bc, e^a/e^{-1}$		Δ_p^2
$a^2, b^2/c, c^2, d^2, e^q, b^a/bc, e^d/e^{-1}$		Δ_p^2
$a^2, b^2/c, c^2, d^2, e^q, b^a/bc, e^b/e^{-1}$		Δ_p^2
Cluster 8: P has SOT ID $(p^4:8)$		
$a^p, b^p/c, c^p, d^p, e^q, b^a/bc, e^a/e^{\rho(q,p,k)}$	$k \in \mathbb{Z}_p^*$	$(p-1)(1-\Delta_p^2)\Delta_{q-1}^p$
$a^p, b^p/c, c^p, d^p, e^q, b^a/bc, e^d/e^{\rho(q,p)}$		$(1-\Delta_p^2)\Delta_{q-1}^p$
$a^p, b^p/c, c^p, d^p, e^q, b^a/bc, e^b/e^{\rho(q,p)}$		$(1-\Delta_p^2)\Delta_{q-1}^p$
$a^2, b^2/c, c^2, d^2, e^q, b^a/bd, e^a/e^{-1}$		Δ_p^2
$a^2, b^2/c, c^2, d^2, e^q, b^a/bd, e^b/e^{-1}$		Δ_p^2
$a^2, b^2/c, c^2, d^2, e^q, b^a/bd, e^b/e^{\rho(q,4)}, e^c/e^{-1}$		$\Delta_p^2\Delta_{q-1}^4$
Cluster 9: P has SOT ID $(p^4:9)$		
$a^p, b^p/c, c^p, d^p, e^q, b^a/bd, e^a/e^{\rho(q,p)}$		$(1-\Delta_p^2)\Delta_{q-1}^p$
$a^p, b^p/c, c^p, d^p, e^q, b^a/bd, e^b/e^{\rho(q,p)}$		$(1-\Delta_p^2)\Delta_{q-1}^p$
$a^p, b^p/c, c^p, d^p, e^q, b^a/bd, e^b/e^{\rho(q,p^2)}, e^c/e^{\rho(q,p)}$		$(1-\Delta_p^2)\Delta_{q-1}^{p^2}$
$a^2/c, b^2/c, c^2, d^2, e^q, b^a/bc, e^a/e^{-1}$		Δ_p^2
$a^2/c, b^2/c, c^2, d^2, e^q, b^a/bc, e^d/e^{-1}$		Δ_p^2
Cluster 10: P has SOT ID $(p^4:10)$		
$a^p/d, b^p/c, c^p, d^p, e^q, b^a/bc, e^b/e^{\rho(q,p)}$		Δ_{q-1}^p
$a^p/d, b^p/c, c^p, d^p, e^q, b^a/bc, e^a/e^{\rho(q,p,k)}$	$k \in \mathbb{Z}_p^*$.	$(p-1)\Delta_{q-1}^p$
$a^p/d, b^p/c, c^p, d^p, e^q, b^a/bc, e^a/e^{\rho(q,p^2,k)}, e^d/e^{\rho(q,p,k)}$	$k \in \mathbb{Z}_p^*$	$(p-1)\Delta_{q-1}^{p^2}$
Cluster 11: P has SOT ID $(p^4:11)$		
$a^p, b^p, c^p, d^p, e^q, b^a/bc, e^d/e^{\rho(q,p)}$		$(1-\Delta_p^2)\Delta_{q-1}^p$
$a^p, b^p, c^p, d^p, e^q, b^a/bc, e^a/e^{\rho(q,p)}$		$(1-\Delta_p^2)\Delta_{q-1}^p$
$a^2, b^2/c, c^2/d, d^2, e^q, b^a/bd, e^a/e^{-1}$		Δ_p^2

$a^2, b^2/c, c^2/d, d^2, e^q, b^a/bd, e^b/e^{-1}$		Δ_p^2
$a^2/c, b^2/d, c^2/d, d^2, e^q, b^a/bd, e^a/e^{\rho(q,4)}, e^c/e^{-1}$		$\Delta_p^2\Delta_{q-1}^4$
$a^2, b^2/c, c^2/d, d^2, e^q, b^a/bd, e^b/e^{\rho(q,4)}, e^c/e^{-1}$		$\Delta_p^2\Delta_{q-1}^4$
Cluster 12: P has SOT ID $(p^4:12)$		
$a^p, b^p/c, c^p, d^p, e^q, b^a/bd, d^a/cd, e^a/e^{\rho(q,p,k)}$	$1 \le k \le \frac{1}{2}(p-1)$	$\frac{1}{2}(p-1-\Delta_p^2)\Delta_{q-1}^p$
$a^p, b^p/c, c^p, d^q, e^q, b^a/bd, d^a/cd, e^b/e^{\rho(q,p)}$		$(1-\Delta_p^2)\Delta_{q-1}^p$
$a^p, b^p/c, c^p, d^p, e^q, b^a/bcd, d^a/cd, d^b/cd, e^a/e^{\rho(q,p,k)}$	$1 \le k \le \frac{1}{2}(p-1)$	$\frac{1}{2}(p-1-\Delta_p^2\Delta_p^3)\Delta_{q-1}^p$
$a^3, b^3/c, c^3, d^3, e^q, b^a/bd^2, d^a/cd, d^b/c^2d, e^a/e^{\rho(q,3)}$		$\Delta_p^3\Delta_{q-1}^3$
$a^2, b^2/c, c^2/d, d^2, e^q, b^a/bc, c^a/cd, e^a/e^{-1}$		Δ_p^2
$a^2, b^2/c, c^2/d, d^2, e^q, b^a/bc, c^a/cd, e^b/e^{-1}$		Δ_p^2
$a^2, b^2/d, c^2/d, d^2, e^q, b^a/bc, c^a/cd, c^b/cd, e^a/e^{-1}$		Δ_p^2
Cluster 13: P has SOT ID $(p^4:13)$		
$a^p, b^p/c, c^p, d^q, e^q, b^a/bd, d^a/c^{r_p}d, e^a/e^{\rho(q,p,k)}$	$1 \le k \le \frac{1}{2}(p-1)$	$\frac{1}{2}(p-1-\Delta_p^2)\Delta_{q-1}^p$
$a^p, b^p/c, c^p, d^q, e^q, b^a/bd, d^a/c^{r_p}d, e^b/e^{\rho(q,p)}$		Δ_{q-1}^p
$a^p, b^p/c, c^p, d^q, e^q, b^a/bcd, d^a/c^{r_p}d, d^b/cd, e^a/e^{\rho(q,p,k)}$	$1 \le k \le \frac{1}{2}(p-1)$	$\frac{1}{2}(p-1)(1-\Delta_p^2\Delta_p^3)\Delta_{q-1}^p$
$a^2, b^2/c, c^2/d, d^2, e^q, b^a/bcd, c^a/cd, e^a/e^{-1}$		Δ_p^2
$a^2, b^2/c, c^2/d, d^2, e^q, b^a/bcd, c^a/cd, e^b/e^{-1}$		Δ_p^2
Cluster 14: P has SOT ID $(p^4:14)$		
$a^p, b^p, c^p, d^p, e^q, c^a/bc, d^a/cd, e^a/e^{\rho(q,p)}$		$(1-\Delta_p^2)\Delta_{q-1}^p$
$a^p, b^p, c^p, d^p, e^q, b^a/bc, c^a/cd, e^d/e^{\rho(q,p)}$		$(1-\Delta_p^2)\Delta_{q-1}^p$
$a^3, b^3/c, c^3, d^3, e^q, b^a/bd, d^a/cd, d^b/cd, e^a/e^{\rho(q,3)}$		$\Delta_p^3\Delta_{q-1}^3$
$a^2/d, b^2/c, c^2/d, d^2, e^q, b^a/bcd, c^a/cd, e^a/e^{-1}$		Δ_p^2
$a^2/d, b^2/c, c^2/d, d^2, e^q, b^a/bcd, c^a/cd, e^b/e^{-1}$		Δ_p^2
Cluster 15: P has SOT ID $(p^4:15)$		
$a^p/b, b^p, c^p, d^p, e^q, c^a/bc, d^a/cd, e^a/e^{\rho(q,p)}$		$(1-\Delta_p^2)(1-\Delta_p^3)\Delta_{q-1}^p$
$a^p/b, b^p, c^p, d^p, e^q, c^a/bc, d^a/cd, e^d/e^{\rho(q,p)}$		$(1-\Delta_p^2)(1-\Delta_p^3)\Delta_{q-1}^p$
$a^3/c, b^3/c, c^3, d^3, e^q, b^a/bd, d^a/c^2d, e^a/e^{\rho(q,3)}$		$\Delta_p^3\Delta_{q-1}^3$
$a^3/c, b^3/c, c^3, d^3, e^q, b^a/bd, d^a/c^2d, e^b/e^{\rho(q,3)}$		$\Delta_p^3\Delta_{q-1}^3$

TABLE 8.2: Non-nilpotent groups of order p^4q with a normal Sylow subgroup P (the isomorphism types and SOT IDs of P are given in Table 5.3); $\mathrm{Irr}_2(p^2,q)$ has multiplicative order q in the ring of 2×2 matrices over $\mathbb{Z}_{p^2}$ and $\mathrm{Irr}_2(p^2,q)\equiv \mathrm{Irr}_2(p,q) \bmod p$.

PC-relators	Parameters	Number of groups
Cluster 1: $P\cong C_{p^4}$		
$a^q, b^{p^4}, b^a/b^{\rho(p^4,q)}$		Δ_{p-1}^q
Cluster 2: $P\cong C_{p^3}\times C_p$		
$a^q, b^{p^3}, c^p, b^a/b^{\rho(p^3,q)}$		Δ_{p-1}^q
$a^q, b^{p^3}, c^p, c^a/c^{\rho(p,q)}$		Δ_{p-1}^q
$a^q, b^{p^3}, c^p, b^a/b^{\rho(p^3,q)}, c^a/c^{\rho(p,q,k)}$	$k\in\mathbb{Z}_q^*$	$(q-1)\Delta_{p-1}^q$
Cluster 3: $P\cong C_{p^2}\times C_{p^2}$		
$a^q, b^{p^2}, c^{p^2}, b^a/b^{\rho(p,q)}$		Δ_{p-1}^q
$a^q, b^{p^2}, c^{p^2}, b^a/b^{\rho(p^2,q,\sigma_q^k)}, c^a/c^{\rho(p^2,q)}$	$0\le k\le \frac{1}{2}(q-1)$	$\frac{1}{2}(q+1-\Delta_q^2)\Delta_{p-1}^q$
$a^q, b^{p^2}, c^{p^2}, (b^a,c^a)/(b,c)^{\mathrm{Irr}_2(p^2,q)}$		$(1-\Delta_q^2)\Delta_{p+1}^q$
Cluster 4: $P\cong C_{p^2}\times C_p^2$		
$a^q, b^p, c^p, d^{p^2}, b^a/b^{\rho(p,q)}$		Δ_{p-1}^q
$a^q, b^p, c^p, d^{p^2}, (b^a,c^a)/(b,c)^{M(p,q,\sigma_q^k)}$	$0\le k\le \frac{1}{2}(q-1)$	$\frac{1}{2}(q+1-\Delta_q^2)\Delta_{p-1}^q$
$a^q, b^p, c^p, d^{p^2}, (b^a,c^a)/(b,c)^{\mathrm{Irr}_2(p,q)}$		$(1-\Delta_q^2)\Delta_{p+1}^q$
$a^q, b^p, c^p, d^{p^2}, d^a/d^{\rho(p^2,q)}$		Δ_{p-1}^q
$a^q, b^p, c^p, d^{p^2}, b^a/b^{\rho(p,q,k)}, d^a/d^{\rho(p^2,p)}$	$k\in\mathbb{Z}_q^*$	$(q-1)\Delta_{p-1}^q$
$a^q, b^p, c^p, d^{p^2}, b^a/b^{\rho(p,q,k)}, c^a/c^{\rho(p,q,\ell)}, d^a/d^{\rho(p^2,q)}$	$k<\ell\in\mathbb{Z}_q^*$	$\frac{1}{2}(q^2-3q+2)\Delta_{p-1}^q$
$a^q, b^p, c^p, d^{p^2}, (b^a,c^a)/(b,c)^{M(p,q)}, d^a/d^{\rho(p^2,q,k)}$	$k\in\mathbb{Z}_q^*$	$(q-1)\Delta_{p-1}^q$
Cluster 5: $P\cong C_p^4$		
$a^q, b^p, c^p, d^p, e^p, b^a/b^{\rho(p,q)}$		Δ_{p-1}^q
$a^q, b^p, c^p, d^p, e^p, (b^a,c^a)/(b,c)^{M(p,q,\sigma_q^k)}$	$0\le k\le \frac{1}{2}(q-1)$	$\frac{1}{2}(q+1-\Delta_q^2)\Delta_{p-1}^q$
$a^q, b^p, c^p, d^p, e^p, b^a/b^{\rho(p,q)}, c^a/c^{\rho(p,q)}, d^a/d^{\rho(p,qk)}$	$1\le k\le q-1$	$(q-1)\Delta_{p-1}^q$
$a^q, b^p, c^p, d^p, e^p, b^a/b^{\rho(p,q)}, c^a/c^{\rho(p,q,\sigma_q^k)}, d^a/d^{\rho(p,q,\sigma_q^\ell)}$	$(k,\ell)\in\mathcal{P}_1$	$\frac{1}{6}(q^2-5q+6+4\Delta_{q-1}^3)\Delta_{p-1}^q$
$a^q, b^p, c^p, d^p, e^p, b^a/b^{\rho(p,q)}, c^a/c^{\rho(p,q)}, d^a/d^{\rho(p,q)}, e^a/e^{\rho(p,q,\sigma_q^k)}$	$0\le k\le q-2$	$(q-1)\Delta_{p-1}^q$
$a^q, b^p, c^p, d^p, e^p, b^a/b^{\rho(p,q)}, c^a/c^{\rho(p,q)}, d^a/d^{\rho(p,q,\sigma_q^k)}, e^a/e^{\rho(p,q,\sigma_q^k)}$	$1\le k\le \frac{1}{2}(q-1)$	$\frac{1}{2}(q-1-\Delta_q^2)\Delta_{p-1}^q$
$a^q, b^p, c^p, d^p, e^p, b^a/b^{\rho(p,q)}, c^a/c^{\rho(p,q)}, d^a/d^{\rho(p,q,\sigma_q^k)}, e^a/e^{\rho(p,q,\sigma_q^\ell)}$	$1\le k<\ell\le q-2$	$\frac{1}{2}(q^2-5q+6)\Delta_{p-1}^q$
$a^q, b^p, c^p, d^p, e^p, b^a/b^{\rho(p,q)}, c^a/c^{\rho(p,q,\sigma_q^k)}, d^a/d^{\rho(p,q,\alpha^\ell)}, e^a/e^{\rho(p,q,\sigma_q^m)}$	$(k,\ell,m)\in\mathcal{P}_2$	$\frac{1}{24}(q^3-9q^2+29q-33+12\Delta_{q-1}^4+27\Delta_q^2)\Delta_{p-1}^q$
$a^q, b^p, c^p, d^p, (b^a,c^a)/(b,c)^{\mathrm{Irr}_2(p,q)}$		$(1-\Delta_q^2)\Delta_{p+1}^q$
$a^q, b^p, c^p, d^p, (b^a,c^a,d^a)/(b,c,d)^{\mathrm{Irr}_3(p,q)}$		$(1-\Delta_q^3)\Delta_{p^2+p+1}^q$
$a^q, b^p, c^p, d^p, e^p, (b^a,c^a)/(b,c)^{\mathrm{Irr}_2(p,q)}, (d^a,e^a)/(d,e)^{(\mathrm{Irr}_2(p,q)^{\sigma_q^k})}$	$0\le k\le \frac{1}{4}(p-1)$	$\frac{1}{4}(q+1+2\Delta_{q-1}^4)(1-\Delta_q^2)\Delta_{p+1}^q$

$a^q, b^p, c^p, d^p, e^p, (b^a, c^a, d^a, e^a)/(b,c,d,e)^{\mathrm{Irr}_4(p,q)}$		$(1-\Delta_q^2)\Delta_{p^2+1}^q$
Cluster 6: P has SOT ID $(p^4:6)$		
$a^q, b^p, c^p, d^p/e, e^p, c^b/ce, b^a/b^{p(p,q,q-1)}, c^a/c^{\rho(p,q)}$		Δ_{p-1}^q
$a^q, b^p, c^{p^2}, d^p, d^b/c^p d, b^a/b^{p(p,q)}, c^a/c^{\rho(p^2,q)}$		Δ_{p-1}^q
$a^q, b^p, c^{p^2}, d^p, d^b/c^p d, b^a/b^{p(p,q,q+1-k)}, c^a/c^{\rho(p^2,q)}, d^a/d^{p(p,q,k)}$	$2 \le k \le \frac{1}{2}(q+1)$	$\frac{1}{2}(q-1-\Delta_q^2)\Delta_{p-1}^q$
$a^q, b^p, c^p, d^p/e, e^p, c^b/ce, (b^a, c^a)/(b,c)^{\mathrm{Irr}_2(p,q)}$		$(1-\Delta_q^2)(1-w_p^2)\Delta_{p+1}^q$
$a^3, b^2/e, c^2/e, d^2/e, e^p, c^a/d, d^a/cd, d^c/de$		$w_p^2 w_q^3$
Cluster 7: P has SOT ID $(p^4:7)$		
$a^q, b^p, c^{p^3}, c^b/c^{1-p^2}, c^a/c^{\rho(p^3,q)}$		Δ_{p-1}^q
Cluster 8: P has SOT ID $(p^4:8)$		
$a^q, b^p, c^{p^2}, d^p, c^b/c^{p+1}, d^a/d^{p(p,q)}$		Δ_{p-1}^q
$a^q, b^p, c^{p^2}, d^p, c^b/c^{p+1}, c^a/c^{\rho(p^2,q)}$		Δ_{p-1}^q
$a^q, b^p, c^{p^2}, d^p, c^b/c^{p+1}, c^a/c^{\rho(p^2,q)}, d^a/d^{p(p,q,k)}$	$k \in \mathbb{Z}_q^*$	$(q-1)\Delta_{p-1}^q$
Cluster 9: P has SOT ID $(p^4:9)$		
$a^q, b^p, c^{p^2}, d^p, c^b/cd, b^a/b^{p(p,q)}, d^a/d^{p(p,q)}$		Δ_{p-1}^q
$a^q, b^p, c^{p^2}, d^p, c^b/cd, b^a/b^{p(p,q,q-1)}, c^a/c^{\rho(p^2,q)}$		Δ_{p-1}^q
$a^q, b^p, c^{p^2}, d^p, c^b/cd, b^a/b^{p(p,q)}, c^a/c^{\rho(p^2,q)}, d^a/d^{\rho(p,q,k+1)}$	$1 \le k \le q-2$	$(q-2)\Delta_{p-1}^q$
$a^q, b^p, c^{p^2}, d^p, c^b/cd, c^a/c^{\rho(p^2,q)}, d^a/d^{\rho(p,q)}$		Δ_{p-1}^q
$a^3, b^2/d, c^2/d, d^2, e^2, c^b/cd, b^a/c, c^a/bc$		$\Delta_p^2\Delta_q^3$
Cluster 10: P has SOT ID $(p^4:10)$		
$a^q, b^p/d, c^{p^2}, d^p, c^b/c^{p+1}, c^a/c^{\rho(p^2,q)}$		Δ_{p-1}^q
Cluster 11: P has SOT ID $(p^4:11)$		
$a^q, b^p, c^p, d^p, e^p, c^b/cd, b^a/b^{p(p,q,q-1)}, c^a/c^{\rho(p,q)}$		Δ_{p-1}^q
$a^q, b^p, c^p, d^p, e^p, c^b/cd, e^a/e^{\rho(p,q)}$		Δ_{p-1}^q
$a^q, b^p, c^p, d^p, e^p, c^b/cd, b^a/b^{p(p,q)}, d^a/d^{p(p,q)}$		Δ_{p-1}^2
$a^q, b^p, c^p, d^p, e^p, c^b/cd, b^a/b^{p(p,q,q+1-k)}, c^a/c^{\rho(p,q,k)}, d^a/d^{p(p,q)}$	$2 \le k \le \frac{1}{2}(q+1)$	$\frac{1}{2}(q-1-\Delta_q^2)\Delta_{p-1}^q$
$a^q, b^p, c^p, d^p, e^p, c^b/cd, b^a/b^{p(p,q)}, c^a/c^{\rho(p,q,q-1)}, e^a/e^{\rho(p,q,k)}$	$1 \le k \le \frac{1}{2}(q-1)$	$\frac{1}{2}(q-1-\Delta_q^2)$
$a^q, b^p, c^p, d^p, e^p, c^b/cd, c^a/c^{\rho(p,q)}, d^a/d^{\rho(p,q)}, e^a/e^{\rho(p,q,k)}$	$k \in \mathbb{Z}_q^*$	$(q-1)\Delta_{p-1}^q$
$a^q, b^p, c^p, d^p, e^p, c^b/cd, b^a/b^{p(p,q)}, c^a/c^{\rho(p,q,\sigma_q^\ell+1)}, d^a/d^{\rho(p,q,\sigma_q^\ell+1)}, e^a/e^{\rho(p,q,k)}$	$(k,\ell) \in \mathcal{P}_3$	$\frac{1}{2}(q^2-2q+1)(1-\Delta_q^2)\Delta_{p-1}^q$
$a^2, b^p, c^p, d^p, e^p, c^b/cd, b^a/b^{-1}, c^a/c^{-1}, e^a/e^{-1}$		Δ_q^2
$a^q, b^p, c^p, d^p, e^p, c^b/cd, (b^a, c^a)/(b,c)^{\mathrm{Irr}_2(p,q)}$		$(1-\Delta_q^2)(1-\Delta_p^2)\Delta_{p+1}^q$
Cluster 12: P has SOT ID $(p^4:12)$		
$a^q, b^p, c^{p^2}, d^p, c^b/cd, d^b/c^p d, c^a/c^{\rho(p^2,q)}, d^a/d^{\rho(p,q)}$		$(1-\Delta_q^2)\Delta_{p-1}^q$
$a^2, b^p, c^{p^2}, d^p, c^b/cd, d^b/c^p d, b^a/b^{-1}, d^a/c^p d^{-1}$		Δ_q^2
$a^2, b^p, c^{p^2}, d^p, c^b/cd, d^b/c^p d, c^a/c^{-1}, d^a/d^{-1}$		Δ_q^2

