MONASH University

Finite p-Groups and Coclass Theory

Subhrajyoti Saha
Master of Science (Mathematics)
Bachelor of Science (Mathematics)

A thesis submitted for the degree of
Doctor of Philosophy
at Monash University

2020

School of Mathematics
Faculty of Science
Monash University
Melbourne, Australia

Dedicated to my parents

Copyright Notice

Declaration

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.

Signed: _____

Print Name: Mr Subhrajyoti Saha

Date: June 03, 2020

Acknowledgements

Firstly, I would like to express my sincere gratitude to my supervisor Dr Heiko Dietrich for the continuous support of my Ph.D study and related research, for his patience, motivation, and immense knowledge. His guidance helped me in all the time of research and writing of this thesis. I learnt a lot from you including being patient, management, focusing on the research problem and of course writing mathematics. When I first started in Monash, I had no idea how to write good mathematics. You are the person who with all patience corrected my erroneous drafts and I gradually learned how to make it better. I am still learning from you and I do not have enough words to thank you for all your support. The mathematics we discussed always inspired me to be a better researcher. I could not have imagined having a better advisor and mentor for my Ph.D study. Thanks would be too small to say for your contribution. I would also like to thank my associate supervisor Prof. Ian Wanless for his valuable comments and suggestions during my Ph.D. His comments on my thesis writing have helped me greatly to improve the quality of my thesis.

I like to thank Prof. Bettina Eick for her help in my Ph.D project. I am grateful to her for supporting me during my visits to Braunschweig and Bonn, Germany. I learnt a lot from her in those visits. I cannot forget the pleasant experience of discussing mathematics with her. She is and always will be an inspiration for me to look up to.

Besides my advisor, I would like to thank panel members of my milestone committee: Prof. Burkard Polster, Dr Daniel Horsley, and Dr Norman Do, for their insightful comments and encouragement, but also for the hard question which incentivised me to widen my research from various perspectives. I also like to thank Dr Santiago Barrera Acevedo for his valuable comments on my thesis.

My sincere thanks goes to Monash University and specially School of Mathematics, thanks for providing as many opportunities to develop my PhD career. From travel funding to regular social events, this school and university provided more than I expected. I am very glad and feel honoured that I chose to do my PhD in this university. In every instance, I got immense help from the School of Mathematics, Monash Connect and Monash Graduate Reseach Office; I am thankful them for making my journey even smoother. Special mention to John Chan for listening to my many ideas on how we could improve PhD life, as well as sorting through all the forms I had to fill in. My

sincere thanks also goes to Ms Linda Mayer, Ms Karen Hogeboom, and all other administrative staff in the School of Mathematics for providing all the necessary support for my research. Without their precious help it would not have been possible to conduct this research.

I would also like to thank Mr Simon Teague, Dr Santiago Barrera Acevedo, Ms Karen Hogeboom and definitely my supervisor Dr Heiko Dietrich for providing me with the opportunity to tutor in various courses as a teaching assistant during my Ph.D. It was a nice experience working with all of you and I really enjoyed learning how to teach better.

I thank my fellow Ph.D scholars for the stimulating discussions, for working together, and for all the fun we have had in the last four years. Also I thank all my friends including those who shared mathematics with me in Jadavpur University and Indian Institute of Technology, Kanpur for their continuous support and encouragement. In these institutes I also came across some of the finest mathematics teachers without whom I would have never loved mathematics this much. Among them I specifically want to thank Prof. Shamik Ghosh, Prof. Arbind K. Lal, Dr Santosha Pattanayak, Dr Ashis Mandal and Prof. S. Ghorai. The mathematics I learned from these great teachers eventually led me to pursue my doctoral studies, so without them I could not be what I am today. But I can not forget how my love for mathematics started during my school life. Two persons in my school life showed me how beautiful mathematics is. I like to thank Mr Dinesh Sarkar and Dr. Bharat Kumar Kar for teaching me, not just mathematics but also many important things in my life. Friends, philosophers and guides in my life; that's what they are and always will be.

Now, I would like to thank Dr Amlan Chakraborty, Department of Chemical Engineering, Monash University and his wife Mrs. Moumita (Titli) Chakraborty for their support in my life. I thank them with all my heart for showing me the right direction, giving me valuable suggestion and helping me in every possible way. Today they are not just friends of mine, they are my family. Amlan and Titli, you are among those few persons in my life whom I really want to be with always. I seriously have no word to express my feeling and gratitude for you both. All those laughs and cries, travel and shopping, writing and reading, tension and happiness and many more that we shared and did together will stay with me forever as a cherished memory. I can not have enough words to thank you two for helping and supporting me in every rough time during these years. When I first arrived in Melbourne in March 2016, I had no friend and then I met Amlan who really became my elder brother in every possible way. I shared your journey towards your doctoral degree and learned so much from you that helped me to be a better researcher. Thank you for everything, thanks a lot. Titli, I don't know how

to thank you. I shared every joy and sadness, every problem and happiness of mine and you gave me the best suggestion. These memories I will always carry with me to cherish. A very big thank you for helping me and being a part of my Ph.D journey, thanks a lot.

In these years, I also met some other wonderful people who kept me happy with motivation, laughter and enthusiasm. I want to thank Dola aunty, Kingshuk uncle for their initial support when I fist came to Australia. Thank you for helping me set up and supporting me when I did not have my parents with me to get myself going and for your advice throughout. I also want to acknowledge Sarmistha aunty and family, Madhumita aunty and family for the lovely time spent in all these years. I would also like to thank my landlord Vinod, for letting me stay without a problem in the same house for all these years and supporting me as a student.

Last but not the least, I would like to thank and convey my respect to my parents, Mrs Chaitali Saha (mom), Prof. Subrata Saha (dad) for their never-ending love and support. Your phone calls every day motivated me in all possible way. Listening to my problems and helping me thereafter made me a better person. Thank you for visiting me and giving support while I needed you most; during my thesis writing. Your inspiration made me what I am today. I always want to see smile in my parents' faces, I hope my endeavour in this project made you two proud. With your blessings I want to be a good human being. I like to convey all possible respect to my paternal grandmother and hope her blessing will make me a better person in my life. I wish my other grandparents were alive and to see this day and I also thank them for showering love to me.

I was supported for my tuition fees and living expenses by Research and Training Programme (RTP) Scholarships. I would like to thank the committees for providing these scholarships to me. I would also like to thank my supervisor Dr Heiko Dietrich for providing me with additional scholarship during the last three months of my PhD. I also like to thank Faculty of Science and the School of Mathematics, Monash University for providing me with the Postgraduate Publications Award (PPA). I would also like to thank Hausdorff Research Institute for Mathematics (HIM), Bonn, Germany for awarding me a travel grant for visiting HIM in 2018.

Thank you to everyone else that I may have missed to note down here but you are deep down in my heart and I have not forgotten your contribution towards this thesis.

Abstract

A finite p-group is a group whose order is a power of a prime p. The classification of finite p-groups by order is a difficult problem mainly because the number of groups (up to isomorphism) grows rapidly with order. Besides the order, the (nilpotency) class is a natural invariant, however finite p-groups of class ≥ 2 defy classification in a sense they are as complicated as all finite groups. Leedham-Green and Newman (1980) suggested to classify finite p-groups by another invariant called *coclass*; the coclass of a finite p-group of order p^n and nilpotency class c is $n - c$. Blackburn (1958) classified the 2- and 3-groups of coclass 1, but a classification for primes greater than 3 is significantly more difficult. A useful feature is that finite p-groups of coclass r can be visualised by a graph, the so called coclass graph $\mathcal{G}(p, r)$.

The coclass graph : The vertices of $\mathcal{G}(p, r)$ are the isomorphism types of finite p-groups of coclass r. Two vertices are connected, say, $G \to H$ if and only if $G \cong H/\gamma(H)$ where $\gamma(H)$ is the last non-trivial term of the lower central series of H. It is a deep result that $\mathcal{G}(p, r)$ consists of finitely many infinite trees, so-called *coclass trees*, and finitely many groups outside these trees. Each coclass tree contains a unique infinite path (*mainline*) starting at its root. Since coclass trees are the building blocks of coclass graphs, they have become one of the main interests in coclass theory. In this thesis we concentrate on two avenues for obtaining more insight into the structure of coclass trees.

Uniserial p-adic space groups : The inverse limit of the groups on the mainline of a coclass tree in $\mathcal{G}(p, r)$ is an infinite pro-p-group of coclass r and, conversely, any such pro-p-group defines an infinite path in $\mathcal{G}(p, r)$. As a result, these pro-p-groups, specially the *uniserial p-adic space groups* play an important role in coclass theory. For odd primes a constructive classification of such space groups is given by Eick (2008), however prime 2 poses severe complications. In this thesis we provide the theoretical description for determining all uniserial 2-adic space groups up to isomorphism. This completes the constructive classification of uniserial p-adic space groups for all primes p.

Skeleton groups : Coclass graphs have in general a very intricate structure. One possible way to look into these graphs is to restrict attention to the subgraph spanned by the so-called *skeleton groups*. Unlike other groups in $\mathcal{G}(p, r)$, skeleton groups can be conveniently parametrised by certain homomorphisms. For some special cases, this structure has been successfully used in the literature. In this thesis we develop, for the first time, a systematic treatment of skeleton groups and show that almost every group in $\mathcal{G}(p, r)$ is *close* to a skeleton group. Being parametrised by certain homomorphisms, a crucial problem is to decide when two homomorphisms define isomorphic groups. We investigate this problem and provide complete solutions for two important cases. Along the way, we also identified and corrected gaps in two proofs in a recent paper on $\mathcal{G}(3, 2)$. We utilise our results to derived some new structure results for coclass trees.

Publications

- Parts of Chapters 4 and 5 (skeleton groups and their isomorphism problem) are published in :

  Heiko Dietrich and **Subhrajyoti Saha**.
  A note on skeleton groups in coclass graphs.
  International Journal of Algebra and Compututation, 29(1):127–146, 2019.

- The content of Chapter 7 (constructive classification of uniserial p-adic space groups) is currently prepared for publication.

Contents

Copyright Notice ii

Declaration of Authorship iii

Acknowledgements iv

Abstract vii

Publications viii

1 Introduction 1
- 1.1 Coclass and coclass graphs . . . 3
- 1.2 Uniserial p-adic space groups . . . 6
- 1.3 Skeleton groups . . . 7
- 1.4 Outline of the thesis . . . 8

2 The Coclass Graph $\mathcal{G}(p, r)$ 9
- 2.1 Coclass trees . . . 9
- 2.2 Periodicities . . . 11
  - 2.2.1 Periodicity of type I . . . 13
  - 2.2.2 Periodicity of type II . . . 16

3 Infinite Pro-p-Groups of Coclass r 20
- 3.1 Infinite pro-p-groups and coclass graphs . . . 20
  - 3.1.1 Structure of infinite pro-p-groups . . . 23
  - 3.1.2 Uniserial p-adic space groups . . . 26
  - 3.1.3 Point groups . . . 28
  - 3.1.4 Coclass of space groups . . . 30
  - 3.1.5 Embedding . . . 30
- 3.2 The Coclass Theorems . . . 31

4 Skeleton Groups 34
- 4.1 Some number theory . . . 35
  - 4.1.1 p-adic numbers . . . 35

4.1.2 Cyclotomic fields . . . 36
4.2 Exterior square . . . 37
4.3 Twisted groups . . . 38
4.4 Skeleton groups . . . 39
4.4.1 The split case . . . 39
4.4.2 The general case . . . 40
4.4.3 Skeleton groups are constructible groups . . . 42

5 Isomorphism Problem of Skeleton Groups 50
5.1 Preliminary results . . . 50
5.2 Isomorphism problem . . . 52
5.2.1 Lifting automorphisms . . . 54
5.2.2 Two special cases . . . 55

6 Orbit Isomorphic Skeleton Groups 62
6.1 Periodicities in skeleton graph . . . 63
6.2 Skeleton groups with cyclic point group . . . 64
6.2.1 Homomorphisms from $T \wedge T$ . . . 65
6.2.2 The automorphism group . . . 68
6.2.3 Orbit isomorphisms . . . 71
6.2.4 The one-parameter case . . . 73
6.2.5 Descendants of a skeleton group . . . 75
6.2.6 The maximal class case . . . 77
6.2.7 Periodic parents of skeleton groups in $\mathcal{G}(7,1)$ . . . 80

7 Uniserial p-adic Space Groups 85
7.1 Background . . . 85
7.2 Point groups (case $p > 2$) . . . 88
7.3 Construction of extensions ($p > 2$) . . . 90
7.3.1 Dimension shifting and coclass . . . 90
7.4 Point groups ($p = 2$) . . . 92
7.4.1 Quaternion point groups . . . 92
7.4.2 Uniserial subgroups of $W_Q(s)$ . . . 93
7.4.3 Centralisers and normalisers . . . 95
7.5 Extensions of quaternion point groups . . . 103

References 107

Chapter 1

Introduction

Groups arise in different areas of science, for example, in quantum theory, crystallography and cryptography. Group theory originated from the works of Lagrange [15], Ruffini [81] and Galois [38] around 1800 when they studied the solvability of algebraic equations by radicals. For this purpose they investigated the *permutations* of the roots of an equation. At that time no formal definition of a group was introduced but they studied what we now know as permutation groups. A very first definition of an abstract group was given by Cayley [8] in 1878. He also used a table to illustrate the laws of operations of group elements, the so-called multiplication table. He further tried to visualise these laws in a graph, see [9], which led to the so-called Cayley graph. Years later, the work of von Dyck [27] made group theory more popular when he formally introduced presentations of groups. Thereafter the scope and applications of group theory grew gradually and at the beginning of the 20th century group theory flourished with the works of many mathematicians.

A prominent theme in group theory is the classification of finite groups. The aim of classification of a given class of groups is to find an explicit list of isomorphism type representatives such that no two groups in the list are isomorphic and every group in the given class is isomorphic to a group in the list. For example, the famous *Classification Theorem of finite simple groups* accounts for all finite simple groups. Every finite group can be constructed as an iterative extension of finite simple groups, however, this process is highly non-trivial and rarely leads to a practical classification of finite groups. In this thesis we restrict our attention to finite p-groups, that is, finite groups of p-power order for a prime p. It is known that p-groups play an important role in group theory. For example Cauchy's Theorem tells us that every finite group whose order is divisible by p contains a subgroup which is a non-trivial p-group. A stronger result is given by Sylow's Theorem [85].

Theorem 1.1 (Sylow's Theorem)**.** *Let G be a finite group of order $|G| = p^a m$ where p is a prime and $p \nmid m$. Then G has a subgroup P, called a Sylow-p-subgroup of G, of order p^a and every subgroup of G, which is a p-group, is conjugate to a subgroup of P.*

The aim of classifying finite p-groups by order is to find an explicit list of isomorphism type representatives of groups of order p^n where we have fixed a prime p and a positive integer n. There have been many attempts to classify finite p-groups by order. A notable investigation is done by Besche, Eick and O'Brien (see [1]). In fact their results were used for parts of the small groups library for the computer algebra system GAP [39]. Some other recent works are carried out by Newman, O'Brien and Vaughan-Lee [46, 47] where they classified the groups of order dividing p^7. Another famous example is the PORC (**p**olynomial **o**n **r**esidue **c**lasses)-conjecture by Higman [46, 47] which claims that for fixed n there exists a polynomial in p which depends only on the residue class of p modulo some fixed integer N such that the number of p-groups of order p^n is given by this polynomial. This conjecture is still open, however recent works by Vaughan-Lee [86, 87] shed more light into the conjecture and provide a deeper insight into the structure of finite p-groups.

Table 1: Number of 2-groups.

Order	Number of groups
2	1
4	2
8	5
16	14
32	51
64	267
128	2328
256	56092
512	10494213
1024	49487365422
2048	>1774274116992170

Higman and Sims [84] also showed that there are $p^{2n^3/27+O(n^{8/3})}$ isomorphism types of groups of order p^n. All these works show that finite p-groups have a very intricate structure and for a fixed prime the number of groups of order p^n grows very fast when n increases, see Table 1; details can be found in [25, 46, 47, 84]. For larger exponents, the sheer number of groups of a fixed prime-power order p^n makes the classification of finite p-groups by order seem impossible. For example, there is no explicit classification of the 49487365422 groups of order 2^{10}. The above discussion indicates that it might be useful to classify p-groups by some invariant other than the order. Besides the order, the (nilpotency) class is thus a natural invariant. Finite p-groups of class ≤ 1 are abelian, and easily described. However, finite p-groups of class ≥ 2 defy classification, as in a

sense they are as complicated as all finite groups, and because intractable problems, like determining simultaneous canonical forms of two endomorphisms of a vector space, are hard to be reformulated within their realm.

1.1 Coclass and coclass graphs

A different approach to classifying finite p-groups is to consider all such groups of a fixed *coclass* (see definition below); this invariant has been formulated by Leedham-Green and Newman [60] in 1980 and, since then, has led to a new area called *Coclass Theory*. We first recall the definition of the lower central series of a group.

Definition 1.2. Let G be a group.

a) The lower central series (or descending central series) of G is the descending series of subgroups

$$G = \gamma_1(G) \geq \gamma_2(G) \geq \ldots \geq \gamma_n(G) \geq \ldots,$$

where each $\gamma_{n+1}(G) = [\gamma_n(G), G]$, the subgroup of G generated by all commutators $[x, y] = x^{-1}x^y = x^{-1}y^{-1}xy$ with x in $\gamma_n(G)$ and y in G.

b) If the lower central series of G terminates in the trivial subgroup, say $\gamma_n(G) > \gamma_{n+1}(G) = 1$, then G is nilpotent of (nilpotency) class $\mathrm{c}(G) = n$.

Coclass describes the relation between the order of a finite p-group and its class.

Definition 1.3. The coclass of a finite p-group G of order p^n is $\mathrm{cc}(G) = n - \mathrm{c}(G)$.

One of the first major results in coclass theory is due to Blackburn [25] who obtained a full classification of the 2- and 3-groups of maximal class. These groups can be defined by "*parametrised presentations*"; these are group presentations whose defining relations have exponents which are arithmetic expressions containing finitely many indeterminate integers as parameters. For example we note from [25] that the isomorphism types of 2-groups of maximal class with order 2^n and $n \geq 4$ are given by the following parametrised presentations of dihedral, semi-dihedral, and generalised quaternion groups respectively.

$$\begin{aligned} D_{2^n} &= \langle a, b \mid a^{2^{n-1}} = 1, b^2 = 1, a^b = a^{-1} \rangle \\ SD_{2^n} &= \langle a, b \mid a^{2^{n-1}} = 1, b^2 = 1, a^b = a^{2^{n-2}-1} \rangle \\ Q_{2^n} &= \langle a, b \mid a^{2^{n-1}} = 1, b^2 = a^{2^{n-2}}, a^b = a^{-1} \rangle \end{aligned} \tag{1.1}$$

Any such classification for $p \geq 5$ and coclass 1 is still not available but many deep results on the structure of these groups are obtained during the investigation of p -groups of

maximal class, for example see [18–20, 56–59]. In fact, inspired by Blackburn's approach to the groups of maximal class, Leedham-Green and Newman [60] started the more general *classification by coclass project*. Together with Definition 1.3, Leedham-Green and Newman proposed five conjectures, known as Conjectures A - E, on the structure of the p-groups of a fixed coclass, we give more details in Section 3.1. These conjectures were investigated over the past decades and finally the strongest one, Conjecture A, was proved independently by Leedham-Green [52] and Shalev [83]. Both proofs used a wide range of theories involving pro-p-groups and Lie algebras. A detailed account of the proofs including further details and references is given in the book of Leedham-Green and McKay [53]. The other conjectures, Coclass Conjectures B - E can be deduced from Coclass Conjecture A, though this is not obvious; a discussion is included in Section 3.2. Since all Coclass Conjectures have been proved, we call them Coclass Theorems. Along the way coclass theory has delivered significant insight into the structure of the p-groups of a fixed coclass. For example, Eick and Leedham-Green [35] introduced certain infinite sequences of p-groups of fixed coclass, so-called *infinite coclass sequences*. It was then proved that for each infinite coclass sequence the groups in this sequence can be described by a parametrised presentation. An advantage of coclass sequences is that they allow one to prove results for an infinite family of groups; results of this flavour have been obtained for automorphism groups, Schur multipliers, character degrees, etc. For example, Eick used these sequences in [31] to investigate the order of the automorphism groups of finite 2-groups of fixed coclass. It is thus believed that the coclass project is capable of producing a detailed description of finite p-groups. We note from [21] that an important conjecture underpinning the coclass project is the following.

Conjecture 1.4. *Let p be a prime and let r be a positive integer. The finite p-groups of coclass r can be divided into finitely many periodicity classes such that the structure of the groups in a periodicity class can be described in a uniform way. In particular all groups in a periodicity class can be defined by a single parametrised presentation.*

Conjecture 1.4 is vague since it has no precise definition of periodicity class. Later investigations and research in this direction identified what a periodicity class could be, we give more details in Section 2.2. In particular, we mention that Conjecture 1.4 is proved for $p = 2$ and arbitrary r; Section 2.2.1 explains why the case $p > 2$ is significantly more difficult. One can observe that if Conjecture 1.4 is true, then a classification of p-groups by coclass is possible and that would be a powerful step towards understanding of p-groups. However, there is only partial evidence available in full support for the above conjecture. We refer to [17–20, 34, 35, 53] for details, also see Section 2.2 for a brief discussion. In particular, Newman, Leedham-Green and McKay [35, 53] suggested that p-groups of coclass greater than 1 are more difficult to classify. In fact, there is still no classification available even for maximal class. We refer to the book [53] for more details

and references. We now discuss one of the most important tools in coclass theory, that is, the coclass graph.

The coclass graph $\mathcal{G}(p,r)$ associated with the finite p-groups of coclass r is an infinite (directed) graph which is defined as follows.

Definition 1.5. The vertices of $\mathcal{G}(p,r)$ are the isomorphism types of finite p-groups of coclass r where a vertex is identified with a group representing its isomorphism class. Two vertices G and H are connected $G \to H$ if and only if $G \cong H/\gamma_{c(H)}(H)$.

When visualising (parts of) $\mathcal{G}(p,r)$, groups of the same order are normally pictured on the same level and smaller groups above larger ones. This way, the direction of an edge is always from top to bottom, so we can leave out arrows. One of the easiest and best known examples is given in Figure 1, the coclass graph $\mathcal{G}(2,1)$: this graph consists of the Klein 4-group V_4, the cyclic group C_4 of order 4, the groups D_8 and Q_8, and the groups in (1.1).

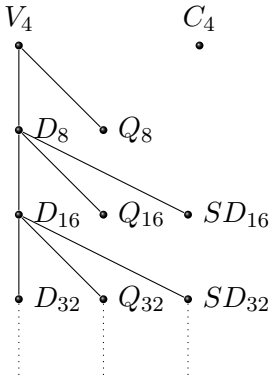

FIGURE 1: The coclass graph $\mathcal{G}(2,1)$.

Towards Conjecture 1.4, the structure of coclass graphs has been studied in detail and along the way many useful results were obtained. Many explicit computations of parts of coclass graphs have revealed surprising periodic patterns, which in some cases have been proved (on a group-theoretic level). It is one of those important results that says that a coclass graph can be partitioned into a finite subgraph, and finitely many infinite trees, so-called *coclass trees*, each having exactly one infinite path (*mainline*) starting at its root; a detailed description and properties of coclass graphs are discussed in Chapter 2.

Since the general structure of $\mathcal{G}(p,r)$ is determined by the structure of its coclass trees, the main aim of coclass theory in recent years is to understand these trees in more detail. There are two promising approaches to investigate coclass trees. First, one attempts to study the mainline groups via so-called *infinite pro-p-groups*: there is a one-one correspondence between the mainlines of coclass trees and certain infinite pro-p-group of coclass r, see Section 3.1. In particular, for a fixed coclass tree, the groups

on its mainline are the nilpotent quotients of the associated infinite pro-p-group. One important kind of such pro-p-groups is the *uniserial p-adic space group*; a brief discussion is given in Section 1.2. Second, the structure of the groups in a coclass tree can be studied by investigating the so-called *skeleton groups*. Those groups played an important role in the investigation of some special coclass graphs, such as $\mathcal{G}(3,2)$ in [34].

It is the aim of this thesis to enhance coclass theory by exploiting both of these approaches; the next sections give an outline of our contributions.

1.2 Uniserial p-adic space groups

Let $\mathbb{Q}_p$ and $\mathbb{Z}_p$ be the field of p-adic numbers and the ring of p-adic integers respectively. The additive group of p-adic integers $(\mathbb{Z}_p, +)$ is a classic example of *pro-p-groups*; these groups are inverse limits of finite p-groups; details are provided in Example 3.2. For example, $\mathbb{Z}_p$ is the inverse limit of the groups $\mathbb{Z}/p^n\mathbb{Z}$ with $n \in \mathbb{N}$, where the homomorphisms $\mathbb{Z}/p^i\mathbb{Z} \to \mathbb{Z}/p^j\mathbb{Z}$ are defined by $z + p^i\mathbb{Z} \mapsto z + p^j\mathbb{Z}$ for all $j \leq i$. As a result, the elements of $\mathbb{Z}_p$ can be considered as sequences $(a_n)_{n\in\mathbb{N}}$ such that each $a_n \in \mathbb{Z}/p^n\mathbb{Z}$ and $a_i \equiv a_j \bmod p^j\mathbb{Z}$ for $j \leq i$ and the addition is done pointwise.

The definition of coclass can be extended to infinite pro-p-groups: the coclass of an infinite pro-p-group S with nilpotent quotients $S_j = S/\gamma_j(S)$ for $j \geq 2$ is defined as $\mathrm{cc}(S) = r$ if there is an integer t such that S_j is a finite p-group of coclass r for all $j \geq t$. Any such pro-p-group will define an infinite path $S_t \to S_{t+1} \to \ldots$ in the coclass graph $\mathcal{G}(p,r)$. On the other hand, the inverse limit of the groups on the infinite path of a coclass tree in $\mathcal{G}(p,r)$ is an infinite pro-p-group of coclass r. For example the inverse limit of the groups in the mainline of $\mathcal{G}(2,1)$ is the infinite dihedral group; that is $D_8 \to D_{16} \to \cdots$ yields $\varprojlim D_{2^n} = \varprojlim C_2 \ltimes C_{2^n} = C_2 \ltimes \mathbb{Z}_2$ with C_2 acting via inversion on $\mathbb{Z}_2$.