$a^2, b^p, c^{p^2}, d^p, c^b/cd, d^b/c^p d, b^a/b^{-1}, c^a/c^{-1}, d^a/c^{-p}d$		Δ_q^2
Cluster 13: P has SOT ID $(p^4:13)$		
$a^q, b^p, c^{p^2}, d^p, c^b/cd, d^b/c^{\sigma_p p}d, c^a/c^{\rho(p^2,q)}, d^a/d^{\rho(p,q)}$		$(1-\Delta_q^2)\Delta_{p-1}^q$
$a^2, b^p, c^p/d^{\sigma_p}, d^p, e^p, c^b/ce, e^b/de, b^a/b^{-1}, e^a/de^{-1}$		Δ_q^2
$a^2, b^p, c^{p^2}, d^p, c^b/cd, d^b/c^{\sigma_p p}d, c^a/c^{-1}, d^a/d^{-1}$		Δ_q^2
$a^2, b^p, c^p/d^{\sigma_p}, d^p, e^p, c^b/ce, e^b/de, b^a/b^{-1}, c^a/c^{-1}d^{-\sigma_p}, d^a/d^{-1}, e^a/d^{-1}e$		Δ_q^2
Cluster 14: P has SOT ID $(p^4:14)$		
$a^q, b^p, c^p, d^p, e^p, d^b/cd, e^b/de, b^a/b^{\rho(p,q)}, d^a/c^{\frac{1}{2}\rho(p,q,q-1)(\rho(p,q)-1)}d^{\rho(p,q,q-1)}, e^a/e^{\rho(p,q,q-2)}$		Δ_{p-1}^q
$a^q, b^p, c^p, d^p, e^p, d^b/cd, e^b/de, b^a/b^{\rho(p,q,k)}, c^a/c^{\rho(p,q)}, d^a/c^{\frac{1}{2}(rho(p,q)-rho(p,q,q+1-k))}d^{\rho(p,q,q+1-k)}, e^a/e^{\rho(p,q,q+1-2k)}$	$k \in \mathbb{Z}_q$	$q\Delta_{p-1}^q$
Cluster 15: P has SOT ID $(p^4:15)$		
$a^q, b^p, c^p, d^{p^2}, d^b/c^{-1}d^{p+1}, d^c/d^{1-p}, b^a/b^{\rho(p,q,q-1)}, c^a/cd^{\frac{1}{2}p(\rho(p,q)-1)}, d^a/d^{\rho(p^2,q)}$		$(1-\Delta_p^3)\Delta_{p-1}^q$
$a^2, b^3/d, c^3/d, d^3, e^3, c^b/ce, e^b/d^2e, b^a/b^2d^2, c^a/c^2d^2, d^a/d^2, e^a/de$		$\Delta_q^2\Delta_p^3$
Parameter sets		

$$\mathcal{P}_1 = \begin{cases} \{(x,y) \in \mathbb{Z}_{q-1}^2 \,:\, 1 \le x \le \frac{1}{3}(q-2),\ \ 2x \le y \le q-2-x\} & (q \equiv 2 \bmod 3) \\ \{(x,y) \in \mathbb{Z}_{q-1}^2 \,:\, 1 \le x \le \frac{1}{3}(q-1),\ \ 2x \le y \le q-2-x\} \cup \{(\frac{1}{3}(q-1), \frac{2}{3}(q-1))\} & (q \equiv 1 \bmod 3) \end{cases}$$

$$\mathcal{P}_2 = \{(x,y,z) \in \mathbb{Z}_{q-1}^3 : 1 \le x \le \tfrac{1}{4}(q-1), 2x \le y \le \tfrac{1}{2}(q-1), x+y \le z \le q-2-x\}$$
$$\cup \{(x,y,z) \in \mathbb{Z}_{q-1}^3 : 1 \le x \le \tfrac{1}{4}(q-1), \tfrac{1}{2}(q+1) \le y \le q-1-2a, x+y+1 \le z \le q-2-x\}$$
$$\cup \{(\tfrac{1}{4}(q-1), \tfrac{1}{2}(q-1), \tfrac{3}{4}(q-1)) : q = 1 \bmod 4\}$$

$$\mathcal{P}_3 = \{(x,y) \in \mathbb{Z}_q^{*2} : x \in \mathbb{Z}_q^*, 0 \le y \le \tfrac{1}{2}(q-3)\}$$

TABLE 8.3: Groups of order p^4q without normal Sylow subgroup

PC-relators	Structure	Number of groups
$\lvert G\rvert = 48$		
$a^2, b^2, c^3, d^2, e^2, c^b/c^2, d^b/e, e^b/d, d^c/de$	$C_2 \times \mathrm{Sym}_4$	$\Delta_p^2\Delta_q^3$
$a^2/b, b^2, c^3, d^2, e^2, c^a/c^2, d^a/e, e^a/d, d^c/e, d^c/de$	$C_4 \ltimes \mathrm{Alt}_4$	$\Delta_p^2\Delta_q^3$
$a^2, b^3, c^2/e, d^2/e, e^2, b^a/b^2, c^a/d, d^a/c, c^b/de, d^b/cd, d^c/de$	$C_2 \ltimes (C_3 \ltimes Q_8)$	$\Delta_p^2\Delta_q^3$
$a^2/e, b^3, c^2/e, d^2/e, e^2, b^a/b^2, c^a/d, d^a/c, c^b/de, d^b/cd, d^c/de$	$C_2.(C_3 \ltimes Q_8)$	$\Delta_p^2\Delta_q^3$
$\lvert G\rvert = 3^4{\cdot}13$		
$a^3, b^{13}, c^3, d^3, e^3, b^a/b^{\rho(13,3)}, c^a/de, d^a/c^2d^2e, e^a/cd^2e, (c^b, d^b, e^b)/(c,d,e)^{\mathrm{Irr}_3(3,13)}$	$C_3 \ltimes (C_{13} \ltimes C_3^3)$	$\Delta_p^3\Delta_q^{13}$

8.2 The SOTGrps package

We have implemented the results in the preceding section and previous chapters in GAP and developed a package called SOTGrps, available at github.com/xpan-eileen/sotgrps_gap_pkg. This section gives an introduction to this package and we briefly comment on its main functionalities. We plan to extend the package by adding more functions and more order types, but this is beyond the scope of this thesis.

Let p, q, r, s be distinct primes. At the time of writing, the SmallGroups library of GAP [27] contains the following orders discussed in this paper: p^2q for all primes $p \neq q$, and p^nq for primes $p \neq q$ with p^n dividing one of $\{2^8, 3^6, 5^5, 7^4\}$ and all relevant orders up to 2000. Our package SOTGrps is available for

- p-groups of order dividing p^4;
- groups of order p^nq where $n \leq 4$;
- groups of order p^2q^2;
- groups of order dividing $pqrs$;
- groups of order p^2qr.

`SOTGroupIsAvailable(n) = true` if n is one of these order types. We remark that our package provides new efficient functionalities for orders p^2q^2 and $p2qr$ that are greater than 2000, and orders p^3q and p^4q with $p > 7$. At the time of writing, SOTGrps contains the following main functions for integers n such that `SOTGroupIsAvailable(n) = true`; these functions constitute a dynamic database of SOTGrps; that is, the package computes efficiently the following information on demand.

- `NumberOfSOTGroups`(n): returns the number $\mathcal{G}(n)$ of isomorphism types $\mathcal{G}(n)$ of groups of order n.
- `AllSOTGroups`(n): returns a list $\mathcal{L}_n$ of all isomorphism class representatives of groups of order n.
- `SOTGroup`(n, i): for $i \in \{1, \ldots, \mathcal{G}(n)\}$, returns the i-th group in the ordered list $\mathcal{L}_n$ without constructing the whole list $\mathcal{L}(n)$.

- `IdSOTGroup`(G): for a group G of order n, returns the SOT[1] ID (n, i), such that G is isomorphic to `SOTGroup`(n, i).

8.2.1 Explicit constructions

For an order n such that `SOTGroupIsAvailable(n) = true`, the list $\mathcal{L}_n$ is determined by making various case distinctions on the structure of the groups of order n. Distinguishing features such as nilpotency, the existence of normal Sylow subgroups, size of the centre, the structure of the derived subgroup, and the structure of the Fitting subgroup are to be considered. Such case distinctions partition $\mathcal{L}_n$ into various *clusters*. The counting formulas for $|\mathcal{L}_n|$ thus consist of the enumeration of the isomorphism types of these groups in each cluster. Since we construct these groups by group extensions, the clusters are further sorted by the group extension decomposition: that is, the structure of the normal subgroup N and the factor group U such that G is an extension of N by U. Moreover, two split extensions of N by U in the same cluster only differ by the U-action on N; these actions are parametrised in a canonical way with respect to the canonical automorphisms defined in Chapter 4. This parametrisation is explained in the proofs of the main theorems in Chapters 5, 6, 7, and Appendix B, and demonstrated in the *Parameter* columns of the tables. Since the enumeration of each cluster reflects the number of parameters (given in the right columns in the tables), these counting formulas are the key ingredients that allow us to directly construct the i-th group in $\mathcal{L}_n$ *without* constructing the whole list of groups. A similar approach is used for the construction functionality provided by the SmallGroups library and by the algorithms in [21]. The following example is a demonstration of this process for groups of order p^2q.

Example 8.2.1. Let $n = p^2q$ with $q > 2$. The proof of Theorem 6.1.1 partitions the groups in $\mathcal{L}_n$ into five cluster as given in Table 6.1. The groups in Cluster 1 are nilpotent and can be sorted by the isomorphism types of the Sylow p-subgroup. Cluster 2 exists only if $q \mid (p+1)(p-1)$; Cluster 3 exists only if $p \mid (q-1)$; Clusters 4 and 5 exist only if $p \mid (q-1)$. To be more specific, Clusters 2 and 3 comprise non-nilpotent groups with a normal Sylow p-subgroup. That is, Clusters 2–4 consists of non-nilpotent split extensions $P \rtimes Q$ and $Q \rtimes P$, where P has order p^2 and $Q \cong C_q$. In the case where P is cyclic, there exists a non-nilpotent extension $Q \rtimes P$ only if $q \mid (p-1)$; such group is unique up to isomorphism. For the other case where P is elementary abelian, we can apply Theorem 4.2.7 since $\mathrm{Aut}(P) \cong \mathrm{GL}_2(p)$. If $q \mid (p+1)$, then Q acts irreducibly on P and the centre of $Q \rtimes P$ is trivial; there is a unique isomorphism type of this split extension. If $q \mid (p-1)$, then there are $\frac{1}{2}(q+3)$ types of $Q \rtimes P$ and they are parametrised by the conjugacy classes of diagonalisable subgroups of $\mathrm{GL}_2(p)$ of order q as seen in the proof of Theorem 4.2.7(ii). The proof also explains how to list these classes canonically: if $\sigma_p \in \mathbb{Z}_p^*$ and $\sigma_q \in \mathbb{Z}_q^*$ are the canonical generators and $\rho(p,q) = \sigma_p^{(p-1)/q}$, then the subgroups C_q in $\mathrm{GL}_2(p)$ are sorted as $\langle \mathrm{diag}(\rho(p,q), 1)\rangle$ and $\langle M(p,q,\sigma_q^k))\rangle$ with $k \in \{0, \ldots, \frac{1}{2}(q-1)\}$ using canonical automorphisms defined in Notations 4.1.1 and 4.2.1. On the other hand, if $p \mid (q-1)$, then Cluster 2 and 3 are empty, whereas Cluster 4 and 5 consist of at least two isomorphism types of non-nilpotent groups with a normal Sylow q-subgroup; there are two isomorphism types in Cluster 5 if and only if $p^2 \mid (q-1)$.

We now exemplify some explicit cases. If $n = 29^2 \cdot 7$, then Clusters 1-5 have 2, 5, 1, 0, 0 groups, respectively. The group G with ID $(29^2 \cdot 7, 6)$ is in Cluster 2, and $G \cong C_7 \rtimes C_{29}^2$ where a generator

[1] We remark that the ordering of $\mathcal{L}_n$ constructed by `AllSOTGroups`(n) may differ from the ordering imposed by `AllSmallGroups`(n) in GAP's Small Group Library (if applicable). Hence for a group G implemented in GAP, `IdSmallGroup`(G) and `IdSOTGroup`(G) do not necessarily coincide. In this thesis, by ID we always refer to the SOT ID given in `SOTGrps`.

$u \in C_7$ acts on generators $v, w \in C_{29}^2$ via $M(29,7,\sigma_7^2) = \mathrm{diag}(\rho(p,q), \rho(p,q,\sigma_7^2))$; here $\sigma_{29} = 2$ and $\sigma_7 = 3$, so $\rho(29,7) = \sigma_{29}^4 = 16$ and $\rho(29,7,\sigma_7^2) = 24$. Hence, we construct G by the (so-called canonical) pc-presentation $\mathrm{Pc}\langle u, v, w \mid u^7, v^{29}, w^{29}, v^u/v^{16}, w^u/w^{24}\rangle$. If $n = 7^2{\cdot}29$, then Clusters 1-5 have 2, 0, 0, 1, 1 groups, respectively. In this case, we see that there exists no groups of such order that has a trivial centre. The group G with ID $(7^2{\cdot}29, 3)$ is in Cluster 4 and $G \cong C_{7^2} \ltimes C_{29}$ where a generator $u \in C_{7^2}$ acts on a generator $v \in C_{29}$ via an automorphism $\rho(29,7)$ of order 7; we construct G by the pc-presentation $\mathrm{Pc}\langle u, v \mid u^{49}, v^{29}, v^u = v^{16}\rangle$.

8.2.2 Group IDs

Many applications of group theory use the classification of finite groups of a given order. More specifically, given an arbitrary group G of order n, we often want to know the *isomorphism type* of G; that is, which group in the list of isomorphism class representatives $\mathcal{L}_n$ is G isomorphic to? In theory, once the list $\mathcal{L}_n$ is known, this question can be answered by exhaustively testing whether $G \cong H$ for each $H \in \mathcal{L}_n$. However, when $|\mathcal{L}_n|$ and n are large, this approach is practically inefficient. This motivates our goal of finding an identification function for groups of order n that computes a complete isomorphism invariant. As mentioned in the Introduction, the group ID inherited from the canonical ordering of $\mathcal{L}_n$ is such a complete invariant. For example, we saw that the isomorphism classes of groups of a given order type are partitioned into subclasses by various case distinctions, and in each subclass there is a natural ordering on the parametrised isomorphism representatives with respect to the canonical choices of automorphisms of groups.

Reversing the construction process, we find an identification function that computes the group ID of a given group G, namely, the position of the unique group H in the ordered list $\mathcal{L}_n$ such that $H \cong G$. To be more specific, we first determine the order type of $|G|$ and depending on the order type we choose to compute its Sylow subgroups, centre, derived subgroup, or Fitting subgroup to determine which cluster it belongs to. For order types that are discussed in this thesis, if G is nonsolvable, then we know $G \cong \mathrm{Alt}_5$ and we are done. If G is solvable, then we compute a parametrised pc-presentation of G with respect to our canonical choices of automorphisms and determine the value of the parameter. This translates to the position of G in its respective cluster, from which we further deduce its position in $\mathcal{L}_n$, namely, the group ID. We exemplify this process for an explicit group as follows.

Example 8.2.2. Consider the group $G = \langle u, v, w \mid u^7,\ v^{29},\ w^{29},\ w^v/w,\ v^u/v^{24},\ w^u/v^{11}w^7\rangle$. We first determine $n = |G| = 29^2{\cdot}7$ and compute a Sylow 29-subgroup P and a Sylow 7-subgroup Q. We find that $C_{29}^2 \cong P \trianglelefteq G$, so $G \cong Q \ltimes C_{29}^2$. This tells us that G is a group of order p^2q in Cluster 2 as given in Table 6.1 with $p = 29$ and $q = 7$. Moreover, since $7 \mid (29-1)$ and $Z(G)$ is trivial, we know that G has ID $(29^2{\cdot}7, 2+2+k)$, where $k \in \{1, 23\}$ is the parameter of the canonical pc-presentation of G with respect to the canonical Q-action on P. If G is given as a matrix or permutation group, then we need to firstly choose a suitable pcgs and compute a pc-presentation of G, but in this case we can use the given presentation with generators $u \in Q$ and $v, w \in P$ and observe that $v^u = v^{24}$ and $w^u = v^{11}w^7$. This gives the matrix representation of u acting on v, w via $\left(\begin{smallmatrix} 24 & 0 \\ 11 & 7 \end{smallmatrix}\right) \in \mathrm{GL}_2(29)$. This matrix has eigenvalues $\{24, 7\}$, so it is conjugate to $\mathrm{diag}(24,7) = \mathrm{diag}(\rho(29,7,2), \rho(29,7,3))$ with $\rho(29,7) = 16$. Since u^4 is also a generator of Q, we can raise the matrix to its power of 4, which yields $\mathrm{diag}(\rho(29,7), \rho(29,7,3^5)) = M(29,7,\sigma_7^5)$, and it represents the same Q-action on P. That is, G has a canonical pc-presentation of the form $\mathrm{Pc}\langle a, b, d \mid a^7, b^{29}, c^{29}, (b^a, c^a) = (b,c)^{M(29,7,\sigma_7^5)}\rangle$. From this we obtain parameter 5, but our canonical choices of representatives are parametrised by $k \in \{0, \ldots, \frac{1}{2}(q-1) = 3\}$. We thus look for a parameter $k \in \{0, \ldots, 3\}$ such that $\langle M(29,7,\sigma_7^5)\rangle$ and $\langle M(29,7,\sigma_7^k)\rangle$ are conjugate in

$\mathrm{GL}_2(29)$: since $3^{-5 \bmod (q-1)} = 3$ in $\mathbb{Z}_7^*$, following the proof of Theorem 4.2.7(i) we determine the parameter $k = 1$. Therefore, G has ID $(29^2 \cdot 7, 5)$.

8.2.3 Accuracy of results

SOTGrps arises from the implementation of our classification results. The proofs are constructive and mainly rely on Theorem 2.4.2 in Chapter 2 and Theorem 4.2.7 in Chapter 4 and the resulting corollaries. We compared our enumeration results with [24] and [37] and confirmed that our counting formulas derived from explicit constructions and the formulas from counting subgroup classes coincide. Moreover, for orders that are available in GAP's SmallGroups library, we checked our results against the existing database. We also compared our construction with that obtained by the GrpConst package (see [6]) and the Cubefree package (see [22]) for a larger range of orders that are not yet available in the SmallGroups library. The identification function is derived by reversing the construction process, as exemplified in Example 8.2.2, which involves choosing a pcgs and computing a presentation if the input is a solvable group. In particular, once a presentation is chosen, we often need to compute the module structure and calculate its parameter with respect to our canonical choices. One useful test is to feed the function with multiple "random" copies[2] of the same group and check whether it outputs the same, correct ID. This way we ensure that the identification function handles different inputs properly, and we avoid doing ad-hoc computations that rely on the input already given in a canonical form.