Interestingly, Coclass Theorem D shows that there are only finitely many isomorphism types of infinite pro-p-groups of coclass r. It is known that such pro-p-groups are closely related to *uniserial p-adic space groups*. A detailed description of such groups is given in Section 3.1. Here we briefly discuss the definition. We denote d copies of the abelian group $(\mathbb{Z}_p, +)$ and $(\mathbb{Q}_p, +)$ by $\mathbb{Z}_p^d$ and $\mathbb{Q}_p^d$ respectively for any positive integer d. We start with the definition of uniserial action from [53, Section 7.4]. A finite p-group P acts uniserially on a $\mathbb{Z}_pP$-module T if $[T : T_i] = p^i$ for all $i \geq 0$ where $T_0 = T$ and $T_i = [T_{i-1}, P]$ for all $i \geq 1$. Here $[T_{i-1}, P]$ is the subgroup of T_{i-1} generated by the elements $-t + t^g$ where $t \in T_{i-1}$ and $g \in P$. The linearly ordered series $T = T_0 > T_1 > T_2 > \ldots$ is the uniserial series for this action. A uniserial p-adic space group S of dimension d is an extension of $T \cong \mathbb{Z}_p^d$ by a finite p-group P where P acts faithfully and uniserially on

T. For such a uniserial p-adic space group, P is called the point group and T is called the translation subgroup of S. Since these uniserial p-adic space groups are important, a constructive classification for determining these groups is thus considered to be an important tool for the investigation of $\mathcal{G}(p,r)$. For odd primes there is an algorithm, given by Eick [30] to determine these space groups. However the case $p = 2$ remained open and only special instances of point groups were considered in [44]. One aim of this thesis is to fill this gap and to complete the constructive classification of uniserial p-adic space groups for all primes; details are given in Chapter 7.

1.3 Skeleton groups

Since the structure of coclass trees is in general very intricate, one possible way to look into these trees is to first restrict attention to certain subgraphs. One such important subgraph is the graph spanned by skeleton groups. These groups are *twisted* finite quotients of the pro-p-group associated with the coclass tree. It is to be noted that the main difficulty towards proving Conjecture 1.4 is that so far there is no method known to take account of the groups in a coclass tree which are far away from a mainline group. Skeleton groups can provide a meaningful approach to overcome this difficulty. Since Conjecture 1.4 is proved for $p = 2$, we assume that p is an odd prime in the following. Motivated by the results in [53], we prove in Theorem 4.19 that almost every group in the graph $\mathcal{G}(p,r)$ is *close* (of distance bounded in p and r) to a skeleton group. Skeleton groups therefore determine the general structure of coclass graphs. These groups are studied in [17–20, 34] for special cases motivated by so-called *constructible groups* defined in [53, Section 8.4]. One aim of this thesis is to introduce a systematic treatment of the skeleton groups of any coclass. To define skeleton group in a coclass tree, one starts with the associated uniserial pro-p-group S. If S has translation subgroup T and point group P, then the skeleton groups are defined as extensions of a twisted quotient of T (twisted by a $\mathbb{Z}_pP$-module homomorphism $\gamma : T \wedge T \to T$) by the point group P. The detailed description is provided in Chapter 4. An immediate problem is to decide when two homomorphisms lead to isomorphic skeleton groups. Only special instances of this problem are discussed in current literature, for example see [18, 20, 34]. One aim of this thesis is to study this isomorphism problem in a more general context. An isomorphism between skeleton groups induced by the automorphism of S is called an *orbit isomorphism* in [34]; this situation is particularly interesting since it means that the construction of skeleton groups up to isomorphism depends solely on the structure of S. However, it is also shown in [34] that there exist *exceptional isomorphisms* between skeleton groups which are not induced by automorphisms of S. We investigate some cases where all isomorphisms between skeleton groups can be realised by orbit isomorphisms,

see Chapter 5. These results will be utilised in Chapter 6 to derive some new structure results for coclass trees. The contents of the Chapters 4 and 5 are published in [22].

1.4 Outline of the thesis

- Chapters 2 and 3 are dedicated towards preliminary definitions and results. In these chapters we will also introduce the notations required to describe coclass graphs and pro-p-group of coclass r. These chapters contain the background for the rest of the thesis.

- Chapter 4 is about skeleton groups. As mentioned before, we introduce a systematic description of skeleton groups; for example:
  - We define skeleton groups for general coclass r, see Definitions 4.4 and 4.7.
  - We show that almost every group in a coclass graph is *close* to a skeleton group, see Theorem 4.19.

- The isomorphism problem of skeleton groups was investigated in special cases, for example, $p = 3$ and $r = 2$ (see [34]) or $p \geq 3$ and $r = 1$ (see [20]). In Chapter 5 we study the isomorphism problem in a more general situation; for example:
  - We provide a complete solution of the isomorphism problem in two important cases (pro-p-groups with cyclic or meta-cyclic point groups), see Section 5.2.2.
  - We identified and corrected gaps in two proofs in [34] related to the isomorphism problem, see Remarks 5.2, 5.7 and 5.13.

  Contents of Chapters 4 and 5 are published in [22].

- In Chapter 6 we discuss some properties and applications of skeleton groups which *do not* admit exceptional isomorphisms. Based on our results in Chapter 5, we improve a known periodicity result for coclass graphs, see Theorem 6.4. In Theorem 6.43 we also provide a family of examples that shows that a conjectured periodicity result in [18] (about "periodic parents") cannot be true. This illustrates that despite the existence of several periodic patterns in $\mathcal{G}(p, r)$, it still remains a challenge to use periodicity towards a proof of Conjecture 1.4 for odd p.

- In Chapter 7 we discuss uniserial 2-adic space groups. A theoretical insight into these groups is important to understand the coclass trees in $\mathcal{G}(2, r)$. The results of this chapter are motivated by the constructive classification of space groups for odd primes given by Eick [35]. The case $p = 2$ is more complicated, because of the existence of so-called *quaternion point groups*. Our main result is a constructive classification similar to the odd prime case.

Chapter 2

The Coclass Graph $\mathcal{G}(p, r)$

In this chapter, we discuss some known structural results for coclass graphs. A detailed account of these results can be found in [18, 19, 34, 53]. Recall the definition of coclass and coclass graph from Chapter 1. A few more notations are needed for further discussion. A group H in $\mathcal{G}(p, r)$ is a *descendant* of a group G if $G = H$ or if there is a path from G to H in $\mathcal{G}(p, r)$. If this path has length 1, then H is an *immediate descendant* of G and G is called the *parent* of H. A group G in a coclass graph is called *terminal* if it has no descendant except G itself. If this is not the case then G is called *capable*. One example of a coclass graph is given in Figure 1. Another example of $\mathcal{G}(2, 2)$ is given in Figure 2. However, structures of these graphs are relatively easy compared to the general structure of coclass graphs. In order to understand the full scale of the complicacy one can observe that except for few graphs like $\mathcal{G}(2, 1)$, $\mathcal{G}(3, 1)$ and $\mathcal{G}(5, 1)$ it currently seems impossible to sketch significant parts of other coclass graphs. As mentioned in Chapter 1, with finitely many exceptions, every group in $\mathcal{G}(p, r)$ lies in a coclass tree; we first give a formal definition of these trees.

2.1 Coclass trees

The descendant tree of a group G in $\mathcal{G}(p, r)$ is the subtree of $\mathcal{G}(p, r)$ which is induced by all descendants of G.

Definition 2.1. A coclass tree of $\mathcal{G}(p, r)$ is a descendant tree which is maximal with respect to the property that its root is the initial vertex of exactly one infinite path. This unique maximal path is the *mainline* of the coclass tree.

For example, the coclass graph $\mathcal{G}(2,1)$ has only one coclass tree and its mainline starts from V_4, see Figure 1. $\mathcal{G}(2,2)$ has five coclass trees, see Figure 2 where the roots of the coclass trees are indicated by the boxes.

As mentioned in the Introduction, coclass trees are uniquely associated with infinite pro-p-groups of finite coclass; this relationship will be described in Chapter 3. Here we only concentrate on the graph-theoretic structures and hence refrain from giving any details on the related pro-p-groups.

The next theorem, which was obtained in the course of proving the Coclass Theorems, describes the general structure of coclass graphs. Details can be found in [53, Corollary 11.2.3]. Since the proof involves structural results of pro-p-groups, we give a brief proof in Theorem 3.5 and Lemma 3.6.

Theorem 2.2. *The graph $\mathcal{G}(p,r)$ consists of finitely many coclass trees and finitely many groups not lying in any coclass tree.*

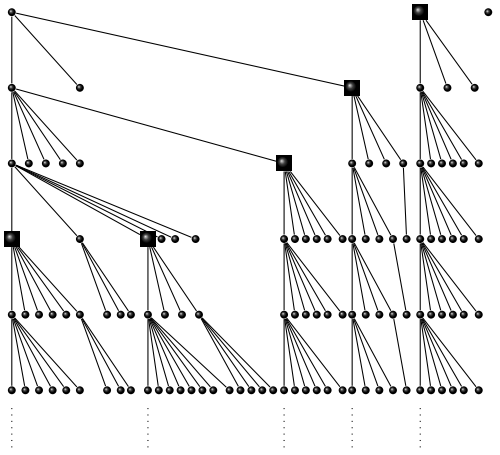

FIGURE 2: The coclass graph $\mathcal{G}(2,2)$ and the roots of its coclass trees.

We now need some more notation to describe coclass trees. The depth of a vertex in a rooted tree is its distance from the root, and the depth of a rooted tree is the maximum depth of a vertex in the tree. The width of a rooted tree is the maximum number of vertices at the same depth.

Definition 2.3. Let $\mathcal{T}$ be a coclass tree with mainline $S_1 \to S_2 \to \ldots$.

a) The j-th branch $\mathcal{B}_j$ of $\mathcal{T}$ is the subtree of $\mathcal{T}$ induced by all descendants of S_j which are not descendants of S_{j+1}. For a positive integer k, denote by $\mathcal{B}_j[k]$ the subtree of $\mathcal{B}_j$ induced by the groups of depth at most k in $\mathcal{B}_j$.

b) For a positive integer k, the shaved coclass graph $\mathcal{G}_k(p,r)$ is the subgraph of $\mathcal{G}(p,r)$ induced by the mainline groups of the coclass trees in $\mathcal{G}(p,r)$ and their descendants of distance at most k.

Thus, by construction, the branches of a coclass tree are finite subtrees which are pairwise disjoint and connected via the mainline, see Figure 3.

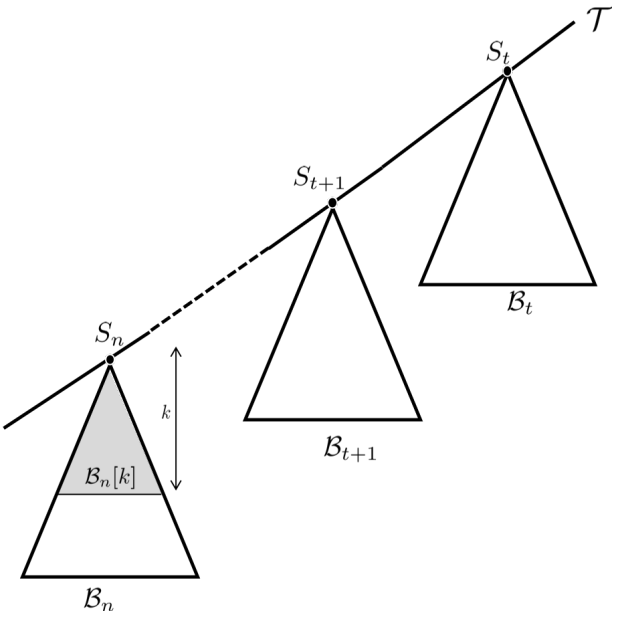

FIGURE 3: Branches of a coclass tree.

Theorem 2.2 describes the general structure of a coclass graph, but it remains to describe the structure of its coclass trees. For example, it is known that $\mathcal{G}(p, 1)$ has only one coclass tree; if $p \geq 7$, then the set of widths of its branches is unbounded, see [20, Corollary 1.2]. In fact, the size of the branches increases too fast for a reasonable amount of computational examination. Even the branches of the coclass tree of $\mathcal{G}(5, 1)$ are much more complicated then the branches we have seen in $\mathcal{G}(2, 1)$ and $\mathcal{G}(2, 2)$; Figures 4 and 5 display the branches $\mathcal{B}_{14}$ and $\mathcal{B}_{18}$ of $\mathcal{G}(5, 1)$ having roots of order 5^{14} and 5^{18}; in these figures, a vertex labelled with an integer m stands for m terminal immediate descendants of the corresponding parent; we refer to [17, Chapter 10] for more details.

Many computer experiments suggest that significant parts of the branches in a coclass tree exhibit periodic patterns; this is well illustrated in the graphs shown in Figures 1 and 2; see also Figures 4 and 5. A good deal of current research, for example [17, 18, 20], is now concentrated on studying periodicity results. We discuss some of these results in the following sections.

2.2 Periodicities

Motivated by the observed periodic patterns and the success for $p = 2$, one aims to find a finite description of coclass graphs for all prime and coclass. This will also allow to draw conclusions from these graph-theoretic structures to the structure of the groups

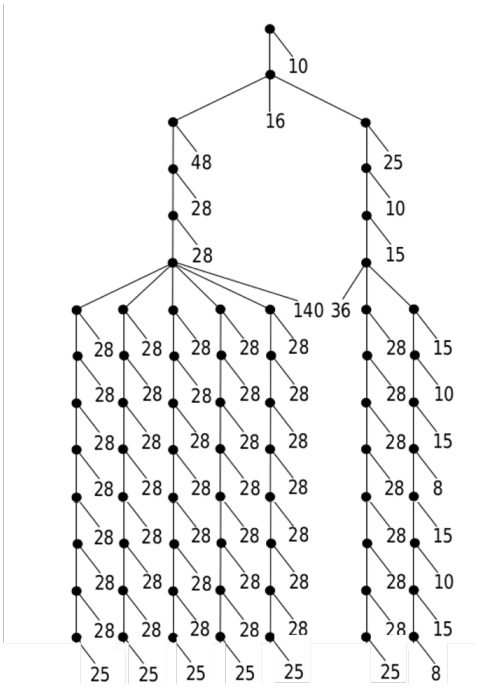

FIGURE 4: $\mathcal{B}_{14}$ of the coclass tree in $\mathcal{G}(5, 1)$.

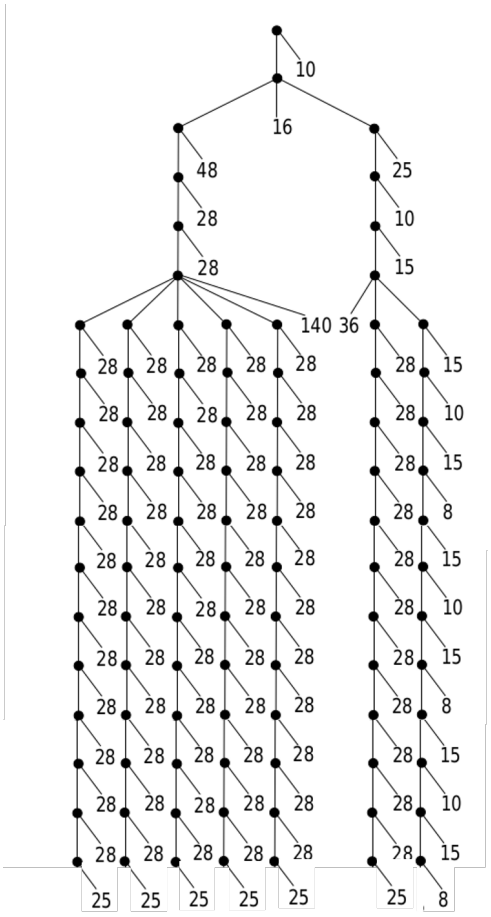

FIGURE 5: $\mathcal{B}_{18}$ of the coclass tree in $\mathcal{G}(5, 1)$.

involved. Towards this aim one considers the following conjecture, see [17, Section 1.1.2]; this is a weaker version of Conjecture 1.4.

Conjecture 2.4. *Let p be a prime and r be a positive integer. The coclass graph $\mathcal{G}(p,r)$ can be described by a finite subgraph and periodic patterns.*

Newman and O'Brien examined the coclass graph $\mathcal{G}(2,r)$ in detail and suggested that Conjecture 2.4 is true for $\mathcal{G}(2,r)$, see [73]. They proposed Conjecture P which is proved independently by du Sautoy [25] and later by Eick and Leedham-Green [35]. Since Conjecture P is now proved, we denote this as Theorem P.

Coclass Theorem P. *If $\mathcal{T}$ is a coclass tree of $\mathcal{G}(2,r)$ with branches $\mathcal{B}_1, \mathcal{B}_2, \ldots$, then there exists an integer $d = d(\mathcal{T})$ such that, up to finitely many exceptions, for $j \geq 1$ the branches $\mathcal{B}_j$ and $\mathcal{B}_{j+d}$ are isomorphic as rooted trees.*

Theorem P is the first evidence towards Conjecture 2.4. The proof was first completed by du Sautoy [25] using zeta functions and model theory. This proof was a qualitative version of the conjecture and was non-constructive in the sense that one cannot obtain any information of the groups involved. The constructive proof by Eick and Leedham-Green [35] is based on an explicit group-theoretic construction. In fact, the results of du Sautoy, Eick and Leedham-Green not only hold only for $p = 2$, but also for any shaved coclass tree for any prime p and fixed coclass $r \geq 1$. These results lead to what is now known as *periodicity of type I*.

2.2.1 Periodicity of type I

The periodicity of type I deals with shaved coclass trees $\mathcal{G}_k(p,r)$. It says that for a chosen depth k and for all large enough n, the shaved branch $\mathcal{B}_n[k]$ repeats itself in some subsequent branches. We first state the result here, see also Figure 6.

Theorem 2.5. *If $\mathcal{T}$ is a coclass tree in $\mathcal{G}(p,r)$ with branches $\mathcal{B}_1, \mathcal{B}_2, \ldots$ then for every positive integer k, there exist integers $f = f(\mathcal{T}, k)$ and $d = d(\mathcal{T})$ such that, for every $n \geq f$, there is a graph isomorphism $\pi_n : \mathcal{B}_n[k] \to \mathcal{B}_{n+d}[k]$.*

Theorem 2.5, also known as the periodicity of type I, shows that the shaved coclass graph $\mathcal{G}_k(p,r)$ can be described by a finite subgraph and periodic patterns. The constructive proof in [35] is based on an explicit group-theoretic construction and describes the groups in a coclass tree $\mathcal{T}$ as suitable group extensions and then uses cohomology theory to deduce the required graph isomorphisms. In this approach, detailed information on the periodicity is uncovered. Importantly, the explicit description of the graph isomorphisms helps to describe the structure of the groups involved. The proof also provides explicit

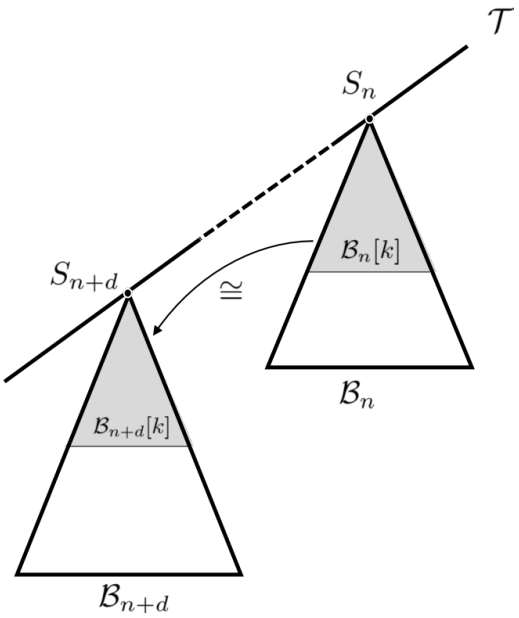

FIGURE 6: Periodicity of type I.

bounds for the parameters mentioned in Theorem 2.5. As a result of these explicit bounds, the periodicity of type I tells us that if there is an upper bound for the depths of all branches of a particular coclass tree, then the whole coclass tree can be constructed from a finite subtree with finitely many calculations using periodicity of type I. The latter holds for all coclass tree if $p = 2$. Consequently it is shown in [35] that the 2-groups of coclass r can be described by finitely many parametrised presentations with one integer parameter, similar to the groups in (1.1). This proves Conjecture 1.4 for $p = 2$ and generalises (1.1). However the case $p \geq 3$ is widely open because in general there is no bound for the depths of all branches of a particular coclass tree.

The periodicity of type I is significantly improved in the case of coclass 1 by Dietrich [19]. We briefly summarise the results related to this improvement; details can be found in [17–19]. Fix a prime $p \geq 7$ and consider the graph $\mathcal{G}(p,1)$ (the case $p \geq 5$ is similar but needs some technical adjustments). Let $e_n = \max\{0, n-2p+8\}$ and $c_p = 4p-19$. The following results have been proved in [17, Theorem 2.6] and [19, Theorem 1.1]; see Figure 7 for an illustration.

Theorem 2.6. *Using the notation of the previous paragraph the following hold.*

a) *If $n \geq p+1$, then $\mathcal{B}_n[e_n] \cong \mathcal{B}_{n+p-1}[e_n]$ as rooted trees.*

b) *The depth of $\mathcal{B}_n$ is at least e_n and at most $e_n + c_p$.*

Eick and Leedham-Green [35] determined an upper bound for the parameter f mentioned in Theorem 2.5. Using these bounds for coclass 1, one can show that a shaved subtree of $\mathcal{B}_n$ of depth approximately $n/6d$ can be embedded into $\mathcal{B}_{n+d}$ where $d = p-1$. In contrast, the periodicity result in Theorem 2.6 embeds the subtree of $\mathcal{B}_n$ of depth $e_n \approx n$

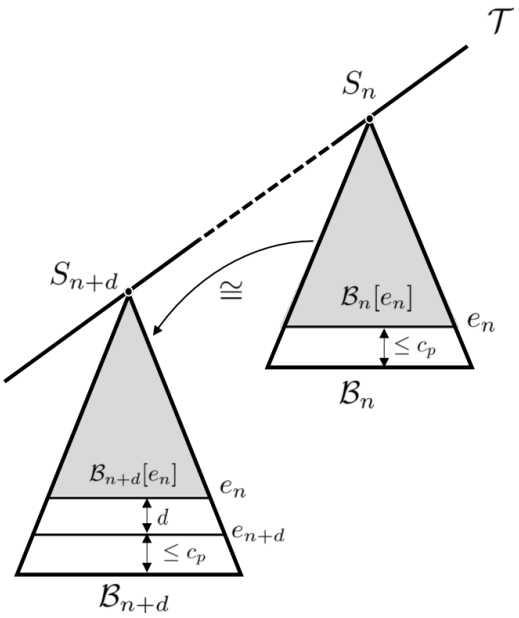

FIGURE 7: Periodicity of type I for coclass 1 where $d = p - 1$.

into $\mathcal{B}_{n+p-1}$. Thus Theorem 2.6 is a stronger version of the periodicity of type I as given in Theorem 2.5. In this thesis we demonstrated a similar improvement for a special class of skeleton groups see Theorem 6.4 for details.

In general, it is not possible to describe whole coclass graph in general using the periodicity of type I. The difficulties are two-fold. One problem is that the number of coclass trees in $\mathcal{G}(p,r)$ grows quickly as r grows. Eick [30, Section 6] showed that $\mathcal{G}(3,3), \mathcal{G}(3,4)$, and $\mathcal{G}(5,3)$ already have more than $10^3, 10^{11}$, and 10^{16} coclass trees respectively; this makes an explicit classification nearly impractical with a few exception like $p = 2$. Another problem is that for odd primes the set of depths of the branches in a coclass tree is usually unbounded. In fact from [35, Remark 4] we can see that there exists an integer k such that almost all vertices of $\mathcal{G}(p,r)$ are contained in $\mathcal{G}_k(p,r)$ only if either $p = 2$, or both $p = 3$ and $r = 1$. This explains why not all coclass graphs can be described using the periodicity of type I: for odd primes, it is necessary to consider the unbounded growth of the branches. The aim is to use a second periodic pattern to describe the growth of the branches. It seems to be true that descendant tree of a group deep enough in a branch is isomorphic to the descendant tree of a group in a previous branch. In order to describe the coclass tree by a finite calculation, we need a description of the said isomorphisms. The periodicity results that take account such branches are known as *periodicity of type II*. Currently this is investigated by considering *periodic parents*, see [18, 20] for details. But there is still not enough evidence to support Conjecture 1.4. However, partial evidence is available for special cases, see [20, 34] for details. We briefly discuss these in the next section.

2.2.2 Periodicity of type II

Let us fix a coclass tree $\mathcal{T}$ with branches $\mathcal{B}_n$ for $n \geq 1$. Let k be an integer and define the k-step descendant tree $\mathcal{D}_k(G)$ of a group G in $\mathcal{B}_n$ as the subtree of $\mathcal{B}_n$ induced by the descendants of distance at most k from G. Let the depth of the branch $\mathcal{B}_n$ in $\mathcal{T}$ be M_n. Also suppose m_n is as large as possible such that $\mathcal{B}_n[m_n] \cong \mathcal{B}_{n+d}[m_n]$. So by Theorem 2.5, for suitably chosen n, the shaved branch $\mathcal{B}_{n+d}[m_n]$ can be constructed from $\mathcal{B}_n[m_n]$. Let $r_n = M_{n+d} - m_n$; we recall from Theorem 2.6 that for a fixed prime p and coclass 1, we have $r_n = p - 1$ (a constant in p) which might not be true in general. So, if the branches have unbounded depths (there is no upper bound for all M_n), then in order to describe the coclass tree, we need to describe the groups in $\mathcal{D}_{r_n}(G)$ for every group G at depth m_n in $\mathcal{B}_{n+d}$. Computer experiments [18] suggest that for $r = 1$ and $p = 5, 7, 11$, almost always the unique ancestor H at distance $p-1$ from G satisfies $\mathcal{D}_{p-1}(G) \cong \mathcal{D}_{p-1}(H)$, see Figures 4 and 5. Hence, one expects that, in general, for a given group G at depth m_n, there is a group H at depth $m_n - r_n$ such that $\mathcal{D}_{r_n}(H) \cong \mathcal{D}_{r_n}(G)$ in $\mathcal{B}_{n+d}$, see Figure 8. In [18], such a group H is called a periodic parent of G.