In practice, we tried to avoid typos and errors introduced by data transcription by cross-checking our GAP implementation with the proofs and the tables. After we compared SOTGrps with other existing packages, we checked our tables again by reimplementing the lists of pc-presentations in GAP and confirmed that they match the SOTGrps output.

8.2.4 Performance

We now comment on the performance of SOTGrps: all computations were carried out with GAP 4.11.0 on a computer with Intel(R) Core(TM) i5-7500 CPU@3.40GHz and 16GB RAM.[3]

- There are 20514 groups of order p^2q at most 10^5. SmallGroups required 196 seconds to construct these groups, while our code took 16 seconds. Our code identified the groups constructed with SmallGroups in 78 seconds, whereas SmallGroups required 778 seconds to identify our groups. There are 159800 groups of order up to 10^6 and our code required 120 seconds for the construction of these groups; SmallGroups took 15181 seconds. The reason for the increased runtime required for SmallGroups is because for some order types the construction involves some computations (also causing longer runtime for the order types described below), whereas our code directly writes down the group presentations.
- Among the 74844 groups of order p^2q, p^3q, p^2q^2 or p^2qr at most 50000, there are 74562 that are available in the SmallGroups library. Our code required 47 seconds to construct

[2] For this purpose, we used GAP to generate three to five "random" permutation group copies and five "random" PcGroup copies, and verified that the identification function returned the same, correct group ID.

[3] All our runtimes were determined by using the option USE_NC:=true in our code: this prevents GAP from checking consistency of polycyclic presentations, which becomes a major bottleneck when large primes are involved.

these groups, whereas SmallGroups required 27359 seconds. Moreover, SmallGroups took 43356 seconds to identify our groups, while our code required 259 seconds to identify the groups constructed with SmallGroups. It required 0.2 seconds for our code to construct the remaining 282 groups.

- Our code is also practical for larger primes. For example, the construction of the 37371, 6566, and 21348 groups of order $9341^3 \cdot 467$, $127691^2 \cdot 113^2$, and $415631^2 \cdot 467 \cdot 89$ took 32, 5, and 17 seconds, respectively.[4] For such large orders we cannot compare our results with those of `GrpConst` or `Cubefree`, because the latter computations do not terminate in a reasonable period of time (within a few hours). This is partly because these packages use general-purpose algorithms which invoke computations with group homomorphisms and matrix groups (bottlenecks akin to this also occur to other order types). Our code avoids these bottlenecks by directly writing down polycyclic presentations of the (solvable) groups; the main bottleneck in our code seems to be GAP's pc-group arithmetic for large primes.

- At the time of writing, the SmallGroup library does not cover groups of order p^4q except for the special cases where p is at most 7 as mentioned before. `GrpConst` can in theory be used to construct these groups, but it tends to be less efficient than `SOTGrps` and does not terminate within a reasonable time even for "small" orders such as $19^4 \cdot 3$. For even smaller orders such as $11^5 \cdot 5 = 73205$, which is not yet available in the SmallGroup library, `GrpConst` required 326 seconds to construct the list of all groups while `SOTGrps` only took 0.07 seconds. More importantly, `SOTGrps` offers an identification function for groups of order p^4q while `GrpConst` does not.

8.3 Future work

In `SOTGrps` we use the canonical ordering of $\mathcal{L}_n$ to assign each group an ID, and the reverse process leads to an identification function. A closely related problem is to compute an isomorphism between two groups with the same group ID. At the time of writing, the SmallGroup library only offers a generic isomorphism function constructed by first principles (see `IsomorphismGroups` in GAP Manual [27]). In light of Theorem 2.4.2 and the subsequent corollaries, we can improve this isomorphism function using our explicit construction results. For instance, if two groups G_1, G_2 both have group ID (n, x), then to compute an isomorphism $i\colon G_1 \to G_2$, we first determine a canonical copy $G \in \mathcal{L}_n$ that is the isomorphism class representative with ID (n, x). Once the groups are identified and are isomorphic, we know that they can be constructed as extensions of the same building blocks by Theorem 2.1.3. For example, many of the groups considered in this thesis and in `SOTGrps` are split extensions with few exceptions and we know that two such extensions only differ in the module structure. Theorem 2.4.2 shows that to find the isomorphism it suffices to compute and compare these group actions and determine the conjugate element that relates the two actions (see Section 2.4). Then we compute an isomorphism $i_1\colon G_1 \to G$ and similarly an isomorphism $i_2\colon G_2 \to G$. The composition map $i = i_2^{-1} \circ i_1$ is an isomorphism as desired. Having such an isomorphism function will not only make the package more complete but will also provide more practical tools for the study of these groups and may shed light on relevant applications.

[4] The performance of our code is even better (5, 1, and 3 seconds, respectively) if groups are returned as GAP objects `pcp-group` (instead of `pc-group`) by setting USE_PCP:=true.

Appendix A

Preliminary results

We briefly recall some definitions and preliminary results that are used in this thesis. For details and proofs we refer to standard textbook references, such as [33], [35], [43], and [45].

Theorem A.0.1 (Frattini). *If G is a finite group, then its Frattini subgroup $\Phi(G)$ is nilpotent.*

Theorem A.0.2 (Frattini's argument). *If G is a finite group with normal subgroup H, and P is a Sylow subgroup of H. Then $G = N_G(P)H$.*

Lemma A.0.3 ([35], 1A.1). *Let G be a group and H a subgroup of G. If $[G\colon H] = p$, where p is the smallest prime dividing $|G|$, then $H \lhd G$.*

Theorem A.0.4 (Burnside). *If G is a group of exponent 2, then G is abelian.*

Theorem A.0.5 ([3], Lemma 6). *A finite p-group is nilpotent.*

Theorem A.0.6 (Burnside basis theorem; [43], Theorem 5.3.2). *Let G be a finite p-group. Then $\Phi(G) = [G,G]G^{[p]}$. If $[G\colon \Phi(G)] = p^r$, then every generating set of G has a subset of r elements which also generates G.*

Theorem A.0.7 ([43], Theorem 5.3.8). *Any finite extraspecial group has order p^{1+2r} for some positive integer r. For each r, there are two isomorphism type of extraspecial groups. Extraspecial 2-groups are central products of copies of the dihedral group D_4 and the quaternion group Q_8.*

Theorem A.0.8 (Sylow). *Let G be a finite group and p prime divisor of $|G|$. Write $|G| = p^a m$ such that $p \nmid m$, and write $n_p(G) = |\mathrm{Syl}_p(G)|$ for the number of Sylow p-subgroups of G. Then the following are true:*

(i) $n_p(G) \equiv 1 \bmod p$.

(ii) $n_p(G) \mid m$.

(iii) *Every p-subgroup of G is contained in a Sylow p-subgroup of G.*

(iv) *If $P \in \mathrm{Syl}_p(G)$, then all Sylow p-subgroups of G are conjugate to P.*

Theorem A.0.9 (Characterisation of finite nilpotent groups, [35], Theorem 1.26)**.** *The following statements are equivalent for any finite group G:*

(i) *G is nilpotent.*

(ii) *For every subgroup $H \leq G$, there exists a subnormal series of G that contains H as a term.*

(iii) *If H is a proper subgroup of G, then $H < N_G(H)$.*

(iv) *Every maximal subgroup of G is normal.*

(v) *G is the direct product of its Sylow subgroups.*

(vi) *$[G, G] < \Phi(G)$.*

Theorem A.0.10 ([43], Theorem 5.1.9)**.** *For a nilpotent group G, the nilpotency class of G is the length of its upper central series, as same as the length of its lower central series.*

Theorem A.0.11 ([35], Corollary 1.28)**.** *Let G be a finite group and $m = |G|$. Then the following statements are equivalent:*

(i) *$F(G) = \prod_{p|m} O_p(G)$.*

(ii) *$F(G)$ is the unique largest normal nilpotent subgroup of G.*

(iii) *$F(G)$ is the Fitting subgroup of a group G.*

Theorem A.0.12 (Fundamental theorem of finitely generated abelian groups; [33], Theorem 9.12)**.** *A nontrivial finitely generated abelian group is isomorphic to a direct product of finitely many cyclic groups of infinite or prime-power orders. More specifically, such a group is isomorphic to*

$$C_{d_1} \times \cdots C_{d_r} \times (\mathbb{Z}, +)^s$$

for uniquely defined $r, s \in \mathbb{N}$ and $d_1, \ldots, d_r \in \mathbb{N}^+$ with $d_i \mid d_{i+1}$ for all $1 \leq i \leq r$.

Theorem A.0.13 ([9], Lemma 1.3)**.** *Let H and K be groups whose orders are coprime, and let $G = H \times K$. Then $\mathrm{Aut}(G) \cong \mathrm{Aut}(H) \times \mathrm{Aut}(K)$.*

Theorem A.0.14 (Cauchy–Frobenius; [35], 1.A.6)**.** *Let G be a finite group acting on a set X. For each $g \in G$ let $\mathrm{Fix}_X(g)$ be the set of fixed points of g in X.Then the number of G-orbits in X equals*

$$\frac{1}{|G|} \sum_{g \in G} |\mathrm{Fix}_X(g)|.$$

Appendix B

Determination of groups of order p^4q

Let p, q be distinct primes, and let G be a group of order p^4q throughout. Let $P \in \mathrm{Syl}_p(G)$ and $Q \in \mathrm{Syl}_q(G)$. Since Q is of order q, it is cyclic and isomorphic to C_q, with $\mathrm{Aut}(Q) \cong C_{q-1}$. There are 14 isomorphism types of groups of 16 and there are 15 isomorphism types of groups of odd order p^4. We make case distinction on the isomorphism types of groups of order p^4 and use results in Chapter 5. In this section we give brief explanation of our determination of groups of order p^4q. Recall that Eick and Moede [25] proved the enumeration results for these groups. Our explicit determination of the isomorphism types of such groups directly results a counting formula that agrees with that of Eick and Moede. More specifically, we divide our discussion into three parts: first we determine groups of order p^4q without normal Sylow subgroups, then we determine the non-nilpotent groups of such order with a normal Sylow q-subgroup, and lastly we determine the non-nipotent groups with a normal Sylow p-subgroup. This way, in combination with the aforementioned results for groups of order p^4, we obtain a list of the isomorphism types of groups of order p^4q and a formula for each of the summand in (8.1.1).

First consider groups of order p^4q without normal Sylow subgroups. The following result follows by a direct application of Theorem 8.1.1.

Lemma B.0.1 ([25], Theorem 2)**.** *If G is a group of order p^4q with no normal Sylow subgroup, then $|G| = 2^4{\cdot}3$ or $3^4{\cdot}13$.*

Since a group of order p^4q is solvable, we deduce that if G has no normal Sylow subgroup, then it has a normal subgroup H with index p; that is, $|H| = p^3q$. Moreover, if $Q \in \mathrm{Syl}_q(H)$ then Q is not normal in H, for otherwise $Q \lhd G$, contradicting our assumption. Groups of order p^3q without a normal Sylow q-subgroup are determined in Lemma 6.2.2 and Lemma 6.2.5, from which we know that $H \cong \mathrm{Sym}_4$ or H has a normal Sylow p-subgroup. Using this fact we can readily determine all groups of order $n \in \{2^4{\cdot}3, 3^4{\cdot}13\}$ without normal Sylow subgroups in GAP [27]. In particular, we obtain the following result.

Lemma B.0.2. *Let G be a group of order 48 or $3^4{\cdot}13$ with no normal Sylow subgroup. If $|G| = 48$ contains no normal Sylow subgroup, then G is isomorphic to one of the following:*

$$C_2 \ltimes \mathrm{Sym}_4, \quad C_4 \ltimes \mathrm{Alt}_4, \quad \mathrm{GL}_2(3), \quad C_2.\mathrm{SL}_2(3),$$

where $C_2.\mathrm{SL}_2(3)$ is a non-split extension with a normal subgroup isomorphic to $\mathrm{SL}_2(3) \cong C_3 \ltimes Q_8$ (see (6.2.3) for a presentation). If $|G| = 3^4{\cdot}13$, then G contains a normal subgroup $H \cong C_{13} \ltimes C_3^3$ where

C_{13} acts on C_3^3 via the irreducible matrix $\mathrm{Irr}_3(3,13)$*, and $G \cong C_3 \ltimes H$, where C_3 acts on trivially on $C_3^3 \lhd H$ and C_3 acts on a Sylow 13-subgroup of H via $\rho(13,3)$ (see Notation 4.1.1).*

The following lemmas complete the determination of groups of order p^4q; in the proofs we omit some technical details if they are due to direct but complicated computation.

Lemma B.0.3. *Let $\mathcal{N}_q$ be the number of isomorphism types of non-nilpotent groups of order p^4q with a normal Sylow q-subgroup. Then*

$$\mathcal{N}_q = (5p + 19 - \Delta_p^2)\Delta_{q-1}^p + (5+2p)\Delta_{q-1}^{p^2} + 2\Delta_{q-1}^{p^3} + \Delta_{q-1}^{p^4}.$$

Proof. By Theorem 2.4.1, if G is a non-nilpotent group of order p^4q with a normal Sylow q-subgroup, then $G = P \ltimes_\varphi Q$, where P has order p^4 and $Q \cong C_q$. First note that G is nilpotent if and only if φ is trivial, thus it suffices to only consider the cases where φ is nontrivial. It follows that $Z(G) \leq \operatorname{Ker}\varphi$. Since both Q and $\operatorname{Aut}(Q)$ are cyclic, we apply Corollary 2.4.6 for the classification of such groups. Using the same notation in Corollary 2.4.6, for each $K \in \mathcal{K}_\ell$ where $\ell \mid \gcd(|P|, |\operatorname{Aut}(Q)|)$, we write $\mathrm{ind}_K = [\operatorname{Aut}(P/K) \colon A_K]$. Note that $\operatorname{Aut}(Q) \cong C_{q-1}$ and $P/\operatorname{Ker}\varphi$ embeds into $\operatorname{Aut}(Q)$, so it follows that $\operatorname{Ker}\varphi \leq [P,P]$ and $|P/\operatorname{Ker}\varphi|$ divides $q-1$. We make a case distinction on the isomorphism type of P. For an isomorphism type P with SOT ID $(p^4 : x)$ as listed in Table 5.3; we write n_x for the number of isomorphism types of non-nilpotent semidirect products $P \ltimes C_q$ where P is of type $(p^4 : x)$. Recall that for group homomorphisms that are described by the image of a generating set, we abbreviate the map on the generating sets by omitting fixed points. For example, given two group presentations with the same generating set $\{a,b,c,d,e\}$, we write $\{a \mapsto b, b \mapsto a\}$ for the homomorphism $\{a \mapsto b, b \mapsto a, c \mapsto c, d \mapsto d, e \mapsto d\}$.

1. If $P \cong C_{p^4}$, then for each $\ell \in \{1, p, p^2, p^3\}$ there is a unique $\operatorname{Aut}(P)$-class of normal subgroups $K \in \mathcal{K}_\ell$ with $P/K \cong C_\ell$. Since P is abelian, $\operatorname{Ker}\varphi = Z(G)$. We determine that $\mathrm{ind}_K = 1$ for each representative K and apply Corollary 2.4.6 to count that

   $$n_1 = \Delta_{q-1}^p + \Delta_{q-1}^{p^2} + \Delta_{q-1}^{p^3} + \Delta_{q-1}^{p^4}.$$

   Conversely, we identify the isomorphism type of G by computing $Z(G)$:

   - If $Z(G) \cong C_{p^3}$, then $G \cong \mathrm{Pc}\langle a,b \mid a^{p^4}, b^q, b^a = b^{\rho(q,p)}\rangle$.
   - If $Z(G) \cong C_{p^2}$, then $p^2 \mid (q-1)$ and $G \cong \mathrm{Pc}\langle a,b \mid a^{p^4}, b^q, b^a = b^{\rho(q,p^2)}\rangle$.
   - If $Z(G) \cong C_p$, then $p^3 \mid (q-1)$ and $G \cong \mathrm{Pc}\langle a,b \mid a^{p^4}, b^q, b^a = b^{\rho(q,p^3)}\rangle$.
   - If $Z(G) = 1$, then $p^4 \mid (q-1)$ and $G \cong \mathrm{Pc}\langle a,b \mid a^{p^4}, b^q, b^a = b^{\rho(q,p^4)}\rangle$.

2. If $P \cong C_{p^3} \times C_p$, then $Z(G) = \operatorname{Ker}\varphi$. By looking at normal subgroups of P with cyclic quotient, we find that $\operatorname{Ker}\varphi = K \in \{C_{p^3},\ C_{p^2} \times C_p,\ C_{p^2},\ C_p^2,\ C_p\}$. Since there is a unique $\operatorname{Aut}(P)$-class of normal subgroups for each such representative K, and $\mathrm{ind}_K = 1$. Applying Corollary 2.4.6, we find that

   $$n_2 = 2\Delta_{q-1}^p + 2\Delta_{q-1}^{p^2} + \Delta_{q-1}^{p^3}.$$

   Conversely, we identify the isomorphism type of G by computing $Z(G)$:

   - If $Z(G) \cong C_{p^3}$, then $p \mid (q-1)$ and $G \cong \mathrm{Pc}\langle a,b,c \mid a^{p^3}, b^p, c^q, c^b = c^{\rho(q,p)}\rangle$.

- If $Z(G) \cong C_{p^2} \times C_p$, then $p \mid (q-1)$ and $G \cong \mathrm{Pc}\langle a,b,c \mid a^{p^3}, b^p, c^q, c^a = c^{\rho(q,p)}\rangle$.
- If $Z(G) \cong C_{p^2}$, then we can write $P = \mathrm{Pc}\langle a,b \mid a^{p^3}, b^{p}\rangle$ and $Z(G)$ is of the form $\langle a^p b^k\rangle$ for some $k \in \mathbb{Z}_p^*$. Since such subgroups $\langle a^p b^k\rangle$ are in the same $\mathrm{Aut}(P)$-class with representative $\langle a^p b\rangle$, it follows that

$$G \cong \mathrm{Pc}\langle a,b,c,d \mid a^{p^2} = c, b^p = c, c^p, d^q, d^a = d^{\rho(q,p^2)}\rangle.$$

- If $Z(G) \cong C_p^2$, then $p^2 \mid (q-1)$ and $G \cong \mathrm{Pc}\langle a,b,c \mid a^{p^3}, b^p, c^q, c^a = c^{\rho(q,p^2)}\rangle$.
- If $Z(G) \cong C_p$, then $p^3 \mid (q-1)$ and $G \cong \mathrm{Pc}\langle a,b,c \mid a^{p^3}, b^p, c^q, c^a = c^{\rho(q,p^3)}\rangle$.

3. If $P \cong C_{p^2} \times C_{p^2}$, then $Z(G) = \mathrm{Ker}\,\varphi$. Subgroups of P with cyclic quotients are isomorphic to $C_{p^2} \times C_p$ or C_{p^2}. Since each of such subgroups lies in a unique $\mathrm{Aut}(P)$-class with a representative $K \in \mathcal{K}_p \cup \mathcal{K}_{p^2}$ with $\mathrm{ind}_K = 1$, we apply Corollary 2.4.6 and find

$$n_3 = \Delta_{q-1}^p + \Delta_{q-1}^{p^2}.$$

Conversely, we identify the isomorphism type of G by computing $Z(G)$:

- If $Z(G) \cong C_{p^2} \times C_p$, then $p \mid (q-1)$ and $G \cong \mathrm{Pc}\langle a,b,c \mid a^{p^2}, b^{p^2}, c^q, c^a = c^{\rho(q,p)}\rangle$.
- If $Z(G) \cong C_{p^2}$, then $p^2 \mid (q-1)$ and $G \cong \mathrm{Pc}\langle a,b,c \mid a^{p^2}, b^{p^2}, c^q, c^a = c^{\rho(q,p^2)}\rangle$.