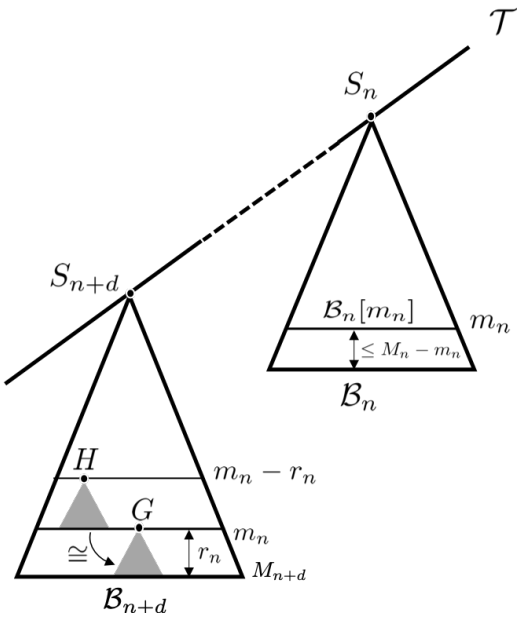

FIGURE 8: Periodic parent.

Computer experiments for $p \geq 7$ suggest that there are infinitely many groups (deep within the branches) for which the $(p-1)$-step parent is not a periodic parent; in fact, we prove in Theorem 6.43 that there is an infinite family of groups in $\mathcal{G}(7,1)$ where this fails. However, a modified result for coclass 1 is obtained in [18, Theorem 1.2].

Theorem 2.7. *Consider $\mathcal{G}(p,1)$ with $p \geq 5$ and $p \equiv 5 \bmod 6$. Write $d = p-1$. There is an integer $n_0 = n_0(p)$ such that, for all $n \geq n_0$, the following holds. Let G be a group*

at depth e_n in $\mathcal{B}_{n+d}$ having immediate descendants and let H be the d-step parent of G. If the automorphism group of H is a p-group, then H is a periodic parent of G.

In addition to Theorem 2.7, a stronger yet partial result for periodic parents in $\mathcal{G}(p,1)$ has been proved in [18, Theorem 1.3]. One can observe from [18] that the condition $p \equiv 5 \bmod 6$ plays an essential role for these results to be true. Our results in Theorem 6.43 suggests that the statement of Theorem 2.7 is not true for $p \equiv 1 \bmod 6$.

Computer experiments for coclass greater than 1 also suggested some other interesting periodic patters. Conjecture W [34] is one of them; it proposes a new periodicity that could be used to describe the branches with unbounded depth, see Figure 9. We state Conjecture W after introducing some required notation. Recall from Section 1.3 that the skeleton groups are defined via some homomorphisms. Let $\Gamma_{j,k}$ be the subgraph induced by the skeleton groups of depth k in the branch $\mathcal{B}_j$ of a coclass tree. One can verify that the periodicity of type I (as in Theorem 2.5) induces a bijection between the skeleton trees $\Gamma_{j,k}$ and $\Gamma_{j+id,k}$ for each $i \geq 0$. If $G \in \Gamma_{j+id,k}$ then let $\overline{G}$ be its image in $\Gamma_{j,k}$ under this bijection.

Conjecture W. *Let $\mathcal{T}$ be a coclass tree in $\mathcal{G}(p,r)$. Then there exist integers $d = d(\mathcal{T})$ and $l = l(\mathcal{T})$ such that if $\mathcal{B}_{l+id}$ for $i = 0, 1, \ldots$ is a sequence of branches in $\mathcal{T}$ of unbounded depth then there exist integers $k \geq d$ and a map $\nu : \Gamma_{l,k} \to \Gamma_{l,k-d}$ that satisfies the following: if G is in $\Gamma_{l+id,k}$, and H is in $\Gamma_{l+(i-1)d,k-d}$ such that $\nu(\overline{G}) = \overline{H}$, then the descendant trees of G and H are isomorphic.*

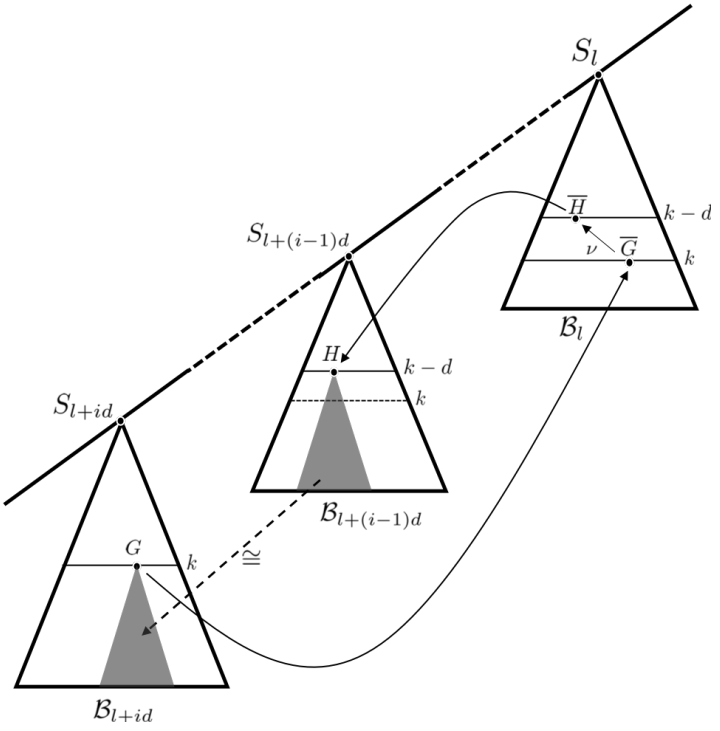

FIGURE 9: Conjecture W.

Following Theorem 2.5, for every k one can arrange the infinitely many branches of a coclass tree into d sequences such that $\mathcal{B}_n[k] = \mathcal{B}_{n+id}[k]$ for $i \geq 0$ and large enough n. The theorem then completely describes a sequence of branches of bounded depth k. Recall from Section 1.3 that almost every group in the graph $\mathcal{G}(p,r)$ is close (of distance bounded in p and r) to a skeleton group. Hence, Conjecture W, if true, along with this fact is capable of describing a sequence of branches of unbounded depth. We briefly illustrate how this can be done; we refer [34, Section 9] for details. Consider a coclass tree $\mathcal{T}$ with branches $\mathcal{B}_1, \mathcal{B}_2, \ldots$ having unbounded depth. We first choose an explicit value of k. The periodicity of type I implies that, for fixed $l \geq f(\mathcal{T}, k)$, the graphs $\mathcal{B}_{l+id}[k]$ are all isomorphic for all $i \geq 0$, and hence may be constructed using finite calculations, see Theorem 2.5. If Conjecture W is true then the descendant tree of $G \in \Gamma_{l+d,k}$ is isomorphic to the descendant tree of the image H of $\nu(\overline{G}) \in \Gamma_{l,k-d}$ in $\Gamma_{l+(i-1)d}$. Thus the subgraph of $\mathcal{B}_{l+d}$ containing both the skeleton groups of depth at most k and the descendants of groups at depth k may be constructed. Now the subgraph of $\mathcal{B}_{l+2d}$ containing both the skeleton groups of depth at most k and the descendants of groups at depth k can be constructed from the corresponding subgraph of $\mathcal{B}_{l+d}$ and the map ν using Theorem 2.5. The corresponding subgraphs of $\mathcal{B}_{l+id}$ for all $i > 0$ can be constructed recursively in the same way. Thus, the complete graphs $\mathcal{B}_{l+id}$ for all $i > 0$ may be constructed by a finite calculation using Theorem 2.5 provided Conjecture W is true. We note from [34] that the central difficulty in proving Conjecture W is finding a description for the map ν. The investigations of $\mathcal{G}(3,2)$ and $\mathcal{G}(5,1)$ suggest that ν can be defined by taking the d-step parent of a given group.

The periodicity of type I and the results related to periodic parents in case $p \equiv 5 \bmod 6$ produced a great insight into the structure of $\mathcal{G}(5,1)$; see [18, 19]. We recall some of the related results from [18, 19], a brief historical description can also be found in [20, Appendix A]. The investigation of the structure of $\mathcal{G}(5,1)$ started with the work of Newman [72]. Later Dietrich, Eick and Feichtenschlager [21], did extensive computer experiments which suggest in $\mathcal{G}(5,1)$ the following might be true: $\mathcal{B}_n[n-1] \cong \mathcal{B}_{n+4}[n-1]$ and $\mathcal{B}_{n+4} \setminus \mathcal{B}_{n+4}[n-1] \cong \mathcal{B}_n \setminus \mathcal{B}_n[n-5]$ for all large enough n. Afterwards Dietrich [18] proved that $\mathcal{B}_n[n-4] \cong \mathcal{B}_{n+4}[n-4]$ and $\mathcal{B}_{n+4}[n] \setminus \mathcal{B}_{n+4}[n-4] \cong \mathcal{B}_n[n-4] \setminus \mathcal{B}_n[n-8]$ for all large enough n. These periodicity results describe $\mathcal{G}(5,1)$ almost completely except the groups which are at the last 4 levels in the branches, see also Figures 4 and 5.

The structure of the branches in $\mathcal{G}(p,r)$ is still wide open and very little is known about these graphs. Conjecture W, if true, will be a powerful tool to investigate the branches with unbounded depth. This is because of the fact that almost every group in a branch, however deep, is at a bounded distance (in terms of p and r) from a skeleton group; we will elaborate this result in Chapter 4. Recently a fair amount of research work has been done on skeleton groups and often periodicity results are first investigated for the

skeleton subgraphs. The recent investigation in [20] (for odd p and $r = 1$) illustrates this well; it provides the first evidence supporting Conjecture W for coclass trees with branches of unbounded widths. Motivated by these results, we discuss skeleton groups in Chapters 4 and 5.

Chapter 3

Infinite Pro-p-Groups of Coclass r

This chapter aims to introduce the results related to infinite pro-p-groups of fixed coclass that play an important role in the structure of coclass graphs. The results in this chapter can be found in [23, 30, 51, 53–55, 65]

3.1 Infinite pro-p-groups and coclass graphs

The inverse limit of the groups in the mainline of any coclass tree is a special type of infinite pro-p-group. Here we give a detailed description of these groups. For further details we refer to the book by Dixon, du Sautoy, Mann and Segal [23, Chapter 10].

Definition 3.1. a) A partially ordered set $(I, \leq)$ is said to be *inductively ordered* if for all $i, j \in I$ there exists $k \in I$ such that $i \leq k$ and $j \leq k$.

b) Let $(I, \leq)$ be an inductively ordered set and $\{G_i \mid i \in I\}$ be a family of groups with surjective homomorphisms $\{\theta_{ij} : G_i \to G_j \mid j \leq i\}$ such that $\theta_{jk} \circ \theta_{ij} = \theta_{ik}$ for all $k \leq j \leq i$. Then $(\{G_i\}_{i\in I}, \{\theta_{ij}\}_{j\leq i})$ is called an *inverse system of groups* . Its *inverse limit* is defined as the subgroup G of $\prod_{i\in I} G_i$ consisting of the elements $(g_k)_{k\in I}$ such that if $j \leq i$ then $\theta_{ij}(g_i) = g_j$. We write $G = \varprojlim G_i$.

c) A pro-p-group is the inverse limit of an inverse system of finite p-groups.

If every G_i in the above definition is a finite group, then we can furnish $\prod_{i\in I} G_i$ with the product topology of discrete spaces. In this way, the inverse limit with the induced topology becomes a topological group, that is, a group which is a topological space such that group multiplication and inversion are continuous. In this thesis, we will not focus on the topological structure of a pro-p-group but the notion of *closed* or *open* subgroups of any such group will be followed according to the said definition of topological group, we refer to [53, Section 7.1] and [23, Chapter 1].

We can see from Definition 3.1 that any finite p-group is a pro-p-group. The classical infinite example is the additive group of p-adic integers $\mathbb{Z}_p$.

Example 3.2. Let p be a prime and for all $n \geq 1$ let $\mathbb{Z}/p^n\mathbb{Z}$ be the additive group of integers modulo p^n. Consider $\mathbb{N}$ as an inductively ordered set with natural order $\leq$ and let $\mathcal{F} = (\{\mathbb{Z}/p^i\mathbb{Z}\}_{i\in I}, \{\theta_{ij}\}_{j\leq i})$ be the inverse system of groups where $\theta_{ij} : \mathbb{Z}/p^i\mathbb{Z} \to \mathbb{Z}/p^j\mathbb{Z}$ is defined by $z + p^i\mathbb{Z} \mapsto z + p^j\mathbb{Z}$ for $j \leq i$. Then the inverse limit of $\mathcal{F}$ is $\mathbb{Z}_p$. Every integer m defines a p-adic integer by defining a sequence $(m \bmod p^n)_{n\in\mathbb{N}}$.

Remark 3.3. Following Example 3.2, it can be seen from [23, Lemma 1.24 and Definition 1.25] that for every pro-p-group G, there is a natural $\mathbb{Z}_p$-action where each $z \in \mathbb{Z}_p$ acts on $g \in G$ as $g^z = \varprojlim g^{z_n}$ with $z_n = z \bmod p^n$. Note that, if $g, h \in G$ commute and $y, z \in \mathbb{Z}_p$, then $g^{y+z} = g^y g^z$, $(g^y)^z = g^{yz}$, and $(gh)^z = g^z h^z$. In particular, if G is abelian, then G is a $\mathbb{Z}_p$-module. We note that a group G is finitely generated as a pro-p-group (that is as a topological group), if there exists a finite subset $X \subseteq G$ such that the only open subgroup of G containing $\langle X\rangle$ is G. For example, $(\mathbb{Z}_p, +)$ is generated (topologically) by $\{1\}$, whereas $\langle 1\rangle = (\mathbb{Z}, +)$ as abstract groups. In this context we note from [23, Chapter 1] that if G and H are pro-p-groups and G is finitely generated, then every abstract group homomorphism $G \to H$ is continuous. This means every homomorphism from a finitely generated pro-p-group G to a pro-p-group H is compatible with the $\mathbb{Z}_p$-action. In particular, the identity map $G \to G$ is continuous and, hence, the topology of G is determined uniquely by the group structure, see also [17, Section 5.2].

The definition of coclass can be extended to infinite pro-p-groups, see [53, Definition 7.4.1].

Definition 3.4. A pro-p-group S with nilpotent quotients $S_j = S/\gamma_j(S)$ has coclass $\mathrm{cc}(S) = r$ if there is an integer t such that S_j is a finite p-group of coclass r for all $j \geq t$. This is equivalent to saying that S_t is a finite p-group of coclass r and $\gamma_i(S)/\gamma_{i+1}(S)$ has order p for all $i \geq t$.

By definition, every infinite pro-p-group S of coclass r yields an infinite path $S_t \to S_{t+1} \to \ldots$ in the coclass graph $\mathcal{G}(p, r)$; in the following, the label of the branch $\mathcal{B}_n$ is usually chosen such that $\mathcal{B}_n$ has root $S_n = S/\gamma_n(S)$. On the other hand, the inverse limit of the groups on an infinite path in $\mathcal{G}(p, r)$ is an infinite pro-p-group of coclass r. For constructing these pro-p-groups, up to isomorphism, the inverse limit does not depend on the chosen epimorphisms, see [23, Chapter 10]. The following is one of the central theorems in coclass theory which relates the isomorphism types of infinite pro-p-groups of coclass r with the coclass trees in $\mathcal{G}(p, r)$. Given the importance of these pro-p-groups, we include a proof as given in [23, page 267].

Theorem 3.5. *There is a one-one correspondence between the isomorphism types of the infinite pro-p-groups of coclass r and the coclass trees of $\mathcal{G}(p,r)$.*

Proof. First consider a mainline $G_1 \to G_2 \to \ldots$ in $\mathcal{G}(p,r)$. Since G_{n+1} and G_n are connected in the coclass graph $\mathcal{G}(p,r)$, we can form a family of surjective homomorphisms $\phi_n : G_{n+1} \to G_n$. Taking the inverse limit, $G = \varprojlim G_n$ is an infinite pro-p-group. Note that each $|G_n| = p^{c+n-1+r}$ where $c = \mathrm{c}(G_1)$. As a result we have $\ker\phi_n = \gamma_{c+n}(G_{n+1})$. We first show that the infinite pro-p-group G is independent of the chosen epimorphisms. Suppose there is is a second family of epimorphisms $\psi_n : G_{n+1} \to G_n$, and and let G_ϕ and G_ψ be the inverse limits with respect to ϕ_n and ψ_n, respectively. Using [23, p. 267; Excercise 1(i)], for every $f_n \in \mathrm{Aut}(G_n)$ we find $f_{n+1} \in \mathrm{Aut}(G_{n+1})$ such that $\phi_n \circ f_{n+1} = f_n \circ \psi_n$. This produces an inverse system of groups given by $\ldots \to \mathrm{Aut}(G_{n+1}) \to \mathrm{Aut}(G_n) \to \ldots$ and since $\phi_n \circ f_{n+1} = f_n \circ \psi_n$ for all n, we deduce $G_\phi \cong G_\psi$, see [23, p. 267; Excercise 1(ii)]. This shows that G is independent of the chosen epimorphisms. In order to show that G has coclass r, we consider the natural projections $\pi_n : G \to G_n$. Suppose $K_n = \ker\pi_n$. Since $|G_n| = p^{c+n-1+r}$ and $\ker\phi_n = \gamma_{c+n}(G_{n+1})$, there is some N such that $|G : K_n\gamma_{i+1}(G)| = p^{i+r}$ for all $i \geq 1$ and $n \geq N$. This in turn shows that $G/\gamma_n(G)$ is a finite p-group and it has coclass r for all $n \geq N$. Hence G has coclass r.

Conversely, let G be an infinite pro-p-group of coclass r; let $m \geq 1$ be as small as possible such that $|G/\gamma_{i+1}(G)| = p^{i+r}$ for all $i \geq m$. We take $H_i = G/\gamma_{m+i}(G)$ for $i \geq 1$ with the natural projection maps. By definition each H_n is a finite p-group of coclass r and, by [23, p. 267; Excercise 2], it follows that $G = \varprojlim H_n$. Thus the groups $\{H_n \mid n \in \mathbb{N}\}$ form a mainline in $\mathcal{G}(p,r)$ which corresponds to the infinite pro-p-group G of coclass r. □

Coclass Theorem D (see Section 3.2 for the statement) shows that there are only finitely many isomorphism types of infinite pro-p-group of fixed coclass r. Recall that Theorem 2.2 tells us that there are finitely many coclass trees and finitely many groups outside these trees in any coclass graph. In view of Theorem 3.5, to complete the proof of Theorem 2.2, it now remains to show that there are only finitely many groups outside the coclass trees of a coclass graph. The proof below is based on the results provided in [53, Chapter 4].

Lemma 3.6. *In any coclass graph $\mathcal{G}(p,r)$, there are only finitely many groups outside the coclass trees.*

Proof. Let $\mathcal{S}$ be a family of pairwise non-isomorphic finite p-groups of coclass r such that no group in $\mathcal{S}$ is part of any coclass tree in $\mathcal{G}(p,r)$. We show that $\mathcal{S}$ is finite. Assume for a contradiction that $\mathcal{S}$ is infinite. Now let $\mathcal{S}_1 = \mathcal{S}$ and $X_1 = \langle 1\rangle$. By

assumption, the groups $G/\gamma_2(G)$ with $G \in \mathcal{S}_1$ all have order at most p^{r+1}. Hence the groups $\{G/\gamma_2(G) \mid G \in \mathcal{S}_1\}$ fall into a finite number of isomorphism classes. Thus, there are infinite subset $\mathcal{S}_2 \subseteq \mathcal{S}_1$ and a group X_2 such that $\mathcal{S}_2 = \{G \in \mathcal{S}_1 \mid G/\gamma_2(G) \cong X_2\}$. Inductively we can form a chain of infinite subsets $\mathcal{S}_1 \supseteq \mathcal{S}_2 \supseteq \ldots$ of $\mathcal{S}$ and a sequence of groups $X_1, X_2, \ldots$ such that $G/\gamma_i(G) \cong X_i$ for all $G \in \mathcal{S}_i$. As a consequence we have $X_{i+1}/\gamma_i(X_{i+1}) \cong X_i$. Thus the inverse limit of the groups X_i forms an infinite pro-p-group, say R. In addition, for all $i > 1$ there is $G \in \mathcal{S}$ such that $G/\gamma_i(G) \cong R/\gamma_i(R)$. Since every $G \in \mathcal{S}$ has coclass r it follows from [53, Corollary 11.1.5] that R has coclass r. Theorem 3.5 shows that R corresponds to coclass tree, say $\mathcal{T}_R$, and there will be some group $H \in \mathcal{S}_1$ such that $H \in \mathcal{T}_R$, a contradition. Hence, $\mathcal{S}$ is finite. □

Theorem 3.5 and Theorem D tell us that there are only finitely many coclass trees in a coclass graph. By Lemma 3.6 we see that there are finitely many groups outside these coclass trees; this completes the proof for Theorem 2.2.

3.1.1 Structure of infinite pro-p-groups

In this section we briefly discuss some of the important structural results for an infinite pro-p-group of finite coclass. We start with the definition of uniserial action.

Definition 3.7. A finite p-group P acts uniserially on a $\mathbb{Z}_pP$-module T if $[T : T_i] = p^i$ for all $i \geq 0$ where $T_0 = T$ and $T_i = [T_{i-1}, P]$ for all $i \geq 1$. Here $[T_{i-1}, P]$ is the subgroup of T_{i-1} generated by the elements $-t + t^g$ where $t \in T_{i-1}$ and $g \in P$. The linearly ordered series $T = T_0 > T_1 > T_2 > \ldots$ is the uniserial series for this action.

The following lemma connects certain subgroups of an infinite pro-p-group with the terms of its lower central series. The proof this lemma relies on many topological arguments, so we refrain from giving the details here, rather we refer to [53, Section 7.4] for a complete proof. This lemma will be used in the proof of many subsequent results.

Lemma 3.8. *Let G be an infinite pro-p-group of finite coclass such that $\gamma_i(G)/\gamma_{i+1}(G)$ is of order p for all $i \geq u$ for some integer u. Then*

a) *G is finitely generated as a pro-p-group.*

b) *If $j \geq u$ then $G/\gamma_j(G)$ acts uniserially on $\gamma_u(G)/\gamma_j(G)$, and if $N \triangleleft G$ and $\gamma_u(G) \geq N \geq \gamma_j(G)$, then $N = \gamma_i(G)$ for some $j \geq i \geq u$.*

The following, from [53, Lemma 7.4.10], is a structural result related to uniserial action.

Lemma 3.9. *Let P be a finite p-group acting uniserially on a $\mathbb{Z}_pP$-module T where the terms of the uniserial series are given by T_i for $i \geq 0$. If N is non-trivial $\mathbb{Z}_pP$-submodule of T then there is $j \geq 0$ such that $N = T_j$. Further if $T \cong \mathbb{Z}_p^d$ for some positive integer d then $T_{i+d} = pT_i$ for all $i \geq 0$.*

Proof. We first show that $\bigcap T_i$ is trivial. Note that for any $t > 0$, the quotient T/p^tT is finite and so $T_i \leq p^tT$ for some large enough i. This shows that $\bigcap_i T_i \leq \bigcap_t p^tT$ which is trivial. Now let N be a non-trivial $\mathbb{Z}_pP$-submodule of T. So N contains an element of $T_i \setminus T_{i+1}$ for some i. As N is closed and T_i/T_{i+1} is cyclic, it follows that N contains T_i. Since N contains an element of $T_i \setminus T_{i+1}$, we have $N = T_j$ for some $j \leq i$. This also proves the last assertion of the statement as pT_i is a $\mathbb{Z}_pP$-submodule and $|T_i : pT_i| = |T_i : T_{i+d}|$ for all $i \in \mathbb{Z}$. □

Many structural results of an infinite pro-p-group depend on its *hypercentre*.

Definition 3.10. The upper central series of a group G is the sequence of subgroups $1 = Z_0 \triangleleft Z_1 \triangleleft \cdots \triangleleft Z_i \triangleleft \cdots$, where each successive group is defined by $Z_{i+1}/Z_i = Z(G/Z_i)$. The hypercentre $Z_\infty(G)$ of G is defined as the union of the upper central series of G.

The next result, from [53, Lemma 7.4.4], describes the hypercentre of an infinite pro-p-group of finite coclass.

Lemma 3.11. *Let G be an infinite pro-p-group G of coclass r and let u be an integer such that $\gamma_i(G)/\gamma_{i+1}(G)$ has order p for all $i \geq u$. Then the hypercentre H of G has finite order p^h for some $h < r$, contains every finite normal subgroup of G and intersects $\gamma_u(G)$ trivially. Additionally, G/H is a group of coclass $r - h$ with trivial hypercentre.*

Proof. Following the definition of the hypercentre, it is sufficient to prove that the centre Z of G has finite order p^z with $z < r$, has non-trivial intersection with every non-trivial finite normal subgroup of G and intersects $\gamma_u(G)$ trivially, and that G/Z has coclass $r - z$. By Lemma 3.8 we find that $G/\gamma_j(G)$ acts uniserially on $\gamma_u(G)/\gamma_j(G)$ for all $j \geq u$. Note that the quotients $\gamma_i(G)/\gamma_{i+1}(G)$ are all cyclic for all $i \geq u$ and hence $\gamma_u(G)$ must intersect Z trivially; otherwise $G/\gamma_j(G)$ can not act uniserially on $\gamma_u(G)/\gamma_j(G)$. Since $\gamma_u(G)$ has finite index, Z is of finite order p^z; otherwise $\gamma_u(G)$ can not intersect Z trivially. Now let N be a non-trivial finite normal subgroup of G. Then N is a finite union of conjugacy classes, each of order p^i for some i. By the Orbit-Stabiliser Theorem, we find that the number of conjugacy classes with just one element must be a multiple of p and so N intersects Z non-trivially. Consider now $j \geq u$; since $\gamma_u(G)$ intersects Z trivially, $|G : \gamma_j(G)Z| = |G : \gamma_j(G)|p^{-z}$. Since $G/\gamma_j(G)Z$ has nilpotency class at most j, we have G/Z has coclass $r - z$ where $z < r$. □

We conclude this section with the following two lemmas which will be used later in the proof of Theorem 3.16.