4. If $P \cong C_{p^2} \times C_p^2$, then $Z(G) = \mathrm{Ker}\,\varphi$. Subgroups of P with cyclic quotients are isomorphic to $C_{p^2} \times C_p$, C_p^2, or C_p^3, and there is a unique $\mathrm{Aut}(P)$-class containing each of such subgroups. For each representative $K \in \mathcal{K}_p \cup \mathcal{K}_{p^2} \cup \mathcal{K}_{p^3}$ we determine $\mathrm{ind}_K = 1$ and apply Corollary 2.4.6 to count that

$$n_4 = 2\Delta_{q-1}^p + \Delta_{q-1}^{p^2}.$$

Conversely, we identify the isomorphism type of G by computing $Z(G)$:

- If $Z(G) \cong C_{p^2} \times C_p$, then $p \mid (q-1)$ and $G \cong \mathrm{Pc}\langle a,b,c,d \mid a^{p^2}, b^p, c^p, d^q, d^b = d^{\rho(q,p)}\rangle$.
- If $Z(G) \cong C_p^3$, then $p \mid (q-1)$ and $G \cong \mathrm{Pc}\langle a,b,c,d \mid a^{p^2}, b^p, c^p, d^q, d^a = d^{\rho(q,p)}\rangle$.
- If $Z(G) \cong C_p^2$, then $p^2 \mid (q-1)$ and $G \cong \mathrm{Pc}\langle a,b,c,d \mid a^{p^2}, b^p, c^p, d^q, d^a = d^{\rho(q,p^2)}\rangle$.

5. If $P \cong C_p^4$, then subgroups of P with cyclic quotients are isomorphic to C_p^3 and lie in a unique $\mathrm{Aut}(P)$-class. It follows that $n_5 = \Delta_{q-1}^p$, and $G \cong C_p^3 \times (C_p \ltimes C_q)$ if it exists.

6. If P is of type $(p^4 : 6)$, then we can write $P = \mathrm{Pc}\langle a,b,c,d \mid a^p, b^p = c, c^p, d^p, d^a = cd\rangle$ for $p > 2$, and $P = \mathrm{Pc}\langle a,b,c,d \mid a^p, b^p = c, c^p, d^p, b^a = bc, d^a = cd\rangle$ for $p = 2$, whose normal subgroups with cyclic quotients are of the form $C_{p^2} \times C_p$, p_+^{1+2}, p_-^{1+2} (recall that we follow the convention that $2_+^{1+2} \cong D_4$ and $2_-^{1+2} \cong Q_8$ if $p = 2$). There are three $\mathrm{Aut}(P)$-classes of $\mathcal{K}_p$, with representatives $K \in \{\langle b,c,d\rangle, \langle a,c,d\rangle, \langle a,bd,c\rangle\}$ respectively, and $\mathrm{ind}_K = 1$ for each K. In total, there are $n_6 = 3\Delta_{q-1}^p$ isomorphism types of such groups. Observe that the Fitting subgroup of G is $F(G) = \mathrm{Ker}\,\varphi \times Q$, it follows that $|F(G)| = p^3q$, and $G/F(G) \cong C_p$. This gives a way to identify the isomorphism type of such a group G by computing $F(G)$:

- If $F(G) \cong (C_p \times C_{p^2}) \times C_q$ and $p > 2$, then

$$G \cong \mathrm{Pc}\langle a,b,c,d,e \mid a^p, b^p = c, c^p, d^p, e^q, d^a = cd, e^a = e^{\rho(q,p)}\rangle;$$

if $F(G) \cong (C_2 \times C_4) \times C_q$, then

$$G \cong \mathrm{Pc}\langle a,b,c,d,e \mid a^2, b^2 = c, c^2, d^2, e^q, b^a = bc, d^a = cd, e^a = e^{\rho(q,p)}\rangle;$$

- If $F(G) \cong p_+^{1+2} \times C_q$ and $p > 2$, then

$$G \cong \mathrm{Pc}\langle a,b,c,d,e \mid a^p, b^p = c, c^p, d^p, d^a = cd, e^b = e^{\rho(q,p)}\rangle;$$

if $F(G) \cong D_4 \times C_q$, then

$$G \cong \mathrm{Pc}\langle a,b,c,d,e \mid a^2, b^2 = c, c^2, d^2, e^q, b^a = bc, d^a = cd, e^b = e^{\rho(q,p)}\rangle;$$

- If $F(G) \cong p_-^{1+2} \times C_q$ and $p > 2$, then

$$G \cong \mathrm{Pc}\langle a,b,c,d,e \mid a^p, b^p = c, c^p, d^p, e^q, d^a = cd, d^b = cd, e^a = e^{\rho(q,p)}\rangle;$$

if $F(G) \cong Q_8 \times C_q$, then

$$G \cong \mathrm{Pc}\langle a,b,c,d,e \mid a^2, b^2 = d, c^2 = d, d^2, e^q, c^a = cd, c^b = cd, e^a = e^{-1}\rangle.$$

7. If P is of type $(p^4 : 7)$, then we can write $P = \mathrm{Pc}\langle a,b,c,d \mid a^p = b, b^p = c, c^p, d^p, d^a = cd\rangle$ for $p > 2$, and $P = \mathrm{Pc}\langle a,b,c,d \mid a^2, b^2 = c, c^2, d^2, b^a = bc\rangle$ for $p = 2$. First consider the case $p > 2$, and note that normal subgroups in P with cyclic quotients are of the form C_{p^3}, $C_{p^2} \times C_p$, C_{p^2}, C_p^2. There are two $\mathrm{Aut}(P)$-orbits in $\mathcal{K}_p$ and two orbits in $\mathcal{K}_{p^2}$. In particular, if $K \in \mathcal{K}_p$ is isomorphic to C_{p^3}, then $\mathrm{ind}_K = p - 1$; if $K \in \mathcal{K}_p$ is isomorphic to $C_{p^2} \times C_p$, then $\mathrm{ind}_K = 1$; if $C_{p^2} \cong K \in \mathcal{K}_{p^2}$, then $\mathrm{ind}_K = p - 1$; if $C_p^2 \cong K \in \mathcal{K}_{p^2}$, then $\mathrm{ind}_K = 1$. For the construction and identification of such groups, we note that $F(G) \cong \mathrm{Ker}\,\varphi \times Q$ and $\mathrm{Ker}\,\varphi \in \mathrm{Syl}_p(F(G))$. We compute from the above presentation of P that if $p > 2$, then $\langle c\rangle = [P,P]$, $\langle c,d\rangle = \Omega(P)$, $\langle b,c\rangle = Z(P)$, and $\langle b,c,d\rangle$ are characteristic in P.
Now consider the case $p = 2$, note that normal subgroups in P with cyclic quotients have size $p^3 = 8$, and $\mathcal{K}_2 = \{C_4 \times C_2,\ D_4,\ C_2^3\}$. For each $K \in \mathcal{K}_2$, we find $\mathrm{ind}_K = 1$. It follows from Corollary 2.4.6 that

$$n_7 = (p + \Delta_p^2)\Delta_{q-1}^p + p(1 - \Delta_p^2)\Delta_{q-1}^{p^2}.$$

These groups can be constructed and identified as follows:

- If $F(G) \cong C_{p^3} \times C_q$, then $p > 2$ and $K \in \mathcal{K}_p$ takes the form $\langle ad^k, b, c\rangle$ with $k \in \mathbb{Z}_p$. Since such groups are in the same $\mathrm{Aut}(P)$-class, it suffices to consider

$$G \cong G(k) = \mathrm{Pc}\langle a,b,c,d,e \mid a^p = b, b^p = c, c^p, d^p, e^q, d^a = cd, e^d = e^{\rho(q,p,k)}\rangle \quad \text{(B.0.1)}$$

for some $k \in \mathbb{Z}_p^*$. Any isomorphism $G(k) \to G(k')$ maps the pcgs $\{a \mapsto a^{x_1}b^{x_2}c^{x_3}d^{x_4}$, $b \mapsto b^{x_1}c^{x_2}$, $c \mapsto c^{x_1}$, $d \mapsto c^{y_1}d^{y_2}$, $e \mapsto e^z\}$ with $x_i, y_i \in \mathbb{Z}_p$, $z \in \mathbb{Z}_q^*$, and $x_1, y_2 > 0$. A routine calculation shows that such an isomorphism exists if and only if $k = k'$. Therefore, there are precisely $p - 1$ isomorphism types of the form $G(k)$ as described in (B.0.1), parametrised by $k \in \mathbb{Z}_p^*$. Conversely, given such a group G, to determine the value of k it is sufficient to determine the action of $\Omega(P) = \langle c,d\rangle$ on Q, where $\langle c\rangle = [P,P]$.
- If $F(G) \cong (C_p \times C_{p^2}) \times C_q$ and $p > 2$, then it suffices to consider $K = \langle b,c,d\rangle \in \mathcal{K}_p$

and

$$G \cong G(k) = \mathrm{Pc}\langle a,b,c,d,e \mid a^p = b, b^p = c, c^p, d^p, e^q, d^a = cd, e^a = e^{\rho(q,p,k)}\rangle$$

for some $k \in \mathbb{Z}_p^*$. However, for each $k \in \mathbb{Z}_p^*$, the map $\{a \mapsto a^k, b \mapsto b^k, c \mapsto c^k\}$ extends to an isomorphism $G(k) \to G(1)$. Therefore, there is a unique isomorphism type of such groups and it suffices to consider $k = 1$.
If $F(G) \cong C_4 \times C_2$, then $G \cong \mathrm{Pc}\langle a,b,c,d \mid a^2, b^2 = c, c^2, d^2, b^a = bc, e^a = e^{-1}\rangle$.

- If $F(G) \cong C_{p^2} \times C_q$, then $p > 2$ and $K \in \mathcal{K}_{p^2}$ takes the form $\langle b^k d, c\rangle$ for some $k \in \mathbb{Z}_p^*$. Since they are in the same $\mathrm{Aut}(P)$-class, it suffices to consider $K = \langle bd, c\rangle$. Under $\alpha \in \mathrm{Aut}(P)$ defined by $\alpha(a) = a$, $\alpha(bd) = b$, $\alpha(b) = c$, $\alpha(c) = d$, this allows us to consider

$$G \cong G(k) = \mathrm{Pc}\langle a,b,c,d,e \mid a^p = b, b^p = d, c^p = d, d^p, e^q, c^a = cd, \\ e^a = e^{\rho(q,p^2,k)}, e^b = e^{\rho(q,p,k)}\rangle$$

for some $k \in \mathbb{Z}_p^*$. A routine calculation shows that each $k \in \mathbb{Z}_p^*$ adds a new isomorphism type $G(k)$. On the other hand, we know that for any $x, k \in \mathbb{Z}_p^*$, the groups

$$\mathrm{Pc}\langle a,b,c,d,e \mid a^p = b, b^p = d, c^p = d, d^p, e^q, c^a = cd^x, e^a = e^{\rho(q,p^2,k)}, e^b = e^{\rho(q,p,k)}\rangle,$$

and

$$\mathrm{Pc}\langle a,b,c,d,e \mid a^p = b, b^p = d, c^p = d, d^p, e^q, c^a = cd, e^a = e^{\rho(q,p^2,x^{-1}k)}, e^b = e^{\rho(q,p,x^{-1}k)}\rangle$$

are isomorphic. This directly gives a way to determine the isomorphism type of a given group G by computing a presentation of the form $G(k)$ and finding the parameter k.

- If $F(G) \cong C_p^2 \times C_q$, then $p > 2$ and $K = \langle c, d\rangle$. This shows that

$$G \cong G(k) = \mathrm{Pc}\langle a,b,c,d,e \mid a^p = b, b^p = c, c^p, d^p, e^q, d^a = cd, \\ e^a = e^{\rho(q,p^2,k)}, e^b = e^{\rho(q,p,k)}\rangle$$

for some $k \in \mathbb{Z}_p^*$. Since $\{a \mapsto a^k, b \mapsto b^k, c \mapsto c^k\}$ extends to an isomorphism $G(k) \to G(1)$, the isomorphism type of $G(k)$ is independent of the choice of k and $G \cong G(1)$.

- If $F(G) \cong C_4 \times C_2$, then $G \cong \mathrm{Pc}\langle a,b,c,d,e \mid a^2, b^2 = c, c^2, d^2, e^q, b^a = bc, e^a = e^{-1}\rangle$.
- If $F(G) \cong D_4 \times C_q$, then $G \cong \mathrm{Pc}\langle a,b,c,d,e \mid a^2, b^2 = c, c^2, d^2, e^q, b^a = bc, e^d = e^{-1}\rangle$.
- If $F(G) \cong C_2^3 \times C_q$, then $G \cong \mathrm{Pc}\langle a,b,c,d,e \mid a^2, b^2 = c, c^2, d^2, e^q, b^a = bc, e^b = e^{-1}\rangle$.

8. If P is of type $(p^4 : 8)$, then we can write $P = \mathrm{Pc}\langle a,b,c,d \mid a^p, b^p = c, c^p, d^p, b^a = bc\rangle$ for $p > 2$, and $P = \mathrm{Pc}\langle a,b,c,d \mid a^2, b^2 = c, c^2, d^2, b^a = bd\rangle$ for $p = 2$. If $p > 2$, then there are three $\mathrm{Aut}(P)$-classes of normal subgroups of P with cyclic quotient; these subgroups have size p^3, and $\mathcal{K}_p = \{\langle b,c,d\rangle \cong C_{p^2} \times C_p,\ \langle a,b,c\rangle \cong p_-^{1+2},\ \langle a,c,d\rangle \cong C_p^3\}$. For each such $K \in \mathcal{K}_p$, we determine that $\mathrm{ind}_K = p-1, 1, 1$, respectively. We compute from the above presentation for $p > 2$ that the subgroups $\langle c,d\rangle = Z(P)$, $\langle c\rangle = [P,P]$, and $\langle a,c,d\rangle = \Omega(P)$ are characteristic in P. If $p = 2$, then we can choose $\mathcal{K}_4 = \{\langle a,d\rangle \cong C_2^2\}$ and $\mathcal{K}_2 = \{\langle b,c,d\rangle \cong C_4 \times C_2,\ \langle a,c,d\rangle \cong C_2^3\}$. For each representative $K \in \mathcal{K}_2 \cup \mathcal{K}_4$, we

find $\mathrm{ind}_K = 1$. Applying Corollary 2.4.6 yields that there are

$$n_8 = (p + 1 - \Delta_p^2)\Delta_{q-1}^p + \Delta_p^2\Delta_{q-1}^4$$

isomorphism types of such groups. We explicitly construct and identify these groups as follows:

- If $F(G) \cong (C_p \times C_{p^2}) \times C_q$ and $p > 2$, then $K = \langle b, c, d\rangle$ and

  $$G \cong G(k) = \mathrm{Pc}\langle a, b, c, d, e \mid a^p, b^p = c, c^p, d^p, e^q, b^a = bc, e^a = e^{\rho(q,p,k)}\rangle$$

  for some $k \in \mathbb{Z}_p^*$. To see this, first note that for any $x, k \in \mathbb{Z}_p^*$, the groups

  $$\mathrm{Pc}\langle a, b, c, d, e \mid a^p, b^p = c, c^p, d^p, e^q, b^a = bc^x, e^a = e^{\rho(q,p,k)}\rangle,$$

  and

  $$\mathrm{Pc}\langle a, b, c, d, e \mid a^p, b^p = c, c^p, d^p, e^q, b^a = bc, e^a = e^{\rho(q,p,x^{-1}k)}\rangle$$

  are isomorphic via $\{a \mapsto a^x\}$. Thus, it suffices to fix $x = 1$. Moreover, for $k, k' \in \mathbb{Z}_p^*$, any isomorphism $G(k) \to G(k')$ maps the pcgs $\{a \mapsto a^{x_1}b^{x_2}c^{x_3}d^{x_4}, b \mapsto b^{y_1}c^{y_2}d^{y_3}, c \mapsto c^{y_1}, d \mapsto c^{z_1}d^{z_2}, e \mapsto e^u\}$, where $x_i, y_i, z_i \in \mathbb{Z}_p$, $u \in \mathbb{Z}_q^*$, $x_1, y_1 > 0$, and z_1, z_2 are not both zero. A routine calculation shows that such an isomorphism exists if and only if $k = k'$. Therefore, each $k \in \mathbb{Z}_p^*$ adds a new isomorphism type $G(k)$.
  If $F(G) \cong (C_p \times C_{p^2}) \times C_q$ and $p = 2$, then

  $$G \cong \mathrm{Pc}\langle a, b, c, d, e \mid a^2, b^2 = c, c^2, d^2, e^q, b^a = bd, e^a = e^{-1}\rangle.$$

- If $F(G) \cong p_-^{1+2} \times C_q$, then $p > 2$ and $K = \langle a, b, c\rangle$. This shows that

  $$G \cong G(k) = \mathrm{Pc}\langle a, b, c, d, e \mid a^p, b^p = c, c^p, d^p, e^q, b^a = bc, e^d = e^{\rho(q,p,k)}\rangle$$

  for some $k \in \mathbb{Z}_p^*$. Since $\{d \mapsto d^k\}$ extends to an isomorphism $G(k) \to G(1)$ for any $k \in \mathbb{Z}_p^*$, the isomorphism type of $G(k)$ is independent of the choice of k; that is, $G \cong G(1)$.
- If $F(G) \cong C_p^3 \times C_q$ and $p > 2$, then $K = \langle a, c, d\rangle$ and

  $$G \cong G(k) = \mathrm{Pc}\langle a, b, c, d, e \mid a^p, b^p = c, c^p, d^p, e^q, b^a = bc, e^b = e^{\rho(q,p,k)}\rangle$$

  for some $k \in \mathbb{Z}_p^*$. However, for any $k \in \mathbb{Z}_p^*$, the map $\{b \mapsto b^k, c \mapsto c^k\}$ extends to an isomorphism $G(k) \to G(1)$. Therefore, the isomorphism type of $G(k)$ is independent of the choice of k and $G \cong G(1)$.
  If $F(G) \cong C_p^3 \times C_q$ and $p = 2$, then

  $$G \cong \mathrm{Pc}\langle a, b, c, d, e \mid a^2, b^2 = c, c^2, d^2, e^q, b^a = bd, e^b = e^{-1}\rangle.$$

- If $F(G) \cong C_2^2 \times C_q$, then $4 \mid (q - 1)$ and

  $$G \cong \mathrm{Pc}\langle a, b, c, d, e \mid a^2, b^2 = c, c^2, d^2, e^q, b^a = bd, e^b = e^{\rho(q,4)}, e^c = e^{-1}\rangle.$$

9. If P is of type $(p^4 : 9)$, then we can write $P = \mathrm{Pc}\langle a, b, c, d \mid a^p, b^p = c, c^p, d^p, b^a = bd\rangle$ for $p > 2$, and $P = \mathrm{Pc}\langle a, b, c, d \mid a^2 = c, b^2 = c, c^2, d^2, b^a = bc\rangle$ for $p = 2$. If $p > 2$, then there are three $\mathrm{Aut}(P)$-classes of normal subgroups of P with cyclic quotient. In partic-

ular, $\mathcal{K}_p = \{\langle b,c,d\rangle \cong C_{p^2}\times C_p,\ \langle a,c,d\rangle \cong C_p^3\}$ and $\mathcal{K}_{p^2} = \{\langle a,d\rangle \cong C_p^2\}$. For each $K \in \mathcal{K}_p \cup \mathcal{K}_{p^2}$, we find that $\mathrm{ind}_K = 1$. Moreover, we compute that $Z(P) = \langle c,d\rangle$, $[P,P] = \langle d\rangle$, $\Omega(P) = \langle a,c,d\rangle$, and $\mho(P) = \langle c\rangle$ are characteristic in P. If $p = 2$, then there are two $\mathrm{Aut}(P)$-classes of normal subgroups with cyclic quotient in P. These subgroups have order 8 with representatives $K \in \mathcal{K}_2 = \{\langle b,c,d\rangle \cong C_4\times C_2,\ \langle a,b,c\rangle \cong Q_8\}$. For each $K \in \mathcal{K}_2$ we find $\mathrm{ind}_K = 1$. Corollary 2.4.6 implies that

$$n_9 = 2\Delta_{q-1}^p + (1-\Delta_p^2)\Delta_{q-1}^{p^2}$$

isomorphism types in total. We explicitly construct and identify these groups as follows:

- If $F(G) \cong (C_{p^2}\times C_p)\times C_q$ and $p > 2$, then $K = \langle b,c,d\rangle$ and

  $$G \cong G(k) = \mathrm{Pc}\langle a,b,c,d,e \mid a^p, b^p = c, c^p, d^p, e^q, b^a = bd, e^a = d^{\rho(q,p,k)}\rangle$$

  for some $k \in \mathbb{Z}_p^*$. However, since for each $k \in \mathbb{Z}_p^*$, the map $\{a \mapsto a^k, d \mapsto d^{(k^{-1})}\}$ extends to an isomorphism $G(k) \to G(1)$, the isomorphism type of $G(k)$ is independent of the choice of k and $G \cong G(1)$.
  If $F(G) \cong C_4 \times C_2$, then

  $$G \cong \mathrm{Pc}\langle a,b,c,d,e \mid a^2 = c, b^2 = c, c^2, d^2, e^q, b^a = bc, e^a = e^{-1}\rangle.$$