Lemma 3.12. *Let G be a pro-p-group of finite coclass which has trivial centre. Then G contains a unique subgroup which is maximal with respect to being open normal self-centralising abelian; this subgroup is a free $\mathbb{Z}_p$-module of finite rank.*

Proof. We describe the proof as given in [53, Corollary 7.4.5 and Lemma 7.4.8]. Since G has finite coclass, there is a positive integer u such that $\gamma_i(G)/\gamma_{i+1}(G)$ has order p for all $i \geq u$. Now Coclass Theorem C (see Section 3.2 for the statement) shows that G is soluble, and so the last non-trivial term A of the derived series of $\gamma_u(G)$ is an open abelian normal subgroup of G. Let T be a maximal open abelian normal subgroup of G. The topological argument in [53, Lemma 7.2.2(v)] shows that T is finitely generated; hence the torsion subgroup $\widehat{T}$ of T is a finite normal subgroup of G. So by Lemma 3.11 we see that $\widehat{T}$ is trivial. This shows that T is a free $\mathbb{Z}_p$-module of finite rank. Let $C = C_G(T)$. Since T is an open normal subgroup, G/T is a finite p-group (see [23, Proposition 1.2]), hence the normal subgroup $C/T \trianglelefteq G/T$ intersects $Z(G/T)$ nontrivially (see [80, 5.2.1]). Thus, there exists $a \in C \setminus T$ with $aT \in Z(G/T)$; now $\langle T, a\rangle$ is an abelian normal open subgroup of G, contradicting the maximality of T. This proves that $C = T$, and T is self-centralising. Let U be any other open abelian normal subgroup of G. Then $U \cap T$ is open in T and hence contains p^kT for some k. Since T is self-centralising, G/T acts faithfully on T, and so also on $U \cap T$; recall that $p^kT \leq U \cap T$. If $u \in U$, then uT acts trivially on the abelian group $U \cap T$, and so $u \in T$ since G/T acts faithfully on $U \cap T$. This proves that $U \leq T$, and the uniqueness of T follows from the maximality. □

Lemma 3.13. *Let G be a pro-p-group of finite coclass r. If G has trivial centre, then G has an open normal subgroup $T \cong \mathbb{Z}_p^d$, where $d = (p-1)p^{s-1}$ where $1 \leq s \leq r$ for odd p and $1 \leq s \leq r+2$ for prime 2.*

Proof. We describe the proof as given in [53, Theorem 7.4.12]. From Lemma 3.12 we see that G contains an open normal self-centralising abelian subgroup T which is a free $\mathbb{Z}_p$-module of finite rank, say d; hence G/T acts faithfully on T. Let u be an integer such that $\gamma_i(G)/\gamma_{i+1}(G)$ has order p for all $i \geq u$. Then by definition, G acts uniserially on $\gamma_u(G)$ and hence acts on T by Lemma 3.11. For any group H we denote by $H^{[p]}$, the group generated by the p-th power of the elements in H. Note that, $G/\gamma_i(G)$ is a finite p-group of coclass r for all $i \geq u$, and so by applying [53, Theorems 6.3.8 and 6.3.9] for large j, there exists w such that if $j \geq w$ then $\gamma_j(G)^{[p]} = \gamma_{j+d}(G)$ and has index p^d in $\gamma_j(G)$ where $d = (p-1)p^{s-1}$ with $1 \leq s \leq r$ for odd p and $1 \leq s \leq r+2$ for prime 2. □

Lemma 3.13 gives rise to the important class of infinite pro-p-groups of coclass r with trivial centre. Such groups are called *uniserial p-adic space groups*. We discuss the structure of these groups in the subsequent sections.

3.1.2 Uniserial p-adic space groups

In this section we discuss some properties of uniserial p-adic space groups and how they are related to infinite pro-p-groups. The results in this section are based on [53, Section 7.4]. We note from [53, Lemma 10.4.1] that if $T = \mathbb{Z}_p^d$ then the uniserial series for T can be extended "to the left" as $\ldots \geq T_{-2} > T_{-1} > T_0 > T_1 > T_2 > \ldots$ where $T_{-i} = p^{-1}T_{-i+d} \leq \mathbb{Q}_p^d$ for all $i > 0$.

Definition 3.14. a) A p-adic pre-space group S of dimension d is an extension of a d-dimensional $\mathbb{Z}_p$-module T by a finite p-group P. If P acts faithfully on T then S is called a p-adic space group.

b) Let T be a normal subgroup in a p-adic pre-space group S. If T is maximal with respect to being open, abelian, torsion-free, and normal, then T is a translation subgroup of S with corresponding point group S/T.

c) A p-adic pre-space group S is called split if there is a translation subgroup T such that S is a split extension of T by a suitable point group; otherwise, S is called non-split.

d) A p-adic pre-space group S is uniserial if there exists a translation subgroup on which the corresponding point group acts uniserially. In addition, if the point group acts faithfully, then S is a uniserial p-adic space group.

We now give an example of a uniserial p-adic space group. Before providing the details, we briefly recall what a semidirect product of groups is. Given two groups N and H such that H acts on N via a group homomorphism $\phi : H \to \mathrm{Aut}(N)$, we can construct a new group $H \ltimes_\phi N$, called the (outer) semidirect product of N and H with respect to ϕ, whose underlying set is $H \times N$ and the group operation is defined as $(h_1, n_1)(h_2, n_2) = (h_1h_2, \phi(h_2)(n_1)n_2)$. If the action of H on N is clear from the context then we usually drop ϕ in the notation and simply write $H \ltimes N$. For the following example we take θ to be a primitive p^s-th root of unity over $\mathbb{Q}_p$ for some $s \geq 1$ so that the p^s-th local cyclotomic field is $\mathbb{Q}_p(\theta)$ and its valuation ring is defined as $\mathbb{Z}_p[\theta] = \{\sum_{i=0}^{d_s-1} a_i\theta^i \mid a_i \in \mathbb{Z}_p\}$ where $d_s = p^{s-1}(p-1)$, a detailed description of these structures are given in Section 4.1.2. The following is an illustration of [53, Example 7.4.14(ii)]. This will also serve as a standard example in later chapters.

Example 3.15. Let p be an odd prime, $s \geq 1$ and $T = (\mathbb{Z}_p[\theta], +)$. So T is a $\mathbb{Z}_p$-module of dimension $p^{s-1}(p-1)$. Let $\kappa = \theta - 1$ and denote by $\mathfrak{p}$ the ideal of $\mathbb{Z}_p[\theta]$ generated

by κ. Then $\mathfrak{p}$ is the unique maximal ideal of the principal ideal domain $\mathbb{Z}_p[\theta]$ and the residue class field $\mathbb{Z}_p[\theta]/\mathfrak{p}$ of $\mathbb{Q}_p(\theta)$ is isomorphic to $\mathbb{F}_p$, the field of order p. For $z \in \mathbb{N}$ define $\mathfrak{p}^z = \{\kappa^z t \mid t \in T\}$. Let P be a cyclic group of order p^s and generated by g. We define an action of P on T via multiplication by θ, that is, $t^{g^i} = \theta^i t$. Let $T_0 = T$ and following Definition 3.7 we have $T_1 = \langle -t + \theta t \mid t \in T \rangle = \mathfrak{p}$ and one can show by induction that $T_n = \mathfrak{p}^n$ for all $n \geq 1$. We note that $\mathfrak{p}^z/\mathfrak{p}^{z+1}$ and $T/\mathfrak{p}$ are both cyclic of order p for all $z \geq 1$ and hence they are isomorphic. Thus $|T : T_i| = p^i$ for all $i \geq 1$. This shows that the action of P on T is uniserial. Also, we find that if $t^{g^i} = t$ for all $t \in T$, in particular $1^{g^i} = 1$. Thus $\theta^i = 1$ which shows that $i \equiv 0 \bmod p^s$. So the action is also faithful. Hence $S = P \ltimes T$ is a uniserial p-adic space group.

We now state one of the central theorems on the structure of infinite pro-p-groups, see [23, Theorem 10.1] and [53, Theorem 7.4.12].

Theorem 3.16. *Let G be an infinite pro-p-group of coclass r which has trivial centre. Then G is a uniserial p-adic space group which has an open normal subgroup $T \cong \mathbb{Z}_p^d$, where $d = (p-1)p^{s-1}$ with $1 \leq s \leq r$ for odd p and $1 \leq s \leq r+2$ for prime 2. Moreover, G/T has coclass r.*

The proof of Theorem 3.16 can be found in [53, Section 7.4] and [23, Chapter 10]. Here we briefly discuss the proof using Lemmas 3.12 and 3.13. We can now complete the proof of Theorem 3.16.

Proof of Theorem 3.16. By Lemma 3.11, we see that G has a finite hypercentre H and G/H is a pro-p-group with trivial centre and of coclass less than r. Lemma 3.13 shows that G/H has an open normal subgroup $\tilde{T}$ which satisfies the conditions listed in the theorem. Let u be an integer such that $\gamma_i(G)/\gamma_{i+1}(G)$ has order p for all $i \geq u$. Then the pre-image in G of $\tilde{T}$ contains $T = \tilde{T} \cap \gamma_u(G)$ and from the proof of Lemma 3.11 we see that T is a free uniserial $\mathbb{Z}_p P$-module of dimension d. □

The following result, which is an easy corollary of Theorem 3.16 and Lemma 3.13, summarises the relation between the uniserial p-adic (pre)space groups and infinite pro-p-groups, see [53, Theorem 7.4.12] and [53, Corollary 7.4.13] also for details.

Corollary 3.17. *Every infinite pro-p-group G of finite coclass r is a uniserial p-adic pre-space group of dimension $d_s = (p-1)p^{s-1}$ where $1 \leq s \leq r$ for odd p and $1 \leq s \leq r+2$ for prime 2. If G has trivial hypercentre, then G is a uniserial p-adic space group.*

In general a translation subgroup and the corresponding point group is not unique for a pre-space group. However, the uniqueness holds for uniserial space groups. This follows from Lemma 3.12 and Corollary 3.17. Thus we have the following, see [53, Lemma 7.4.8] for details.

Lemma 3.18. *Every uniserial p-adic space group has a unique characteristic translation subgroup and so each term of its uniserial series is also characteristic.*

Notation 3.19. Unless mentioned otherwise, for the rest of the chapter, we will abbreviate "uniserial p-adic (pre)space group" by "p-adic (pre)space group" or simply "(pre)space group" if the prime p is clear from context.

A large amount of research, for example [30, 51, 52, 60], has contributed towards the determination of the structure of these space groups. A systematic description of these results is given in [53, Chapters 7 and 10]. We provide some of those structural results in the following sections. By definition, every space group is an extension of its translation subgroup by its point group. We discuss these point groups in Section 3.1.3. Coclass of a space group will be discussed in Section 3.1.4. It is an important result that every non-split space group can be embedded into some split space group. We discuss these in Section 3.1.5. This discussion will also prepare the background for Chapter 7 where we will provide a constructive classification of uniserial 2-adic space groups.

3.1.3 Point groups

The aim of this section is to give an overview of the construction of possible point groups for a space group. Results of this section are mainly from [53, Chapters 2, 4 and 10]. For a group H and a non-empty set Ω, the multiplicative group H^Ω is defined as the set of maps from Ω to H with pointwise multiplication $f_1 f_2(\omega) = f_1(\omega) f_2(\omega)$ for all $f_1, f_2 \in H^\Omega$ and $\omega \in \Omega$.

Definition 3.20. Let H be a group, and let G be a finite group acting on a non-empty finite ordered set $\Omega = (\omega_1, \ldots, \omega_m)$. For $g \in G$ and $f = (f(\omega_1), \ldots, f(\omega_m)) \in H^\Omega$, define $f^g \in H^\Omega$ by $f^g(\omega) = (f(\omega_1^{g^{-1}}), \ldots, f(\omega_m^{g^{-1}}))$ for all $\omega \in \Omega$. Given Ω, the (permutational) wreath product $H \wr G$ is defined as the split extension $G \ltimes H^\Omega$. The subgroup H^Ω of $H \wr G$ is the base group of the wreath product and can be identified with the direct product of $|\Omega|$ copies of H.

Remark 3.21. We consider Definition 3.20 in the case when G is isomorphic to the cyclic group C_{p^s} of order p^s. In this case we take the regular (permutation) representation of C_{p^s}, or equivalently assume that the fixed generator of G acts on the set $\Omega = \{1, \ldots, p^s\}$ as the p^s-cycle $(1, 2, \ldots, p^s)$. As a result, for a finite group H, the wreath product $C_{p^s} \wr H$ can then be formed according to Definition 3.20. The base group of $C_{p^s} \wr H$ will be the p^s-fold direct product of H.

Notation 3.22. For the rest of this chapter we fix an odd prime p and write

$$d_s = p^{s-1}(p-1).$$

The point groups of a space group have a well-understood structure and it follows from [53, Section 10.2] that, up to conjugacy in $\mathrm{GL}(d_s, \mathbb{Q}_p)$, the possible point groups in dimension d_s can be realised as subgroups of $\mathrm{GL}(d_s, \mathbb{Z}_p)$. For odd primes, it can further be shown that up to conjugacy in $\mathrm{GL}(d_s, \mathbb{Q}_p)$ it is enough to consider subgroups of $\mathrm{GL}(d_s, \mathbb{Z})$. These kind of point groups are called rational point groups. For $p = 2$ and $s > 1$, the situation is more complicated: in addition to the rational point groups, there are point groups which are subgroups of $\mathrm{GL}(2^s, \mathbb{Q}_2)$ but not of $\mathrm{GL}(2^s, \mathbb{Q})$, and these point groups cannot be conjugated into $\mathrm{GL}(2^s, \mathbb{Q})$. It is known these point groups are isomorphic to certain subgroups of the iterated wreath product of Q_{16} and $s-2$ copies of C_2, where Q_{16} is the generalised quaternion group of order 16.

The above discussion shows that there is a significant difference between odd primes and prime 2 for constructing space groups. For odd primes, Eick [30] has given a constructive classification of uniserial p-adic space groups. The case $p = 2$ remained mostly open. We will investigate this case in Chapter 7 and will provide the theoretical description needed for the required constructive classification.