- If $F(G) \cong C_p^3 \times C_q$, then $p > 2$ and $K = \langle a,c,d\rangle$. It follows that

  $$G \cong \mathrm{Pc}\langle a,b,c,d,e \mid a^p, b^p = c, c^p, d^p, e^q, b^a = bd, e^b = e^{\rho(q,p,k)}\rangle$$

  for some $k \in \mathbb{Z}_p^*$. A routine calculation shows that the map $\{b \mapsto b^k, c \mapsto c^k\}$ extends to an isomorphism $G(k) \to G(1)$. Therefore, $G \cong G(1)$.
- If $F(G) \cong C_p^2 \times C_q$, then $p > 2$, $K = \langle a,d\rangle$, and

  $$G \cong \mathrm{Pc}\langle a,b,c,d,e \mid a^p, b^p = c, c^p, d^p, e^q, b^a = bd, e^b = e^{\rho(q,p^2)}, e^c = e^{\rho(q,p)}\rangle.$$

10. If P is of type $(p^4 : 10)$, then we can write $P = \mathrm{Pc}\langle a,b,c,d \mid a^p = d, b^p = c, c^p, d^p, b^a = bc\rangle$. First note that there are three $\mathrm{Aut}(P)$-classes of normal subgroups of P with cyclic quotient. We choose $\mathcal{K}_p = \{\langle a,c,d\rangle \cong \langle b,c,d\rangle \cong C_{p^2}\times C_p\}$ and $\mathcal{K}_{p^2} = \{\langle b,c\rangle \cong C_p^2\}$ to be the representatives for these classes. For $K = \langle a,c,d\rangle$, we find that $\mathrm{ind}_K = p-1$; for $K = \langle b,c,d\rangle$, we find $\mathrm{ind}_K = 1$; for $K = \langle b,c\rangle$, we find $\mathrm{ind}_K = p-1$. Moreover, we compute from the above presentation of P that that $\langle c,d\rangle = Z(P)$, $\langle c\rangle = [P,P]$, $\langle c,d\rangle = \Omega(P)$, and $\langle b,c,d\rangle$ are characteristic in P. We apply Corollary 2.4.6 and count

    $$n_{10} = p\Delta_{q-1}^p + (p-1)\Delta_{q-1}^{p^2}.$$

    We explicitly construct these groups as follows:

    - If $F(G) \cong (C_{p^2}\times C_p)\times C_q$, then let $g \in G\backslash F(G)$ and there are two possibilities: if $\langle g\rangle \cap F(G) = [P,P]$, then $K = \langle a,c,d\rangle$; otherwise $K = \langle b,c,d\rangle$. In the former case, we have

      $$G \cong G(k) = \mathrm{Pc}\langle a,b,c,d,e \mid a^p = d, b^p = c, c^p, d^p, e^q, b^a = bc, e^b = e^{\rho(q,p,k)}\rangle$$

      for some $k \in \mathbb{Z}_p^*$. However, a routine computation shows that $G(k) \cong G(1)$ for any

$k \in \mathbb{Z}_p^*$. Therefore, $G \cong G(1)$. In the latter case, we see that the groups

$$\mathrm{Pc}\langle a,b,c,d,e \mid a^p = d, b^p = c, c^p, d^p, e^q, b^a = bc^x, e^a = e^{\rho(q,p,k)}\rangle$$

and

$$\mathrm{Pc}\langle a,b,c,d,e \mid a^p = d, b^p = c, c^p, d^p, e^q, b^a = bc, e^a = e^{\rho(q,p,x^{-1}k)}\rangle.$$

are isomorphic via $\{a \mapsto a^x\}$ for any $x \in \mathbb{Z}_p^*$. Thus, it suffices to consider $x = 1$, and

$$G \cong G(k) = \mathrm{Pc}\langle a,b,c,d,e \mid a^p = d, b^p = c, c^p, d^p, e^q, b^a = bc, e^a = e^{\rho(q,p,k)}\rangle$$

for some $k \in \mathbb{Z}_p^*$. Since any isomorphism $G(k) \to G(k')$ can be described by a map on the pcgs, which takes the form

$$\{a \mapsto a^{x_1}b^{x_2}c^{x_3}d^{x_4}, b \mapsto b^{y_1}c^{y_2}d^{y_3}, c \mapsto c^{y_1}, d \mapsto c^{x_2}d^{x_1}, e \mapsto e^z\},$$

where $x_i, y_i \in \mathbb{Z}_p, z \in \mathbb{Z}_q^*$, and $x_1, y_1 > 0$, a routine calculation shows that for $k, k' \in \mathbb{Z}_p^*$, the groups $G(k) \cong G(k')$ if and only if $k = k'$. Thus, each of $k \in \mathbb{Z}_p^*$ adds a new isomorphism type.

- If $F(G) \cong C_{p^2} \times C_q$, then $K = \langle c, d\rangle$. A routine calculation shows that

$$\mathrm{Pc}\langle a,b,c,d,e \mid a^p = d, b^p = c, c^p, d^p, e^q, b^a = bc^x, e^a = e^{\rho(q,p^2,k)}, e^d = e^{\rho(q,p,k)}\rangle$$

and

$$\mathrm{Pc}\langle a,b,c,d,e \mid a^p = d, b^p = c, c^p, d^p, e^q, b^a = bc, e^a = e^{\rho(q,p^2,x^{-1}k)}, e^d = e^{\rho(q,p,x^{-1}k)}\rangle$$

are isomorphic for any $x, k \in \mathbb{Z}_p^*$. Thus it suffices to consider $x = 1$ and

$$G \cong G(k) = \mathrm{Pc}\langle a,b,c,d,e \mid a^p = d, b^p = c, c^p, d^p, e^q, b^a = bc, e^a = e^{\rho(q,p^2,k)}, e^d = e^{\rho(q,p,k)}\rangle$$

for some $k \in \mathbb{Z}_p^*$. Akin to the preceding case, we can compute and show that for any $k, k' \in \mathbb{Z}_p^*$, two groups $G(k)$ and $G(k')$ are isomorphic if and only if $k = k'$. Thus, each $k \in \mathbb{Z}_p^*$ adds a new isomorphism type.

11. If P is of type $(p^4 : 11)$, then we can write $P = \mathrm{Pc}\langle a,b,c,d \mid a^p, b^p, c^p, d^p, c^a = bc\rangle$ for $p > 2$, and $P = \mathrm{Pc}\langle a,b,c,d \mid a^2, b^2 = c, c^2 = d, d^2, b^a = bd\rangle$ for $p = 2$. If $p > 2$, then normal subgroups of P with a cyclic quotient are of order p^3. Choosing $\mathcal{K}_p = \{\langle a,b,c\rangle \cong p_+^{1+2}, \langle b,c,d\rangle \cong C_p^3\}$ to be the representatives, we determine that $\mathrm{ind}_K = 1$ for each $K \in \mathcal{K}_p$ with $p > 2$. If $p = 2$, then we consider $\mathcal{K}_2 \cup \mathcal{K}_4$ where $\mathcal{K}_2 = \{\langle b,c,d\rangle \cong C_8, \langle a,c,d\rangle \cong C_4 \times C_2\}$ and $\mathcal{K}_4 = \{\langle a,d\rangle \cong C_2^2, \langle ac,d\rangle \cong C_4\}$; we find $\mathrm{ind}_K = 1$ for each $K \in \mathcal{K}_2 \cup \mathcal{K}_4$. We apply Corollary 2.4.6 and count

$$n_{11} = 2\Delta_{q-1}^p + 2\Delta_p^2\Delta_{q-1}^4.$$

The isomorphism type representatives are explicitly determined as follows:

- If $F(G) \cong p_+^{1+2} \times C_q$, then $p > 2$, $K = \langle a,b,c\rangle$, and

$$G \cong G(k) = \mathrm{Pc}\langle a,b,c,d,e \mid a^p, b^p, c^p, d^p, e^q, b^a = bc, e^d = e^{\rho(q,p,k)}\rangle,$$

for some $k \in \mathbb{Z}_p^*$. Since $\{d \mapsto d^k\}$ extends to an isomorphism $G(k) \to G(1)$, we conclude that $G \cong G(1)$.

- If $F(G) \cong C_p^3 \times C_q$, then $p > 2$, $K = \langle b, c, d\rangle$, and

$$G \cong G(k) = \mathrm{Pc}\langle a, b, c, d, e \mid a^p, b^p, c^p, d^p, e^q, b^a = bc, e^a = e^{\rho(q,p,k)}\rangle,$$

  for some $k \in \mathbb{Z}_p^*$. However, for each $k \in \mathbb{Z}_p^*$, the map $\{a \mapsto a^k, c \mapsto c^{(k^{-1})}\}$ extends to an isomorphism $G(k) \to G(1)$, thus it suffices to consider $k = 1$ and $G \cong G(1)$.
- If $F(G) \cong C_8$, then $K = \langle b, c, d\rangle$ and

$$G \cong \mathrm{Pc}\langle a, b, c, d, e \mid a^2, b^2 = c, c^2 = d, d^2, e^q, b^a = bd, e^a = e^{-1}\rangle.$$

- If $F(G) \cong C_4 \times C_2$, then $K = \langle a, c, d\rangle$, and

$$G \cong \mathrm{Pc}\langle a, b, c, d, e \mid a^2, b^2 = c, c^2 = d, d^2, e^q, b^a = bd, e^b = e^{-1}\rangle.$$

- If $F(G) \cong C_4$, then $K = \langle ac, d\rangle$. Note that $\alpha(b) = a$, $\alpha(ac) = b$, $\alpha(c) = c$, $\alpha(d) = d$ defines an automorphism $\alpha \in \mathrm{Aut}(P)$. Thus we obtain another presentation of P and determine that

$$G \cong \mathrm{Pc}\langle a, b, c, d, e \mid a^2 = c, b^2 = d, c^2 = d, d^2, e^q, b^a = bc, e^a = e^{\rho(q,4)}, e^c = e^{-1}\rangle.$$

- If $F(G) \cong C_2^2$, then $K = \langle a, d\rangle$ and

$$G \cong \mathrm{Pc}\langle a, b, c, d, e \mid a^2, b^2 = c, c^2 = d, d^2, e^q, b^a = bd, e^b = e^{\rho(q,4)}, e^c = e^{-1}\rangle.$$

12. If P is of type $(p^4 : 12)$, then we write $P = \mathrm{Pc}\langle a, b, c, d \mid a^p, b^p = c, c^p, d^p, b^a = bd, d^a = cd\rangle$ for $p > 2$, and $P = \mathrm{Pc}\langle a, b, c, d \mid a^2, b^2 = c, c^2 = d, d^2, b^a = bc, c^a = cd\rangle$ for $p = 2$. In the case $p > 2$, normal subgroups of P with a cyclic quotient are of order p^3. Moreover, $\mathcal{K}_p = \{\langle b, c, d\rangle \cong C_{p^2} \times C_p,\ \langle a, c, d\rangle \cong p_+^{1+2},\ \langle abd, c, d\rangle \cong p_-^{1+2}\}$. We determine $\mathrm{ind}_K = 1$, $\frac{1}{2}(p-1)$, and $\frac{1}{2}(p-1)$ for each $K \in \mathcal{K}_p$, respectively. Also, we compute that the subgroups $Z(P) = \langle c\rangle$, $[P, P] = \langle c, d\rangle$, $\Omega(P) = \langle a, c, d\rangle$, and $\langle b, c, d\rangle$ are characteristic in P. For $p = 2$, we note that $\mathcal{K}_2 = \{\langle b, c, d\rangle \cong C_8,\ \langle a, c, d\rangle \cong D_4,\ \langle abc, c, d\rangle \cong Q_8\}$, and $\mathrm{ind}_K = 1$ for each $K \in \mathcal{K}_2$. In tandem with Corollary 2.4.6, it follows that

$$n_{12} = (p + \Delta_p^2)\Delta_{q-1}^p.$$

We explicitly construct these groups as follows:

- If $F(G) \cong (C_{p^2} \times C_p) \times C_q$, then $p > 2$ and $K = \langle b, c, d\rangle$. Note that if x is a quadratic residue modulo p and $s^2 \equiv x \bmod p$, then the groups

$$\mathrm{Pc}\langle a, b, c, d, e \mid a^p, b^p = c, c^p, d^p, e^q, b^a = bd^x, d^a = cd, e^a = e^{\rho(q,p,k)}\rangle$$

  and

$$\mathrm{Pc}\langle a, b, c, d, e \mid a^p, b^p = c, c^p, d^p, e^q, b^a = bd, d^a = cd, e^a = e^{\rho(q,p,s^{-1}k)}\rangle$$

  are isomorphic for any $k \in \mathbb{Z}_p^*$. Thus, it suffices to consider $x = 1$ and

$$G \cong G(k) = \mathrm{Pc}\langle a, b, c, d, e \mid a^p, b^p = c, c^p, d^p, e^q, b^a = bd, d^a = cd, e^a = e^{\rho(q,p,k)}\rangle$$

  for some $k \in \mathbb{Z}_p^*$. Two such groups $G(k)$ and $G(k')$ with $k, k' \in \mathbb{Z}_p^*$ are isomorphic if and only if there exists an isomorphism described by $\{a \mapsto a^{x_1}c^{x_2}d^{x_3},\ b \mapsto b^{y_1}c^{y_2}d^{y_3},\ c \mapsto c^{y_1},\ d \mapsto c^{z_1}d^{z_2}$, and $e \mapsto e^u\}$, where $x_i, y_i, z_i \in \mathbb{Z}_p$, $u \in \mathbb{Z}_q^*$. However, such

an isomorphism exists if and only if there exist $x_i, y_i, z_i \in \mathbb{Z}_p^*$ such that $x_1z_2 = y_1$, $x_1y_1 = z_2$, $z_1 = x_1y_3$, and $kx_1 \equiv k' \bmod p$. This requires that $x_1^2 \equiv 1 \bmod p$, from which we further deduce that the parameters $k, k' \in \mathbb{Z}_p^*$ define isomorphic groups if and only if $k' \in \{k, -k\}$. Therefore, there are $\frac{1}{2}(p-1)$ isomorphism types and it suffices to consider $G(k)$ parametrised by $k \in \{1, \dots, \frac{1}{2}(p-1)\}$.

- If $F(G) \cong p_+^{1+2} \times C_q$, then $K = \langle a, c, d\rangle$. If $p = 2$, then

$$G \cong \mathrm{Pc}\langle a, b, c, d, e \mid a^2, b^2 = c, c^2 = d, d^2, e^q, b^a = bc, c^a = cd, e^a = e^{-1}\rangle.$$

  For $p > 2$,

$$G \cong G(k) = \mathrm{Pc}\langle a, b, c, d, e \mid a^p, b^p = c, c^p, d^q, e^q, b^a = bd, c^a = cd, e^b = e^{\rho(q,p,k)}\rangle$$

  for some $k \in \mathbb{Z}_p^*$. Since $\{b \mapsto b^k, c \mapsto c^k\}$ extends to an isomorphism $G(k) \to G(1)$, the isomorphism type of $G(k)$ is independent of the choices of $k \in \mathbb{Z}_p^*$ and $G \cong G(1)$.
- If $F(G) \cong p_-^{1+2} \times C_q$, then $p > 2$ and $K = \langle abd, c, d\rangle$. A routine calculation shows that if $x \in \mathbb{Z}_p^*$ is a quadratic residue modulo p and $s^2 \equiv x \bmod p$, then the groups

$$\mathrm{Pc}\langle a, b, c, d, e \mid a^p, b^p = c, c^p, d^p, e^q, b^a = bc^x d^x, d^a = cd, d^b = cd, e^a = e^{\rho(q,p,k)}\rangle$$

  and

$$\mathrm{Pc}\langle a, b, c, d, e \mid a^p, b^p = c, c^p, d^p, e^q, b^a = bcd, d^a = cd, d^b = cd, e^a = e^{\rho(q,p,s^{-1}k)}\rangle$$

  are isomorphic for any $k \in \mathbb{Z}_p^*$. Thus, it suffices to fix $x = 1$. For $p = 3$, since the map $\{abc \mapsto b, c \mapsto c^{-1}\}$ extends to an automorphism of P, we obtain another presentation of P and find

$$G \cong \mathrm{Pc}\langle a, b, c, d, e \mid a^3, b^3 = c, c^3, d^3, e^q, b^a = bd^2, d^a = cd, d^b = c^2d, e^a = e^{\rho(q,3)}\rangle.$$

  For $p > 3$, since there is an automorphism $\alpha \in P$ such that $\alpha(abd) = b$, $\alpha(a) = a$, $\alpha(c) = c$, and $\alpha(d) = d$, we determine that

$$G \cong G(k) = \mathrm{Pc}\langle a, b, c, d, e \mid a^p, b^p = c, c^p, d^p, e^q, b^a = bcd, d^a = cd, d^b = cd, e^a = e^{\rho(q,p,k)}\rangle$$

  for some $k \in \mathbb{Z}_p^*$. Furthermore, a similar calculation as before shows that two groups $G(k)$ and $G(k')$ with $k, k' \in \mathbb{Z}_p^*$ are isomorphic if and only if $k' \in \{k, -k\}$. Therefore, there are $\frac{1}{2}(p-1)$ isomorphism types $G(k)$ parametrised by $k \in \{1, \dots, \frac{1}{2}(p-1)\}$.
- If $F(G) \cong C_8 \times C_q$, then $K = \langle b, c, d\rangle$ and

$$G \cong \mathrm{Pc}\langle a, b, c, d, e \mid a^2, b^2 = c, c^2 = d, d^2, e^q, b^a = bc, c^a = cd, e^a = e^{-1}\rangle.$$

- If $F(G) \cong Q_8 \times C_q$, then $K = \langle abc, c, d\rangle$. Since there is an automorphism $\alpha \in \mathrm{Aut}(P)$ such that $\alpha(abc) = b$, $\alpha(a) = a$, $\alpha(c) = c$, and $\alpha(d) = d$, we obtain another presentation of P and determine that

$$G \cong \mathrm{Pc}\langle a, b, c, d, e \mid a^2, b^2 = d, c^2 = d, d^2, e^q, b^a = bc, c^a = cd, c^b = cd, e^a = e^{-1}\rangle.$$

13. If P is of type $(p^4 : 13)$, then we write $P = \mathrm{Pc}\langle a, b, c, d \mid a^p, b^p = c, c^p, d^p, b^a = bd, d^a = c^{\sigma_p}d\rangle$ for $p > 2$, and $P = \mathrm{Pc}\langle a, b, c, d \mid a^2, b^2 = c, c^2 = d, d^2, b^a = bcd, c^a = cd\rangle$ for $p = 2$. In the

case $p > 3$, we note that normal subgroups of P with a cyclic quotient are of order p^3 and $\mathcal{K}_p = \{\langle b,c,d\rangle \cong C_{p^2} \times C_p,\ \langle a,c,d\rangle \cong p_+^{1+2},\ \langle abd,c,d\rangle \cong p_-^{1+2}\}$. We further determine that $\mathrm{ind}_K = \frac{1}{2}(p-1), 1, \frac{1}{2}(p-1)$ for each $K \in \mathcal{K}_p$, respectively. Moreover, $Z(G) = \langle c\rangle$, $[P,P] = \langle c,d\rangle$, and $\Omega(P) = \langle a,c,d\rangle$ are characteristic in P. If $p = 3$, then we have $\mathcal{K}_3 = \{\langle b,c,d\rangle \cong C_9 \times C_3,\ \langle a,c,d\rangle \cong 3_+^{1+2}\}$, with $Z(P) = \langle c\rangle$, $[P,P] = \langle c,d\rangle$, and $\langle b,c,d\rangle$ characteristic in P. We further determine that $\mathrm{ind}_K = 1$ for each $K \in \mathcal{K}_3$. For $p = 2$, then we have $\mathcal{K}_2 = \{\langle b,c,d\rangle \cong C_8,\ \langle a,c,d\rangle \cong D_4\}$, and $\mathrm{ind}_K = 1$ for each $K \in \mathcal{K}_2$. In total, we count

$$n_{13} = (p - \Delta_p^3)\Delta_{q-1}^p$$

isomorphism types, which can be explicitly constructed as follows:

- If $F(G) \cong (C_p \times C_{p^2}) \times C_q$, then $p > 2$ and $K = \langle b,c,d\rangle$. Further, note that if x is a quadratic residue modulo p and $s^2 \equiv x \bmod p$, then the groups

  $$\mathrm{Pc}\langle a,b,c,d,e \mid a^p, b^p = c, c^p, d^q, e^q, b^a = bd^x, d^a = c^{\sigma_p}d, e^a = e^{\rho(q,p,k)}\rangle$$

  and

  $$\mathrm{Pc}\langle a,b,c,d,e \mid a^p, b^p = c, c^p, d^q, e^q, b^a = bd, d^a = c^{\sigma_p}d, e^a = e^{\rho(q,p,s^{-1}k)}\rangle$$

  are isomorphic for any $k \in \mathbb{Z}_p^*$. Thus, it suffices to consider $x = 1$ and

  $$G \cong G(k) = \mathrm{Pc}\langle a,b,c,d,e \mid a^p, b^p = c, c^p, d^q, e^q, b^a = bd, d^a = c^{\sigma_p}d, e^a = e^{\rho(q,p,k)}\rangle$$

  for some $k \in \mathbb{Z}_p^*$. A routine calculation shows that two such groups $G(k)$ and $G(k')$ with $k, k' \in \mathbb{Z}_p^*$ are isomorphic if and only if $k' \in \{k, -k\}$. Therefore, it suffices to consider $G(k)$ parametrised by $k \in \{1, \ldots, \frac{1}{2}(p-1)\}$.
- If $F(G) \cong C_q \times C_8$, then $p = 2$ and

  $$G \cong \mathrm{Pc}\langle a,b,c,d,e \mid a^2, b^2 = c, c^2 = d, d^2, e^q, b^a = bcd, c^a = cd, e^b = e^{-1}\rangle.$$
- If $F(G) \cong p_+^{1+2} \times C_q$ or $F(G) \cong D_4 \times C_q$, then $K = \langle a,c,d\rangle$. If $p = 2$, then

  $$G \cong \mathrm{Pc}\langle a,b,c,d,e \mid a^2, b^2 = c, c^2 = d, d^2, e^q, b^a = bcd, c^a = cd, e^b = e^{-1}\rangle;$$

  if $p > 2$, then

  $$G \cong G(k) = \mathrm{Pc}\langle a,b,c,d,e \mid a^p, b^p = c, c^p, d^q, e^q, b^a = bd, d^a = c^{\sigma_p}d, e^b = e^{\rho(q,p,k)}\rangle$$

  for some $k \in \mathbb{Z}_p^*$. However, for any $k \in \mathbb{Z}_p^*$, the map $\{b \mapsto b^k, c \mapsto c^k, d \mapsto d^k\}$ extends to an isomorphism $G(k) \to G(1)$. This the isomorphism type of $G(k)$ is independent of the choice of $k \in \mathbb{Z}_p^*$ and it suffices to consider $G \cong G(1)$.
- If $F(G) \cong p_-^{1+2} \times C_q$, then $p > 3$ and $K = \langle abd,c,d\rangle$. If x is a quadratic residue modulo p and $s^2 \equiv x \bmod p$, then the groups

  $$\mathrm{Pc}\langle a,b,c,d,e \mid a^p, b^p = c, c^p, d^p, e^q, b^a = bc^x d^x, d^a = c^{\sigma_p}d, d^b = cd, d^a = d^{\rho(q,p,k)}\rangle$$

and

$$\mathrm{Pc}\langle a,b,c,d,e \mid a^p, b^p = c, c^p, d^p, e^q, b^a = bcd, d^a = c^{\sigma_p}d, d^b = cd, d^a = d^{\rho(q,p,s^{-1}k)}\rangle$$

are isomorphic for any $k \in \mathbb{Z}_p^*$. Under the automorphism $\alpha \in \mathrm{Aut}(P)$ described by $\alpha(a) = a$, $\alpha(abd) = b$, $\alpha(c) = c$, and $\alpha(d) = d$, we have

$$G \cong G(k) = \mathrm{Pc}\langle a,b,c,d,e \mid a^p, b^p = c, c^p, d^p, e^q, b^a = bcd, d^a = c^{\sigma_p}d, d^b = cd, e^a = e^{\rho(q,p,k)}\rangle$$

for some $k \in \mathbb{Z}_p^*$. By a routine computation, we find that two groups $G(k)$ and $G(k')$ with $k, k' \in \mathbb{Z}_p^*$ are isomorphic if and only if $k' \in \{k, -k\}$. Thus, there are $\frac{1}{2}(p-1)$ isomorphism types $G(k)$ parametrised by $k \in \{1, \ldots, \frac{1}{2}(p-1)\}$.

14. If P is of type $(p^4 : 14)$, then we can write $P = \mathrm{Pc}\langle a,b,c,d \mid a^p, b^p, c^p, d^p, c^a = bc, d^a = cd\rangle$ for $p > 2$; and $P = \mathrm{Pc}\langle a,b,c,d \mid a^2 = d, b^2 = c, c^2 = d, d^2, b^a = bcd, c^a = cd\rangle$ for $p = 2$. If $p > 3$, then normal subgroups of P with a cyclic quotient are of order p^3. We may choose representatives $\mathcal{K}_p = \{\langle b,c,d\rangle \cong C_p^3,\ \langle a,b,c\rangle \cong p_+^{1+2}\}$ for the $\mathrm{Aut}(p)$-classes of these normal subgroups. We further determine that $\mathrm{ind}_K = 1$ for each $K \in \mathcal{K}_p$. If $p = 3$, then $\mathcal{K}_3 = \{\langle b,c,d\rangle \cong C_3^3,\ \langle a,b,c\rangle \cong 3_+^{1+2},\ \langle acd,b,c\rangle \cong 3_-^{1+2}\}$, and $\mathrm{ind}_K = 1$ for each $K \in \mathcal{K}_3$. For $p = 2$, we have $\mathcal{K}_2 = \{\langle b,c,d\rangle \cong C_8,\ \langle a,c,d\rangle \cong Q_8\}$, and $\mathrm{ind}_K = 1$ for each $K \in \mathcal{K}_2$. It follows from Corollary 2.4.6 that $n_{14} = (2 + \Delta_p^3)\Delta_{q-1}^p$. We determine the isomorphism class representatives as follows:

- If $F(G) \cong C_p^3 \times C_q$, then $p > 2$ and $K = \langle b,c,d\rangle$. It follows that

  $$G \cong G(k) = \mathrm{Pc}\langle a,b,c,d,e \mid a^p, b^p, c^p, d^p, e^q, c^a = bc, d^a = cd, e^a = e^{\rho(q,p,k)}\rangle$$

  for some $k \in \mathbb{Z}_p^*$. However, the map $\{a \mapsto a^k, b \mapsto b^{(k^2)}, c \mapsto b^{\frac{1}{2}k(k-1)}c^k\}$ extends to an isomorphism $G(k) \to G(1)$. Therefore, the isomorphism type of $G(k)$ is independent of the choice of k and it suffices to consider $G \cong G(1)$.
- If $F(G) \cong p_+^{1+2} \times C_p$, then $p > 2$ and $K = \langle a,b,c\rangle$. We determine that

  $$G \cong \mathrm{Pc}\langle a,b,c,d,e \mid a^p, b^p, c^p, d^p, e^q, b^a = bc, c^a = cd, e^d = e^{\rho(q,p)}\rangle.$$

- If $F(G) \cong 3_-^{1+2} \times C_q$, then $K = \langle acd,b,c\rangle$. We determine that

  $$G \cong \mathrm{Pc}\langle a,b,c,d,e \mid a^3, b^3 = c, c^3, d^3, e^q, b^a = bd, d^a = cd, d^b = cd, e^a = e^{\rho(q,3)}\rangle.$$

- If $F(G) \cong C_8 \times C_q$, then $K = \langle b,c,d\rangle$ and

  $$G \cong \mathrm{Pc}\langle a,b,c,d,e \mid a^2 = d, b^2 = c, c^2 = d, d^2, e^q, b^a = bcd, c^a = cd, e^a = e^{-1}\rangle.$$

- If $F(G) \cong Q_8 \times C_q$, then $K = \langle a,c,d\rangle$ and

  $$G \cong \mathrm{Pc}\langle a,b,c,d,e \mid a^2 = d, b^2 = c, c^2 = d, d^2, e^q, b^a = bcd, c^a = cd, e^b = e^{-1}\rangle.$$

15. If P is of type $(p^4 : 15)$, then $p > 2$. For $p > 3$ we write

  $$P = \mathrm{Pc}\langle a,b,c,d \mid a^p = b, b^p, c^p, d^p, c^a = bc, d^a = cd\rangle,$$

and for $p = 3$ we write

$$P = \mathrm{Pc}\langle a, b, c, d \mid a^3 = c, b^3 = c, c^3, d^3, b^a = bd, d^a = c^2d\rangle.$$

If $p > 3$, then normal subgroups of P with a cyclic quotient are of order p^3. We may choose $\mathcal{K}_p = \{\langle b, c, d\rangle \cong C_{p^2} \times C_p,\ \langle a, b, c\rangle \cong p_-^{1+2}\}$ to be the representatives for the $\mathrm{Aut}(P)$-classes of these subgroups. We further determine that $\mathrm{ind}_K = 1$ for each $K \in \mathcal{K}_p$. If $p = 3$, then $\mathcal{K}_3 = \{\langle b, c, d\rangle \cong C_9 \times C_3,\ \langle a, c, d\rangle \cong 3_-^{1+2}\}$, and $\mathrm{ind}_K = 1$ for each $K \in \mathcal{K}_3$. In total, there are

$$n_{15} = 2(1 - \Delta_p^2)\Delta_{q-1}^p$$

isomorphism types. We determine these groups as follows:

- If $F(G) \cong C_p^3 \times C_q$, then $p > 3$ and $K = \langle b, c, d\rangle$. We determine that

$$G \cong \mathrm{Pc}\langle a, b, c, d, e \mid a^p = b, b^p, c^p, d^p, e^q, c^a = bc, d^a = cd, e^a = e^{\rho(q,p)}\rangle$$

- If $F(G) \cong p_-^{1+2} \times C_q$ and $p > 3$, then $K = \langle a, b, c\rangle$ and

$$G \cong \mathrm{Pc}\langle a, b, c, d, e \mid a^p = b, b^p, c^p, d^p, e^q, c^a = bc, d^a = cd, e^d = e^{\rho(q,p)}\rangle.$$

- If $F(G) \cong 3_-^{1+2} \times C_q$, then $K = \langle a, c, d\rangle$ and

$$G \cong \mathrm{Pc}\langle a, b, c, d, e \mid a^3 = c, b^3 = c, c^3, d^3, e^q, b^a = bd, d^a = c^2d, e^b = e^{\rho(q,3)}\rangle.$$

- If $F(G) \cong C_9 \times C_3 \times C_q$, then $K = \langle b, c, d\rangle$ and

$$G \cong \mathrm{Pc}\langle a, b, c, d, e \mid a^3 = c, b^3 = c, c^3, d^3, e^q, b^a = bd, d^a = c^2d, e^a = e^{\rho(q,3)}\rangle.$$

The determination of these groups follows by combing all the cases above; the counting formula is derived from $\sum_{i=1}^{15} n_i$. □

In the following, we determine the isomorphism type of non-nilpotent groups of order p^4q with a normal Sylow p-subgroup.

Lemma B.0.4. *Let $\mathcal{N}_p$ be the number of isomorphism types of non-nilpotent groups of order p^4q with a normal Sylow p-subgroup. Then if $q = 2$ then $\mathcal{N}_p = 40$; otherwise,*

$$\begin{aligned}\mathcal{N}_p = {} & \frac{1}{24}(q^3 + 31q^2 + 189q + 423 + 16\Delta_{q-1}^3 + 12\Delta_{q-1}^4)\Delta_{p-1}^q \\ & + \frac{1}{4}(q + 21 + 2\Delta_{q-1}^4)\Delta_{p+1}^q + (1 - \Delta_q^3)\Delta_{p^2+p+1}^q + \Delta_{p^2+1}^q.\end{aligned}$$

Proof. Since p, q are coprime, Theorem 2.4.1 implies that such a group G is isomorphic to a semidirect product $Q \ltimes_\varphi P$ where $|P| = p^4$ and $|Q| = q$. Since G is nilpotent if and only if φ is trivial, it remains to consider nontrivial φ. In particular, since $Q \cong C_q$ is simple, Q acts on P via φ faithfully. The enumeration of the isomorphism types of G follows by determining the number of conjugacy classes of cyclic subgroup of order q in $\mathrm{Aut}(P)$ as an application of Corollary 2.4.3(ii). Further, Lemma 4.2.8 asserts that this is equivalent to determining the number of conjugacy classes of subgroups of order q in $\mathrm{Aut}(P)/O_p(\mathrm{Aut}(P))$. To apply Lemma 4.2.8, an analysis of the automorphism group of each P (up to isomorphism) is required. For space purpose we omit some details on the derivation of the many known results regarding this topic;

we refer to [46] for further details; see also [37, pp. 96 - 97] for a list of $\mathrm{Aut}(P)/O_p(\mathrm{Aut}(P))$ with P of order p^4. For each P of type $(p^4 : x)$ as discussed in Table 5.3, we write c_x for the number of isomorphism types of non-nilpotent split extensions $C_q \ltimes P$. For the determination of such groups, we make some general observations: since Q acts on P faithfully, $Z(G) \leq Z(P)$; since $G/P \cong Q$ is cyclic, $[G,G] \leq P$; since $G \cong Q \ltimes P$ splits over P, if $Z(G)$ is nontrivial, then G is a central extension of $Z(G)$ by $G/Z(G)$, where $G/Z(G)$ is a group of order p^nq with $n \leq 3$. Such groups are classified in Chapter 5 (see Tables 6.1, 6.2, and 6.3). Let $\Phi(P)$ be the Frattini subgroup of P. Then Q acts faithfully on $P/\Phi(P)$; see [43, Theorem 9.3.2]. We use these results alongside Notations 4.1.1, 4.2.1, and 4.2.6 in the following to determine the isomorphism class representatives for the groups as described in the lemma.

1. If $P \cong C_{p^4}$, then $\mathrm{Aut}(P)$ is cyclic of order $p^3(p-1)$. Applying Corollary 2.4.3(ii) yields $c_1 = \Delta^q_{p-1}$, and
$$G \cong \mathrm{Pc}\langle a, b \mid a^q, b^{p^4}, b^a = b^{\rho(p^4,q)}\rangle.$$

2. If $P \cong C_{p^3} \times C_p$, then $\mathrm{Aut}(P)/O_p(\mathrm{Aut}(P)) \cong C^2_{p-1}$. It follows that $c_2 = (q+1)\Delta^q_{p-1}$, counted by the number of conjugacy classes of subgroups of order q in $\mathrm{Aut}(P)$ by Lemma 4.2.8, in bijection with the isomorphism types of said groups. The isomorphism type of a group G in this case can be determined by a case distinction on $Z(G)$ as follows:
   - If $Z(G) \cong C_p$, then $G \cong \mathrm{Pc}\langle a, b, c \mid a^q, b^{p^3}, c^p, b^a = b^{\rho(p^3,q)}\rangle$.
   - If $Z(G) \cong C_{p^3}$, then $G \cong \mathrm{Pc}\langle a, b, c \mid a^q, b^{p^3}, c^p, c^a = c^{\rho(p,q)}\rangle$.
   - If $Z(G) = 1$, then G is isomorphic to one of the following $q-1$ groups
   $$G(k) = \mathrm{Pc}\langle a, b, c \mid a^q, b^{p^3}, c^p, b^a = b^{\rho(p^3,q)}, c^a = c^{\rho(p,q,k)}\rangle$$
   parametrised by $k \in \mathbb{Z}^*_q$.

3. If $P \cong C_{p^2} \times C_{p^2}$, then $\mathrm{Aut}(P)/O_p(\mathrm{Aut}(P)) \cong \mathrm{GL}_2(p)$. By Theorem 4.2.7(i), we have
$$c_3 = \frac{1}{2}(p + 3 - \Delta_q^2)\Delta^q_{p-1} + (1 - \Delta_q^2)\Delta^q_{p+1}.$$
   We apply Lemma 4.2.8 in conjunction with the proof of Theorem 4.2.7(i) to determined the isomorphism class representatives for these groups as follows:
   - If $Z(G) \cong C_{p^2}$, then
   $$G \cong \mathrm{Pc}\langle a, b, c \mid a^q, b^{p^2}, c^{p^2}, b^a = b^{\rho(p,q)}\rangle.$$
   - If $Z(G) = 1$, then Q acts diagonalisably on $P/\Phi(P) \cong C_p^2$ (induced by the action on P) if $q \mid (p-1)$, and Q acts irreducibly on $P/\Phi(P)$ if $q \mid (p+1)$ and $q > 2$. The isomorphism types of such $Q \ltimes P/\Phi(P) \cong C_q \ltimes C_p^2$ are previously determined in Lemma 6.1.6. Lifting the Q-action on $P/\Phi(P)$, we obtain the isomorphism types of $Q \ltimes P$: if $q \mid (p-1)$, then there are $\frac{1}{2}(q + 1 - \Delta_q^2)$ isomorphism types of the form
   $$G(k) = \mathrm{Pc}\langle a, b, c \mid a^q, b^{p^2}, c^{p^2}, b^a = b^{\rho(p^2,q,c_q^k)}, c^a = c^{\rho(p^2,q)}\rangle,$$
   parametrised by $k \in \{0, \ldots, \frac{1}{2}(p-1)\}$ with $\Phi(P) = \langle b^p, c^p\rangle$; if $q \mid (p+1)$ and $q > 2$, then there is a unique isomorphism type with representative
   $$\mathrm{Pc}\langle a, b, c \mid a^q, b^{p^2}, c^{p^2}, (b^a, c^a) = (b, c)^{\mathrm{Irr}_2(p^2,q)}\rangle,$$

where $\mathrm{Irr}_2(p^2,q)$ has multiplicative order q in the ring of 2×2 matrices over $\mathbb{Z}_{p^2}$ and $\mathrm{Irr}_2(p^2,q)\equiv \mathrm{Irr}_2(p,q) \bmod p$.

4. If $P\cong C_{p^2}\times C_p^2$, then $\mathrm{Aut}(P)/O_p(\mathrm{Aut}(P))\cong \mathbb{Z}_p^*\times \mathrm{GL}_2(p)$. If $q\mid (p-1)$, then subgroups of order q in $\mathbb{Z}_p^*\times \mathrm{GL}_2(p)$ are conjugate to cyclic subgroups of one of the following forms:

$$\langle(\rho(p,q),\mathrm{diag}(1,1))\rangle,\ \langle(1,\mathrm{diag}(\rho(p,q),1))\rangle,\ \langle(\rho(p,q,k),\mathrm{diag}(\rho(p,q),1))\rangle,$$

$$\langle(\rho(p,q,k),M(p,q))\rangle,\ \langle(\rho(p,q),\mathrm{diag}(\rho(p,q,k),\rho(p,q,m)))\rangle,$$

where $0\le \ell\le \frac{1}{2}(p-1)$ and $k,m\in\mathbb{Z}_q^*$ with $k<m$. If $q\mid(p+1)$ and $q>2$, then there is a unique conjugacy class of subgroups of order q in $\mathbb{Z}_p^*\times\mathrm{GL}_2(p)$, with representative $\langle(1,\mathrm{Irr}_2(p,q))\rangle$. In total we find

$$c_4=\frac{1}{2}(q^2+2q+3-\Delta_q^2)\Delta_{p-1}^q+(1-\Delta_q^2)\Delta_{p+1}^q+5\Delta_q^2$$

isomorphism types. The isomorphism class representatives are determined as follows:

- If $Z(G)\cong C_{p^2}\times C_p$, then $G\cong (C_q\ltimes C_p)\ltimes C_{p^2}\times C_p$ and

$$G\cong \mathrm{Pc}\langle a,b,c,d\mid a^q,b^p,c^p,d^{p^2},b^a=b^{\rho(p,q)}\rangle.$$

- If $Z(G)\cong C_{p^2}$, then $G\cong (C_q\ltimes C_p^2)\times C_{p^2}$, which is determined by the isomorphism type of the nonabelian direct factor $C_q\ltimes C_p^2$. Such groups are previously determined (Lemma 6.1.6) and there are $\frac{1}{2}(q+1-\Delta_q^2)\Delta_{p-1}^q+(1-\Delta_q^2)\Delta_{p+1}^q$ isomorphism types of such groups. In particular, if $q\mid(p-1)$ then G is isomorphic to one of the following $\frac{1}{2}(q+1-\Delta_q^2)$ groups

$$G(k)=\mathrm{Pc}\langle a,b,c,d\mid a^q,b^p,c^p,d^{p^2},(b^a,c^a)=(b,c)^{M(p,q,\sigma_q^k)}\rangle,$$

parametrised by $k\in\{0,\dots,\lfloor\frac{1}{2}(q-1)\rfloor\}$; if $q\mid(p+1)$ and $q>2$ then

$$G\cong \mathrm{Pc}\langle a,b,c,d\mid a^q,b^p,c^p,d^{p^2},(b^a,c^a)=(b,c)^{\mathrm{Irr}_2(p,q)}\rangle.$$

- If $Z(G)\cong C_p^2$, then $G\cong (C_q\ltimes C_{p^2})\times C_p^2$ is determined by the isomorphism type of the nonabelian direct factor $C_q\ltimes C_{p^2}$. Since $C_q\ltimes C_{p^2}$ is unique up to isomorphism,

$$G\cong \mathrm{Pc}\langle a,b,c,d\mid a^q,b^{p^2},c^p,d^p,b^a=b^{\rho(p^2,q)}\rangle.$$

- If $Z(G)\cong C_p$, then the isomorphism type of $G\cong (C_q\ltimes(C_p\times C_{p^2}))\times C_p$ is determined by that of the nonabelian direct factor $C_q\ltimes(C_p\times C_{p^2})$. From Lemma 6.2.5 we know that there are $(q-1)\Delta_{p-1}^q$ isomorphism types of nonabelian groups $C_q\ltimes(C_p\times C_{p^2})$, and G is isomorphic to one of the $q-1$ isomorphism types

$$G(k)=\mathrm{Pc}\langle a,b,c,d\mid a^q,b^p,c^p,d^{p^2},b^a=b^{\rho(p,q,k)},d^a=d^{\rho(p^2,p)}\rangle$$

parametrised by $k\in\mathbb{Z}_q^*$.

- If $Z(G)=1$, then Q embeds into a subgroup conjugate to $\langle(\rho(p,q,k),M(p,q))\rangle$ or $\langle(\rho(p,q),\mathrm{diag}(\rho(p,q,k),\rho(p,q,m)))\rangle$ in $\mathrm{Aut}(P)$, with $k,m\in\mathbb{Z}_q^*$ and $k<m$. In particular, $q\mid(p-1)$. There are $(q-1+\frac{1}{2}(q^2-3q+2))\Delta_{p-1}^q=\frac{1}{2}(q^2-q)\Delta_{p-1}^q$ isomorphism types of such groups, in accordance with the conjugacy class representatives

of cyclic subgroups with generators described above in $\mathbb{Z}_p^* \times \mathrm{GL}_2(p)$, with isomorphism class representatives of the form

$$\mathrm{Pc}\langle a,b,c,d \mid a^q, b^p, c^p, d^{p^2}, b^a = b^{\rho(p,q,k)}, c^a = b^{\rho(p,q,m)}, d^a = d^{\rho(p^2,q)}\rangle \text{ or}$$
$$\mathrm{Pc}\langle a,b,c,d \mid a^q, b^p, c^p, d^{p^2}, (b^a,c^a) = (b,c)^{M_2(p,q)}, d^a = d^{\rho(p^2,q,\ell)}\rangle,$$

where $k, \ell, m \in \mathbb{Z}_q^*$ and $k < m$.

5. If $P \cong C_p^4$, then $\mathrm{Aut}(P) \cong \mathrm{GL}_4(p)$ has order $q^6(q-1)^4(q^3+q^2+q+1)(q^2+q+1)(q+1)$; the number of nonabelian isomorphism types of $C_q \ltimes C_p^4$ is exactly the number of conjugacy classes of the cyclic subgroups of order q in $\mathrm{GL}_4(p)$. As seen in Theorem 4.2.7(v), if $q = 2$, then there are $s_2(\mathrm{GL}_4(p)) = 4$ isomorphism types; if $q > 2$, then there are

$$\begin{aligned}&\frac{1}{24}(q^3+7q^2+21q+39+16\Delta_{q-1}^3+12\Delta_{q-1}^4-21\Delta_q^2)\Delta_{p-1}^q\\ &+\frac{1}{4}(q+5+2\Delta_{q-1}^4)(1-\Delta_q^2)\Delta_{p+1}^q\\ &+(1-\Delta_q^3)\Delta_{p^2+p+1}^q+(1-\Delta_q^2)\Delta_{p^2+1}^q\end{aligned}$$

isomorphism types. Following the proof for Theorem 4.2.7(v) in conjunction with Corollary 2.4.3(ii), these isomorphism types are explicitly determined in accordance with the conjugacy class representatives of subgroups of order q in $\mathrm{GL}_2(p)$ as follows:

- If $Z(G) \cong C_p^3$, then $q \mid (p-1)$, and $G \cong (C_q \ltimes C_q) \times C_p^3$ is determined by the unique nonabelian isomorphism type of order pq. In particular, there are Δ_{p-1}^q isomorphism types.
- If $Z(G) \cong C_p^2$, then $q \mid (p^2-1)$, and $G \cong (C_q \times C_p^2) \times C_p^2$ is determined by the centreless semidirect product $C_q \times C_p^2$ given in Table 6.1.1. In particular, there are $(1-\Delta_q^2)\Delta_{p+1}^q + \frac{1}{2}(q+1-\Delta_q^2)\Delta_{p-1}^q$ isomorphism types of such groups.
- If $Z(G) \cong C_p$, then $q \mid (p^2-1)(p^2+p+1)$, and $G \cong (C_q \ltimes C_p^3) \times C_p$ is determined by the centreless semidirect product $C_q \ltimes C_p^3$ given in Table 6.3. In particular, there are $\frac{1}{6}(q^2+q+4\Delta_{q-1}^3) + (1-\Delta_q^3)\Delta_{p^2+p+1}^q$ isomorphism types of such groups.
- If $Z(G) = 1$, then $q \mid (p^2-1)(p^3+p^2+p+1)(p^2+p+1)$, and $G \cong C_q \ltimes C_p^4$. There are

$$\begin{aligned}&\frac{1}{24}(q^3+3q^2+5q+3+12\Delta_{q-1}^4-9\Delta_q^2)\Delta_{p-1}^q\\ &+\frac{1}{4}(q+1+2\Delta_{q-1}^4)(1-\Delta_q^2)\Delta_{p+1}^q+(1-\Delta_q^2)\Delta_{p^2+1}^q\end{aligned}$$

isomorphism types. In particular, if $q \mid (p-1)$, then $Q \cong C_q$ acts diagonalisably on P; in accordance with the conjugacy class representatives of subgroups generated by $\mathrm{diag}(\rho(p,q), \rho(p,q,\sigma_q^k), \rho(p,q,\sigma_q^\ell), \rho(p,q,\sigma_q^m))$, the isomorphism class representatives of such $Q \ltimes C_p^4$ are determined as follows. If only one of k, ℓ, m is greater than 1, then there are $q-1$ isomorphism types

$$\mathrm{Pc}\langle a,b,c,d,e \mid a^q, b^p, c^p, d^p, e^p, b^a = b^{\rho(p,q)}, c^a = c^{\rho(p,q)}, d^a = d^{\rho(p,q)}, e^a = e^{\rho(p,q,\alpha^k)}\rangle,$$

parametrised by $k \in \mathbb{Z}_{q-1}$. If two of k, ℓ, m are greater than one, then there are two cases: if k, ℓ, m are not pairwise distinct, then there are $\frac{1}{2}(q-1)$ isomorphism types,

namely,

$$\mathrm{Pc}\langle a,b,c,d,e \mid a^q, b^p, c^p, d^p, e^p, b^a = b^{\rho(p,q)}, c^a = c^{\rho(p,q)}, d^a = d^{\rho(p,q,\alpha^k)}, e^a = e^{\rho(p,q,\alpha^k)}\rangle,$$

parametrised by $k \in \{1, \ldots, \frac{1}{2}(q-1)\}$; if k, ℓ, m are pairwise distinct, then there are $\binom{q-2}{2} = \frac{1}{2}(q-2)(q-3)$ isomorphism types, namely,

$$\mathrm{Pc}\langle a,b,c,d,e \mid a^q, b^p, c^p, d^p, e^p, b^a = b^{\rho(p,q)}, c^a = c^{\rho(p,q)}, d^a = d^{\rho(p,q,\alpha^k)}, e^a = e^{\rho(p,q,\alpha^\ell)}\rangle$$

where $(k, \ell) \in \mathbb{Z}^2_{q-1}$ with $1 \leq k < \ell \leq q-2$. Finally, if k, ℓ, m are all greater than 1, then only the cases where k, ℓ, m are pairwise distinct add new isomorphism types. In particular, there are $\frac{1}{24}(q^3 - 9q^2 + 29q - 33 + 12\Delta^4_{q-1})$ new isomorphism types arisen from this case, namely,

$$a,b,c,d,e \mid a^q, b^p, c^p, d^p, e^p, b^a = b^{\rho(p,q)}, c^a = c^{\rho(p,q,\alpha^k)}, d^a = d^{\rho(p,q,\alpha^\ell)}, e^a = e^{\rho(p,q,\alpha^m)}$$

parametrised by $(k, \ell, m) \in \mathbb{Z}^3_{q-1}$ with

$$1 \leq k \leq \frac{1}{4}(q-1),\ \ 2k \leq \ell \leq \frac{1}{2}(q-1),\ \ k + \ell \leq m \leq q-2-k,$$

or

$$1 \leq k \leq \frac{1}{4}(q-1),\ \ \frac{1}{2}(q+1) \leq \ell \leq q-1-2k,\ \ k+\ell+1 \leq m \leq q-2-k,$$

or

$$k = \frac{1}{4}(q-1),\ \ \ell = \frac{1}{2}(q-1),\ \ m = \frac{3}{4}(q-1).$$

If $q > 2$ and $q \mid (p+1)$, then Q acts reducibly but nondiagonalisably on P and G is isomorphic to one of the $\frac{1}{4}(p+3-2\Delta^4_{p+1})$ isomorphism types

$$G(k) = \mathrm{Pc}\langle a,b,c,d,e \mid a^q, b^p, c^p, d^p, e^p, (b^a, c^a) = (b,c)^{\mathrm{Irr}_2(p,q)}, (d^a, e^a) = (d,e)^{\mathrm{Irr}_2(p,q,\sigma_q^k)}\rangle,$$

where $k \in \{0, \ldots, \lfloor \frac{1}{4}(p-1) \rfloor\}$. If $q > 3$ and $q \mid (p^2+1)$ then Q acts irreducibly on P and

$$G \cong \mathrm{Pc}\langle a,b,c,d,e \mid a^q, b^p, c^p, d^p, e^p, (b^a, c^a, d^a, e^a) = (b,c,d,e)^{\mathrm{Irr}_4(p,q)}\rangle.$$

6. If P is of type $(p^4 : 6)$, then $\mathrm{Aut}(P)/O_p(\mathrm{Aut}(P)) \cong \mathrm{GL}_2(p)$ contains

$$c_6 = \frac{1}{2}(q+3-\Delta_q^2)\Delta^q_{p-1} + \Delta^q_{p+1}(1-\Delta_q^2)$$

conjugacy classes of cyclic subgroups of order q, corresponding to the number of isomorphism types of $G \cong C_q \ltimes P$, where $P \cong \mathrm{Pc}\langle a,b,c,d \mid a^p, b^p = c, c^p, d^p, d^a = cd\rangle$. The isomorphism types of G are determined by a case distinction on the structures of $Z(G)$ and $[G,G]$ as follows:

- If $Z(G) \cong C_{p^2}$, then $Z(G) = Z(P)$ and $G/Z(G) \cong C_q \ltimes C_p^2$. We further deduce that $q \mid (p^2-1)$. If $q \mid (p-1)$, then G has a presentation of the form

$$\mathrm{Pc}\langle a,b,c,d,e \mid a^q, b^p, c^p, d^p = e, e^p, c^b = ce, b^a = b^x t_1, c^a = c^y t_2\rangle,$$

where $t_1, t_2 \in Z(G) = \langle d, e\rangle$ and $x, y \in \mathbb{Z}_p^*$ have order q. It follows from Theorem 3.2.3 that $xy \equiv 1 \bmod q$. A routine calculation shows that it suffices to consider $t_1 = t_2 = 1$ and $y = \rho(p, q)$. Thus,

$$G \cong \mathrm{Pc}\langle a, b, c, d, e \mid a^q, b^p, c^p, d^p = e, e^p, c^b = ce, b^a = b^{\rho(p,q,q-1)}, c^a = c^{\rho(p,q)}\rangle.$$

If $q \mid (p+1)$ and $q > 2$, there is a unique isomorphism type, namely,

$$\mathrm{Pc}\langle a, b, c, d, e \mid a^q, b^p, c^p, d^p = e, e^p, c^b = ce, (b^a, c^a) = (b, c)^{\mathrm{Irr}_2(p,q)}\rangle.$$

- If $Z(G) = 1$, then there are two cases to consider, depending on the structure of the derived subgroup $[G, G]$: if $[G, G] = P$, then Q acts nontrivially on all generators of P; otherwise, Q acts trivially on at least one generator of P. From a routine computation, we deduce that there is a unique isomorphism type for the latter case ($[G, G] < P$), namely,

$$\mathrm{Pc}\langle a, b, c, d \mid a^q, b^p, c^{p^2}, d^p, d^b = c^p d, b^a = b^{\rho(p,q)}, c^a = c^{\rho(p^2,q)}\rangle.$$

For the case $[G, G] = P$, there are $\frac{1}{2}(q - 1 - \Delta_q^2)$ isomorphism types, namely,

$$\mathrm{Pc}\langle a, b, c, d \mid a^q, b^p, c^{p^2}, d^p, d^b = c^p d, b^a = b^{\rho(p,q+1-k)}, c^a = c^{\rho(p^2,q)}, d^a = d^{\rho(p,q,k)}\rangle,$$

parametrised by $k \in \{2, \ldots, \lfloor \frac{1}{2}(q+1)\rfloor\}$.

7. If P is of type $(p^4 : 7)$, then $\mathrm{Aut}(P)/O_p(\mathrm{Aut}(P)) \cong C_{p-1}$, which contains $c_7 = \Delta_{p-1}^q$ normal subgroups of order q. Thus,

$$G \cong \mathrm{Pc}\langle a, b, c \mid a^q, b^p, c^{p^3}, c^b = c^{1-p^2}, c^a = c^{\rho(p^3,q)}\rangle.$$

8. If P is of type $(p^4 : 8)$, then $\mathrm{Aut}(P)/O_p(\mathrm{Aut}(P)) \cong C_{p-1}^2$ contains $c_8 = (q+1)\Delta_{p-1}^q$ conjugacy class of cyclic subgroups of order q. Writing $P = \mathrm{Pc}\langle b, c, d \mid b^p, c^{p^2}, d^p, c^b = c^{p+1}\rangle$, the corresponding isomorphism types of G can be determined by a case distinction on the structures of $Z(G)$ and $[G, G]$ as follows:

   - If $Z(G) \cong C_p$, then a routine manipulation shows that there are two cases depending on the derived subgroup $[G, G]$. If $[G, G] \cong C_p^2$, then Q acts trivially on $\langle b, c\rangle$. In this case, there is a unique isomorphism type, namely,

$$\mathrm{Pc}\langle a, b, c, d \mid a^q, b^p, c^{p^2}, d^p, c^b = c^{p+1}, d^a = d^{\rho(p,q)}\rangle.$$

   If $[G, G] \cong C_{p^2}$, then Q acts nontrivially on $\langle c\rangle$ but trivially on $\langle a, d\rangle$. In this case, there is a unique isomorphism type, namely,

$$\mathrm{Pc}\langle a, b, c, d \mid a^q, b^p, c^{p^2}, d^p, c^b = c^{p+1}, c^a = c^{\rho(p^2,q)}\rangle.$$

   - If $Z(G) = 1$, then Q acts nontrivially on all generators of P. In this case,

$$G \cong G(k) = \mathrm{Pc}\langle a, b, c, d \mid a^q, b^p, c^{p^2}, d^p, c^b = c^{p+1}, c^a = c^{\rho(p^2,q)}, d^a = d^{\rho(p,q,k)}\rangle$$

   for some $k \in \mathbb{Z}_q^*$. A routine computation shows that for any $k, k' \in \mathbb{Z}_q^*$, two groups $G(k)$ and $G(k')$ are isomorphic if and only if $k = k'$. Thus, such groups $G(k)$ account for the remaining $q - 1$ isomorphism types.

9. If P is of type $(p^4 : 9)$ and $p > 2$, then $\mathrm{Aut}(P)/O_p(\mathrm{Aut}(P)) \cong C_{p-1}^2$; if P is of type $(16 : 9)$, then $\mathrm{Aut}(P)/O_p(\mathrm{Aut}(P)) \cong \mathrm{GL}_2(2)$. Applying Corollary 2.4.3(ii) in conjunction with Theorem 4.2.7(ii), we count

$$c_9 = (q+1)\Delta_{p-1}^q + \Delta_2^p\Delta_3^q$$

isomorphism types. With the presentation $P = \mathrm{Pc}\langle b, c, d \mid b^p, c^{p^2}, d^p, c^b = cd\rangle$ for $p > 2$, or $P = \mathrm{Pc}\langle b, c, d, e \mid b^2 = d, c^2 = d, d^2, e^2, c^b = cd\rangle$ for $p = 2$, we determine the isomorphism class representatives as follows.

- If $p = 2$, then $q = 3$ and G is isomorphic to

$$\mathrm{Pc}\langle a, b, c, d, e \mid a^3, b^2 = d, c^2 = d, d^2, e^2, c^b = cd, b^a = c, c^a = bc\rangle.$$

- If $p > 2$ and $Z(G) > 1$, then we observe that $Z(P) \cong C_p$ and there are two cases to consider: if $[G, G] < P$, then Q must act trivially on $\langle c, d\rangle$ and

$$G \cong \mathrm{Pc}\langle a, b, c, d \mid a^q, b^p, c^{p^2}, d^p, c^b = cd, b^a = b^{\rho(p,q)}, d^a = d^{\rho(p,q)}\rangle;$$

  if $[G, G] = P$, then

$$G \cong \mathrm{Pc}\langle a, b, c, d \mid a^q, b^p, c^{p^2}, d^p, c^b = cd, b^a = b^{\rho(p,q,q-1)}, c^a = c^{\rho(p^2,q)}\rangle.$$

- If $p > 2$ and $Z(G) = 1$, then there are two cases depending on the derived subgroup of G. If $[G, G] < P$, then

$$G \cong \mathrm{Pc}\langle a, b, c, d \mid a^q, b^p, c^{p^2}, d^p, c^b = cd, c^a = c^{\rho(p^2,q)}, d^a = d^{\rho(p,q)}\rangle.$$

  If $[G, G] = P$, then the remaining $q - 2$ groups are parametrised by

$$G(k) = \mathrm{Pc}\langle a, b, c, d \mid a^q, b^p, c^{p^2}, d^p, c^b = cd, b^a = b^{\rho(p,q)}, c^a = c^{\rho(p^2,q,k)}, d^a = d^{\rho(p,q,k+1)}\rangle$$

  with $k \in \mathbb{Z}_{q-1}\backslash\{0\}$.

10. If P is of type $(p^4 : 10)$, then $\mathrm{Aut}(P)/O_p(\mathrm{Aut}(P)) \cong C_{p-1}$ contains $c_{10} = \Delta_{p-1}^q$ normal subgroups of order q. It follows that

$$G \cong \mathrm{Pc}\langle a, b, c, d \mid a^q, b^p = d, c^{p^2}, d^p, c^b = c^{p+1}, c^a = c^{\rho(p^2,q)}\rangle.$$

11. If P is of type $(p^4 : 11)$ and $p > 2$, then $\mathrm{Aut}(P)/O_p(\mathrm{Aut}(P)) \cong \mathbb{Z}_p^* \times \mathrm{GL}_2(p)$; if $p = 2$ then $\mathrm{Aut}(P)/O_p(\mathrm{Aut}(P)) = 1$. It follows that

$$c_{11} = c_4 = \frac{1}{2}(q^2 + 2q + 3 - \Delta_q^2)\Delta_{p-1}^q + (1 - \Delta_q^2)\Delta_{p+1}^q + 5\Delta_q^2.$$

Writing $P = \mathrm{Pc}\langle b, c, d, e \mid b^p, c^p, d^p, e^p, c^b = cd\rangle$ for $p > 2$, we note that $Z(P) = \langle d, e\rangle$ and $[P, P] = \langle c\rangle$. The isomorphism types are determined as follows:

- If $Z(G) = Z(P) \cong C_p^2$ and $q \mid (p-1)$, then

$$G \cong \mathrm{Pc}\langle a, b, c, d, e \mid a^q, b^p, c^p, d^p, e^p, c^b = cd, b^a = b^{\rho(p,q,q-1)}, c^a = c^{\rho(p,q)}\rangle;$$

if $Z(G) = Z(P) \cong C_p^2$, $q > 2$, and $q \mid (p+1)$, then

$$G \cong \mathrm{Pc}\langle a, b, c, d, e \mid a^q, b^p, c^p, d^p, e^p, c^b = cd, (b^a, c^a) = (b, c)^{\mathrm{Irr}_2(p,q)} \rangle.$$

- If $Z(G) \cong C_p$ and $[G, G] \cong C_p^2$, then there are two possibilities for the derived subgroup, namely, $[G, G] = Z(P)$ or $[G, G] \neq Z(P)$. In particular, if $[G, G] = Z(P)$, then
$$G \cong \mathrm{Pc}\langle a, b, c, d, e \mid a^q, b^p, c^p, d^p, e^p, c^b = cd, e^a = e^{\rho(p,q)} \rangle;$$
if $[G, G] \neq Z(P)$, then
$$G \cong \mathrm{Pc}\langle a, b, c, d, e \mid a^q, b^p, c^p, d^p, e^p, c^b = cd, b^a = b^{\rho(p,q)}, d^a = d^{\rho(p,q)} \rangle.$$
- If $Z(G) \cong C_p$ and $[G, G] \cong C_p^3$, then G is isomorphic to one of the following $\frac{1}{2}(q - 1 - \Delta_q^2)$ isomorphism types
$$G(k) = \mathrm{Pc}\langle a, b, c, d, e \mid a^q, b^p, c^p, d^p, e^p, c^b = cd, b^a = b^{\rho(p,q,q+1-k)}, c^a = c^{\rho(p,q,k)}, d^a = d^{\rho(p,q)} \rangle$$
parametrised by $k \in \{2, \ldots, \lfloor \frac{1}{2}(q+1) \rfloor\}$.
- If $Z(G) \cong C_p$ and $[G, G] = P$, then we consider two cases: if $q > 2$, then G is isomorphic to one of the following $\frac{1}{2}(q - 1 + \Delta_q^2)$ isomorphism types
$$G(k) = \mathrm{Pc}\langle a, b, c, d, e \mid a^q, b^p, c^p, d^p, e^p, c^b = cd, b^a = b^{\rho(p,q)}, c^a = c^{\rho(p,q,q-1)}, e^a = e^{\rho(p,q,k)} \rangle$$
parametrised by $k \in \{1, \ldots, \frac{1}{2}(q-1)\}$; if $q = 2$, then
$$G \cong \mathrm{Pc}\langle a, b, c, d, e \mid a^2, b^p, c^p, d^p, e^p, c^b = cd, b^a = b^{-1}, c^a = c^{-1}, e^a = e^{-1} \rangle.$$
- If $Z(G) = 1$ and $[G, G] \cong C_p^3$ then G is isomorphic to one of the following $q - 1$ isomorphism types
$$G(k) = \mathrm{Pc}\langle a, b, c, d, e \mid a^q, b^p, c^p, d^p, e^p, c^b = cd, c^a = c^{\rho(p,q)}, d^a = d^{\rho(p,q)}, e^a = e^{\rho(p,q,k)} \rangle$$
parametrised by $k \in \mathbb{Z}_q^*$.
- If $Z(G) = 1$ and $[G, G] = P$, then G is isomorphic to one of the following $\frac{1}{2}(q^2 - 2q + 1)(1 - \Delta_q^2)$ isomorphism types
$$G(k) = \mathrm{Pc}\langle a, b, c, d, e \mid a^q, b^p, c^p, d^p, e^p, c^b = cd, b^a = b^{\rho(p,q)}, c^a = c^{\rho(p,q,\sigma_q^\ell)}, d^a = d^{\rho(p,q,\sigma_q^\ell+1)}, e^a = e^{\rho(p,q,k)} \rangle$$
parametrised by the pairs $(k, \ell) \in \mathbb{Z}_{q-1}^2$ with $\ell \in \{0, \ldots, \lfloor \frac{1}{2}(q-3) \rfloor\}$.

12. If P is of type $(p^4 : 12)$, and $p > 2$ then $\mathrm{Aut}(P)/O_p(\mathrm{Aut}(P)) \cong C_2 \times C_{p-1}$; if $p = 2$ then $\mathrm{Aut}(P)/O_p(\mathrm{Aut}(P)) = 1$. It follows that
$$c_{12} = \Delta_{p-1}^q + 2\Delta_q^2.$$

Writing $P = \mathrm{Pc}\langle b, c, d \mid b^p, c^{p^2}, d^p, c^b = cd, d^b = c^p d\rangle$, the corresponding isomorphism types are determined as follows:

- If $q > 2$, then $q \mid (p-1)$ and there is a unique isomorphism type corresponding to the normal subgroup of order q in $\mathrm{Aut}(P)/O_p(\mathrm{Aut}(P))$. In this case,

$$G \cong \mathrm{Pc}\langle a, b, c, d \mid a^q, b^p, c^{p^2}, d^p, c^b = cd, d^b = c^p d, c^a = c^{\rho(p^2,q)}, d^a = d^{\rho(p,q)}\rangle.$$

- If $q = 2$, then $Z(P) = \langle c^p\rangle$, from which we deduce that $|Z(G)| \leq p$. In this case,

$$G \cong \mathrm{Pc}\langle a, b, c, d \mid a^2, b^p, c^{p^2}, d^p, c^b = cd, d^b = c^p d, b^a = b^{-1}, d^a = c^p d^{-1}\rangle.$$

- If $q = 2$ and $Z(G) = 1$, then there are two cases depending on the derived subgroup $[G, G]$. In particular, if $[G, G] < P$, then $[G, G] \cong C_p \times C_{p^2}$, and

$$G \cong \mathrm{Pc}\langle a, b, c, d \mid a^2, b^p, c^{p^2}, d^p, c^b = cd, d^b = c^p d, c^a = c^{\rho(p^2,2)}, d^a = d^{-1}\rangle;$$

  if $[G, G] = P$, then G is isomorphic to

$$\mathrm{Pc}\langle a, b, c, d \mid a^2, b^p, c^{p^2}, d^p, c^b = cd, d^b = c^p d, b^a = b^{-1}, c^a = c^{\rho(p^2,2)}, d^a = c^{-p} d\rangle.$$

13. If P is of type $(p^4 : 13)$, and $p > 2$ then $\mathrm{Aut}(P)/O_p(\mathrm{Aut}(P)) \cong C_2 \times C_{p-1}$; if $p = 2$ then $\mathrm{Aut}(P)/O_p(\mathrm{Aut}(P)) = 1$. It follows that $c_{13} = c_{12} = \Delta^q_{p-1} + 2\Delta^2_q$. Writing

$$P = \mathrm{Pc}\langle b, c, d \mid b^p, c^{p^2}, d^p, c^b = cd, d^b = c^{\sigma_p p} d\rangle,$$

the isomorphism types of G are determined as follows (akin to the preceding case):

- If $q > 2$, then

$$G \cong \mathrm{Pc}\langle a, b, c, d \mid a^q, b^p, c^{p^2}, d^p, c^b = cd, d^b = c^{\sigma_p p} d, c^a = c^{\rho(p^2,q)}, d^a = d^{\rho(p,q)}\rangle.$$

- If $q = 2$ and $Z(G) = \langle c^p\rangle$, then

$$G \cong \mathrm{Pc}\langle a, b, c, d, e \mid a^2, b^p, c^p = d^{\sigma_p}, d^p, e^p, c^b = cd, d^b = cd, b^a = b^{-1}, e^a = de^{-1}\rangle.$$

- If $q = 2$, $Z(G) = 1$, and $[G, G] \cong C_p \times C_{p^2}$, then

$$G \cong \mathrm{Pc}\langle a, b, c, d \mid a^2, b^p, c^{p^2}, d^p, c^b = cd, d^b = c^{\sigma_p p} d, c^a = c^{\rho(p^2,2)}, d^a = d^{-1}\rangle.$$

  If $q = 2$, $Z(G) = 1$, and $[G, G] = P$, then G is isomorphic to

$$\mathrm{Pc}\langle a, b, c, d, e \mid a^2, b^p, c^p = d^{\sigma_p}, d^p, e^p, c^b = cd, d^b = cd, b^a = b^{-1}, c^a = c^{-1} d^{-\sigma_p}, d^a = d^{-1}, e^a = d^{-1} e\rangle.$$

14. If P is of type $(p^4 : 14)$, then $\mathrm{Aut}(P)/O_p(\mathrm{Aut}(P)) \cong C^2_{p-1}$, which contains

$$c_{14} = (q+1)\Delta^q_{p-1}$$

normal subgroups of order q. Since $Z(P) \cong C_p$, we have $|Z(G)| \leq p$.

Writing $P = \mathrm{Pc}\langle b, c, d, e \mid b^p, c^p, d^p, e^p, d^b = cd, e^b = de\rangle$, the isomorphism types of these groups are determined as follows:

- If $Z(G) \cong C_p$, then $G/Z(G) \cong C_q \ltimes (C_p \ltimes C_p^2)$. Such groups of order p^3q are determined previously (see Lemma 6.2.5). It follows that G is isomorphic to

$$\mathrm{Pc}\langle a,b,c,d,e \mid a^q, b^p, c^p, d^p, e^p, d^b = cd, e^b = de, b^a = b^{\rho(p,q)}, \\ d^a = c^{(2^{-1})\rho(p,q,q-1)(\rho(p,q)-1)} d^{\rho(p,q,q-1)}, e^a = e^{\rho(p,q,q-2)}\rangle.$$

- If $Z(G) = 1$, then there are $q\Delta_{p-1}^q$ isomorphism types, each of which has a presentation of the form

$$\mathrm{Pc}\langle a,b,c,d,e \mid a^q, b^p, c^p, d^p, e^p, d^b = cd, e^b = de, b^a = b^x, c^a = c^{\rho(p,q)}, d^a = c^y d^v, e^a = e^w\rangle,$$

where

$$x = \rho(p,q,k),\ v = \rho(p,q,q+1-k),\ w = \rho(p,q,q+1-2k),\ y = \frac{1}{2}x(x-1)w,$$

are parametrised by $k \in \mathbb{Z}_q$.

15. If P is of type $(p^4 : 15)$, then $p > 2$ and $\mathrm{Aut}(P)/O_p(\mathrm{Aut}(P)) \cong C_{p-1}$. It follows that $c_{15} = \Delta_{p-1}^q$. Such groups are determined as follows:

- If $p > 3$, then G is isomorphic to

$$\mathrm{Pc}\langle a,b,c,d \mid a^q, b^p, c^p, d^{p^2}, d^b = c^{-1}d^{p+1}, d^c = d^{1-p}, d^a = d^{\rho(p^2,q)}, \\ b^a = b^{\rho(p,q,q-1)}, c^a = cd^{(2^{-1})p(\rho(p,q)-1)}\rangle.$$

- If $p = 3$, then $q = 2$ and G is isomorphic to

$$\mathrm{Pc}\langle a,b,c,d,e \mid a^2, b^3 = d, c^3 = d, e^3, c^b = ce, e^b = d^2e, c^a = c^2d^2, d^a = d^2, e^a = de\rangle.$$

Combining all the cases above, the determination and enumeration results follow. □

Bibliography

[1] Jeffrey D. Adler, Michael Garlow, and Ethel R. Wheland. "Groups of order p^4 made less difficult". In: *arXiv preprint:1611.00461* (2016).

[2] Harry A. Bender. "A determination of the groups of order p^5". In: *Ann. of Math. (2)* 29.1-4 (1927), pp. 61–72.

[3] Yakov Berkovich. *Groups of prime power order. Vol. 1*. Vol. 46. De Gruyter Expositions in Mathematics. With a foreword by Zvonimir Janko. Walter de Gruyter GmbH & Co. KG, Berlin, 2008, pp. xx+512.

[4] Hans U. Besche and Bettina Eick. "Construction of finite groups". In: *J. Symbolic Comput.* 27.4 (1999), pp. 387–404.

[5] Hans U. Besche and Bettina Eick. "The groups of order $q^n \cdot p$". In: *Comm. Algebra* 29.4 (2001), pp. 1759–1772.

[6] Hans U. Besche, Bettina Eick, and Eamonn A. O'Brien. "A millennium project: constructing small groups". In: *Internat. J. Algebra Comput.* 12.5 (2002), pp. 623–644.

[7] Hans U. Besche, Bettina Eick, and Eamonn A. O'Brien. "The groups of order at most 2000". In: *Electron. Res. Announc. Amer. Math. Soc.* 7 (2001), pp. 1–4.

[8] Jonathan N. S. Bidwell. "Automorphisms of direct products of finite groups. II". In: *Arch. Math. (Basel)* 91.2 (2008), pp. 111–121.

[9] Jonathan N. S. Bidwell and M. John Curran. "Automorphisms of finite abelian groups". In: *Math. Proc. R. Ir. Acad.* 110A.1 (2010), pp. 57–71.

[10] Jonathan N. S. Bidwell, M. John Curran, and Dennis J. McCaughan. "Automorphisms of direct products of finite groups". In: *Arch. Math. (Basel)* 86.6 (2006), pp. 481–489.

[11] Simon R. Blackburn, Peter M. Neumann, and Geetha Venkataraman. *Enumeration of finite groups*. Vol. 173. Cambridge Tracts in Mathematics. Cambridge University Press, Cambridge, 2007, pp. xii+281.

[12] Wieb Bosma, John Cannon, and Catherine Playoust. "The Magma algebra system. I. The user language". In: *J. Symbolic Comput.* 24.3-4 (1997). Computational algebra and number theory (London, 1993), pp. 235–265.

[13] Kenneth S. Brown. *Cohomology of groups*. Vol. 87. Graduate Texts in Mathematics. Corrected reprint of the 1982 original. Springer-Verlag, New York, 1994.

[14] William Burnside. "On Groups of Order palphaqbeta". In: *Proc. London Math. Soc. (2)* 1 (1904), pp. 388–392.

[15] William Burnside. *Theory of groups of finite order*. 2d ed. Dover Publications, Inc., New York, 1955, pp. xxiv+512.

[16] Michael C. Slattery. "Generation of groups of square-free order". In: *Journal of Symbolic Computation* 42.6 (2007), pp. 668–677.

[17] Arthur Cayley. "VII. On the theory of groups, as depending on the symbolic equation $\Theta^n = 1$". In: *The London, Edinburgh, and Dublin Philosophical Magazine and Journal of Science* 7.42 (1854), pp. 40–47.

[18] Frank N. Cole and James W. Glover. "On Groups Whose Orders are Products of Three Prime Factors". In: *Amer. J. Math.* 15.3 (1893), pp. 191–220.

[19] Heiko Dietrich and Bettina Eick. "On the groups of cube-free order". In: *J. Algebra* 292.1 (2005), pp. 122–137.

[20] Heiko Dietrich, Bettina Eick, and Xueyu Pan. "Groups whose orders factorise into at most four primes". In: *J. Symbolic Comput.* 108 (2022), pp. 23–40.

[21] Heiko Dietrich and Darren Low. "Generation of finite groups with cyclic Sylow subgroups". In: *J. Group Theory* 24.1 (2021), pp. 161–175.

[22] Heiko Dietrich and James B. Wilson. "Isomorphism testing of groups of cube-free order". In: *J. Algebra* 545 (2020), pp. 174–197.

[23] David S. Dummit and Richard M. Foote. *Abstract algebra*. Third. John Wiley & Sons, Inc., Hoboken, NJ, 2004, pp. xii+932.

[24] Bettina Eick. "Enumeration of groups whose order factorises in at most 4 primes". In: *arXiv preprint:1702.02616* (2017).

[25] Bettina Eick and Tobias Moede. "The enumeration of groups of order $p^n q$ for $n \leq 5$". In: *J. Algebra* 507 (2018), pp. 571–591.

[26] Walter Feit and John G. Thompson. "Solvability of groups of odd order". In: *Pacific J. Math.* 13 (1963), pp. 775–1029.

[27] *GAP – Groups, Algorithms, and Programming, Version 4.11.0*. URL: www.gap-system.org. The GAP Group. 2020.

[28] Boris Girnat. "Die Klassifikation der Gruppen bis zur Ordnung p^5". In: *arXiv preprint: 1806.07462* (2018).

[29] Oliver E. Glenn. "Determination of the abstract groups of order p^2qr; p, q, r being distinct primes". In: *Trans. Amer. Math. Soc.* 7.1 (1906), pp. 137–151.

[30] Peter J. Hilton and Urs Stammbach. *A course in homological algebra*. Second. Vol. 4. Graduate Texts in Mathematics. Springer-Verlag, New York, 1997.

[31] Otto Hölder. "Die Gruppen der Ordnungen p^3, pq^2, pqr, p^4". In: *Math. Ann.* 43.2-3 (1893), pp. 301–412.

[32] Otto Hölder. "Die Gruppen mit quadratfreier Ordnungszahl". In: *Nachrichten von der Gesellschaft der Wissenschaften zu Göttingen, Mathematisch-Physikalische Klasse* 1895 (1895), pp. 211–229.

[33] Derek F. Holt, Bettina Eick, and Eamonn A. O'Brien. *Handbook of computational group theory*. Discrete Mathematics and its Applications (Boca Raton). Chapman & Hall/CRC, Boca Raton, FL, 2005.

[34] I. Martin Isaacs. *Character theory of finite groups*. Corrected reprint of the 1976 original [Academic Press, New York; MR0460423]. AMS Chelsea Publishing, Providence, RI, 2006, pp. xii+310.

[35] I. Martin Isaacs. *Finite group theory*. Vol. 92. Graduate Studies in Mathematics. American Mathematical Society, Providence, RI, 2008, pp. xii+350.

[36] Rodney James. "The groups of order p^6 (p an odd prime)". In: *Math. Comp.* 34.150 (1980), pp. 613–637.

[37] Reihard Laue. "Zur Konstruktion und Klassifikation endlicher auflösbarer Gruppen". In: *Bayreuth. Math. Schr.* 9 (1982), pp. ii+304.

[38] Charles R. Leedham-Green and Susan McKay. *The structure of groups of prime power order*. Vol. 27. London Mathematical Society Monographs. New Series. Oxford Science Publications. Oxford University Press, Oxford, 2002, pp. xii+334.

[39] Mike F. Newman. "Determination of groups of prime-power order". In: (1977), 73–84. Lecture Notes in Math., Vol. 573.

[40] Eamonn A. O'Brien. "The p-group generation algorithm". In: *J. Symbolic Comput.* 9.5-6 (1990), pp. 677–698.

[41] Eamonn A. O'Brien and Michael R. Vaughan-Lee. "The groups with order p^7 for odd prime p". In: *J. Algebra* 292.1 (2005), pp. 243–258.

[42] Shouhong Qiao and Cai Heng Li. "The finite groups of cube-free order". In: *J. Algebra* 334 (2011), pp. 101–108.

[43] Derek J. Robinson. *A course in the theory of groups*. Vol. 80. Graduate Texts in Mathematics. Springer-Verlag, New York-Berlin, 1982.

[44] Joseph J. Rotman. *An introduction to homological algebra*. Second. Universitext. Springer, New York, 2009, pp. xiv+709.

[45] Joseph J. Rotman. *An introduction to the theory of groups*. Fourth. Vol. 148. Graduate Texts in Mathematics. Springer-Verlag, New York, 1995, pp. xvi+513.

[46] Gustav Sædén Ståhl, Johan Laine, and Gustav Behm. "On p-groups of low power order". PhD thesis. May 2010.

[47] Mark W. Short. *The primitive soluble permutation groups of degree less than* 256. Vol. 1519. Lecture Notes in Mathematics. Springer-Verlag, Berlin, 1992, pp. x+145.

[48] Charles C. Sims. *Computation with finitely presented groups*. Vol. 48. Encyclopedia of Mathematics and its Applications. Cambridge University Press, Cambridge, 1994, pp. xiii+604.

[49] Hans. U. Besche, Bettina Eick, and Eamonn O'Brien. *SmallGrp – a GAP package Version 1.4.2*. URL: www.gap-system.org/Packages/smallgrp.html. 2021.

[50] Derek R. Taunt. "Remarks on the isomorphism problem in theories of construction of finite groups". In: *Proc. Cambridge Philos. Soc.* 51 (1955), pp. 16–24.

[51] A. E. Western. "Groups of Order p^3q". In: *Proc. Lond. Math. Soc.* 30 (1898), pp. 209–263.

[52] Marcel Wild. "The groups of order sixteen made easy". In: *Amer. Math. Monthly* 112.1 (2005), pp. 20–31.

Index