For odd p, we know from [53, Section 10.2] that the point groups of p-adic space groups of dimension d_s can be represented by some subgroups of $W(s,p)$ where $W(1,p)$ is a cyclic subgroup of $\mathrm{GL}(p-1,\mathbb{Z})$ and $W(s,p) = W(s-1,p) \wr \langle M_s \rangle$ for some cyclic subgroup $M_s \leq \mathrm{GL}(d_s, \mathbb{Z}_p)$ for $s \geq 2$.

Definition 3.23. The cyclic group $W(1,p) \leq \mathrm{GL}(p-1,\mathbb{Z})$ is generated by the matrix

$$A_1 = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 \\ -1 & -1 & -1 & \dots & -1 \end{pmatrix}$$

and for $s \geq 2$, the group $W(s,p) \leq \mathrm{GL}(d_s, \mathbb{Z})$ is generated by the matrices in the set $\{M_s\} \cup \{A^* \mid A \in W(s-1,p)\}$ where

$$M_s = \begin{pmatrix} 0 & I & 0 & \dots & 0 \\ 0 & 0 & I & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & I \\ I & 0 & 0 & \dots & 0 \end{pmatrix} \quad \text{and} \quad A^* = \begin{pmatrix} A & 0 & 0 & \dots & 0 \\ 0 & I & 0 & \dots & 0 \\ 0 & 0 & I & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & I \end{pmatrix}.$$

with I and 0 being the identity and zero matrices, respectively, of dimension d_{s-1}.

For the purpose of constructing point groups, an alternative definition of $W(s,p)$ is given in [30] for odd p; the following is shown in [30, Theorem 17].

Theorem 3.24. *Let $U \in \mathrm{GL}(d_s, \mathbb{Z}_p)$ be a point group of a uniserial p-adic space group. If p is odd then U is conjugate in $\mathrm{GL}(d_s, \mathbb{Q}_p)$ to a subgroup of $W(s,p) \leq \mathrm{GL}(d_s, \mathbb{Z})$.*

The statement of Theorem 3.24 is not true for $p = 2$. We consider this case in Section 7.4.

3.1.4 Coclass of space groups

The results mentioned in this section can be found in [53, Section 10.5]. Recall that the p-adic valuation $\nu_p : \mathbb{Q} \to \mathbb{Z} \cup \{\infty\}$ can be defined by $\nu_p(0) = \infty$ and, for $x \neq 0$, by the formula

$$x = p^{\nu_p(x)} \frac{a}{b}, \quad p \nmid ab \text{ for some } a, b \in \mathbb{Z},$$

see Section 4.1 for further details. The following result describes the coclass of a space group, see [30, Theorem 1] for details.

Theorem 3.25. *Let G be a p-adic space group with point group P and p odd. Then $s \leq \mathrm{cc}(G) \leq p^{s-1} + \ldots + p + 1$ and the dimension of G is at most $(p-1)p^{\mathrm{cc}(G)-1}$. If G is split then the coclass of G is $\nu_p(|P|)$.*

We conclude this section by giving an example of a space group of finite coclass.

Example 3.26. Let p be an odd prime. We show that the space group S obtained in Example 3.15 is of finite coclass. We retain the notations used in Example 3.15 and take $\gamma_1(S) = S$. We now calculate $\gamma_2(S)$. An arbitrary generator of $\gamma_2(S)$ is given by $(g^i, x)^{-1}(g^j, y)^{-1}(g^i, x)(g^j, y)$ where $x, y \in T$ and $i, j \in \mathbb{Z}$. A technical but straightforward calculation shows that $\gamma_2(S)$ is generated by $\{(1, \kappa t) \mid t \in T\}$. By induction we can prove that $\gamma_n(S)$ is generated by $\{(1, \kappa^{n-1} t) \mid t \in T\}$ for any $n \geq 2$. Thus the terms of the lower central series of S are given by $\gamma_1(S) = S$ and $\gamma_i(S) = \mathfrak{p}^{i-1}$ for all $i \geq 2$. It is easy to see that $S/\kappa T \cong P \ltimes T/\kappa T$. Hence we deduce that $|S/\kappa T| = p^{s+1}$. This shows that $S/\gamma_2(S)$ is a group of finite coclass. Finally, $|\gamma_i(S)/\gamma_{i+1}(S)| = |\mathfrak{p}^{i-1}/\mathfrak{p}^i| = p$ for all $i \geq 2$. We conclude that S has finite coclass.

3.1.5 Embedding

It is an important result that any non-split (pre)space group can be embedded into some split (pre)space group. In this section we discuss this and some related results. The content of this section is from [53, Section 10.4]. We begin with an example of a non-split space group.

Example 3.27. This is discussed in [34, p. 1250]. Let $K = \mathbb{Q}_3(\theta)$ be the ninth cyclotomic number field where θ is a primitive ninth root of unity. Write $T = (\mathbb{Z}_3[\theta], +)$ which is a $\mathbb{Z}_3$-module of rank 6 generated by $1, \theta, \ldots, \theta^5$. Let W be the group of order 81 generated by the permutations $a = (1, \theta, \ldots, \theta^8)$ and $y = (1, \theta^3, \theta^6)$. The action of W on T is understood from the permutational structure of the elements of W. A straightforward calculation shows that the action is faithful and uniserial with the uniserial series $T > \mathfrak{p}^1 > \mathfrak{p}^2 > \ldots$ where $\mathfrak{p}^n = (\theta - 1)^n T$. Let $b = (\theta, \theta^4, \theta^7)(\theta^2, \theta^8, \theta^5) \in W$. Hence $D = \langle a, b \rangle$ and T both can be regarded as subgroups of $W \ltimes T$. Let $S = \langle a, b(\theta - 1) \rangle$. Clearly $\mathfrak{p}$ is the kernel of the natural map from S onto D and hence S is a uniserial 3-adic space group which is not a split extension of T by D. Then S can be embedded into the split-space group $D \ltimes \mathfrak{p} = \langle a, b, (\theta - 1) \rangle$.

Recall that if $T \cong \mathbb{Z}_p^d$ is a translation subgroup of a space group then the terms of uniserial series for T are given by T_i for all $i \in \mathbb{Z}$ with $T_{-i} = p^{-1}T_{-i+d} \leq \mathbb{Q}_p^d$ for all $i > 0$. If P is a point group of a pre-space group with a translation subgroup T then the action of P on T can be extended to an action on $p^{-i}T$ for all $i \geq 0$.

Theorem 3.28. *Let G be a p-adic pre-space group with a translation subgroup T and corresponding point group P. Then there exists a smallest integer $i \geq 0$ such that G embeds into the split extension G^* of T_{-i} by P with $G^* \cap T_{-i} = T$.*

The group G^* in Theorem 3.28 is called the *minimal super-split pre-space group* of G corresponding to T. This group will play an important role in Chapters 4 and 5.

3.2 The Coclass Theorems

We first state the Coclass Theorems by sorting them in order of strength, that means, Coclass Theorem B can be deduced from Coclass Theorem A and so on. The discussion in this section is motivated from [36, Section 2.3]. We start with Coclass Theorem E, which was the first one to be proved.

Coclass Theorem E. *Given p and r, there are only finitely many isomorphism types of infinite soluble pro-p-groups of coclass r.*

Coclass Theorem E was first proved by Leedham-Green, McKay and Plesken in [54] for odd primes and in [55] for $p = 2$.

The next in strength are Coclass Theorems D and C.

Coclass Theorem D. *Given p and r, there are only finitely many isomorphism types of infinite pro-p-groups of coclass r.*

Coclass Theorem C. *Every pro-p-group of finite coclass is soluble.*

Coclass Theorem C was first proved in 1987 by Donkin [24] for $p > 3$. His proof uses results related to the automorphism group of a simple Lie algebra over a local field. Later Shalev and Zel'manov [82] provided a proof that is valid for all primes.

Coclass Theorem B. *There is an integer $g = g(p, r)$ such that every p-group of coclass r has soluble length at most g.*

For a proof of Coclass Theorem B (by Leedham-Green) see [53, Corollary 6.4.6]. The function $g(p, r)$ mentioned in Coclass Theorem B turned out to be $4+\log_2((p-1)p^{r-1}-1)$ for odd p and $r + 4$ for $p = 2$. The strongest one is Coclass Theorem A.

Coclass Theorem A. *There is an integer $f = f(p, r)$ such that every p-group of coclass r has a normal subgroup of class 2 with index at most p^f.*

The proof of Coclass Theorem A (see [53, Theorem 6.4.3 and Theorem 6.4.5]) is one of the major achievements in the coclass theory and numerous papers are contributed to the ultimate proof. We mention a few highlights from [23, p. 265]. We also refer to [53] and [17, Appendix A.2] for background and further references. Theorem A was first proved by Leedham-Green, see [52], though only for $p > 3$. This proof relies on Donkin's proof of Coclass Theorem C for $p > 3$. Later Shalev and Zel'manov [82] gave a self-contained proof, for all primes, of the results used in Donkin's proof for Theorem C. Afterwards Shalev gave an independent proof of Coclass Theorem A in [83] which is valid for all primes. We note that Leedham-Green's proof uses the concept of uniserial action and the application of Lie methods, whereas Shalev's proof uses the theory of Lie algebras. An interesting read in this context is the *featured online review* of these two papers written by Mann [63]. The function $f(p, r)$ mentioned in Coclass Theorem A turned out to be $p^{2(p-1)p^{r-1}+r-3}$ for odd p and $2^{3.2^{r+1}+r-2}$ if $p = 2$.

We conclude this section by recalling some brief proofs of Coclass Theorems B–E as consequences of *stronger* Coclass Theorems. Recall that a group G is soluble if the derived series $G \geq G^{(1)} \geq G^{(2)} \geq \ldots$ eventually reaches the trivial subgroup of G where we define $G^{(0)} = G$ and $G^{(i)} = [G^{(i-1)}, G^{(i-1)}]$.

Proof of Theorem B. Let G be a p-group of coclass r. Note that $G^{(i)} \leq \gamma_{2^i}(G)$. Now it follows from the proof of Theorem A, see [53, Section 6.4], that G has derived length at most $i + 2$ if $2^i \geq 2(p-1)p^{r-1} - 2$ for odd p, and if $2^{i+1} \geq 3 \cdot 2^{r+1} - 1$ for $p = 2$. □

Proof of Theorem C. Let G be a pro-p-group of coclass r. Then by definition $G/\gamma_i(G)$ is a finite p-group of coclass at most r for all $i > 1$. By Theorem B we have $G/\gamma_i(G)$ is

soluble of length at most g where g only depends on p and r and hence independent of i. Thus from the proof of Lemma 3.9, we get $G^{(g)} < \bigcap_i \gamma_i(G) = 1$ and so G is soluble. □

Proof of Theorem D. We note from Theorem 3.16 that an infinite pro-p-group G of coclass r has an open normal subgroup $A \cong \mathbb{Z}_p^k$, where $k = (p-1)p^s$ for some $s < r$ if p is odd, $k = 2^s$ for some $s < r+1$ if $p = 2$. Moreover, see [23, Theorem 10.1] we deduce that G/A has coclass r and $[G : A] = p^{r+p^r}$ if p is odd, and $[G : A] = 2^{r+(r+1)^{2^{r+1}}}$ if $p = 2$. As shown in [23, Section 10.4], the proof of this assertion relies on Theorem C. Finally from [23, Theorem 5.8], there are only finitely many isomorphism types of extensions of the pro-p-group $\mathbb{Z}_p^k$ by a finite p-group. □

Theorem E is a direct consequence of Theorem D.

Chapter 4

Skeleton Groups

We have seen in Section 2.2 that large parts of coclass graphs exhibit periodic patterns and it is conjectured that these patterns are sufficient to reconstruct the coclass graph from a finite subgraph. Theorems 2.2 and 3.5 explain that it is sufficient to study this conjecture for coclass trees. Many deep and rich results have been proved for these coclass trees; the book [53] has a detailed description and references. A brief summary of known periodicity results is also given in [20, Appendix A.2]. However, there are still many open questions related to the structure of coclass trees; see Section 2.2 for a detailed discussion. An unfortunate characteristic of previous work on $\mathcal{G}(p,r)$ is that proofs often become quite technical, frequently involving p-adic number theory. It has also become apparent that a more feasible approach for investigating $\mathcal{G}(p,r)$ is to first focus skeleton groups for reasons explained below.

While the precise structure of the groups in a coclass tree $\mathcal{T}$ is very intricate, skeleton groups are notable exceptions: these groups can informally be described as twisted finite quotients of the space group associated with $\mathcal{T}$; the twisting is induced by certain $\mathbb{Z}_pP$-module homomorphisms where P is the point group of the space group associated with $\mathcal{T}$. We show in Theorem 4.19 that almost every group in $\mathcal{T}$ has bounded distance to such a skeleton group. This justifies saying that these groups indeed form the 'skeleton' of $\mathcal{G}(p,r)$ and hence the structure of $\mathcal{G}(p,r)$ is mostly determined by the subtree(s) induced by all skeleton groups. In conclusion, we will see that skeleton groups not only have a direct and a well-understood construction, conveniently parametrised by certain $\mathbb{Z}_pP$-homomorphisms, they also determine the broad structure of the graph $\mathcal{G}(p,r)$. This makes them an interesting and important object to study in coclass theory.

In this chapter we introduce the systematic treatment of skeleton groups. Our work is based on the technical definition of "constructible groups" given in [53, Definition 8.4.9]. Some variations have been studied for special cases in [18–20, 34], but with a very

succinct discussion and proof. Motivated by previous work, we elaborate a less technical definition and prove that skeleton groups are same as the groups defined in [53]; we give definitions and proofs in Section 4.4. Some results of this chapter are published in [22].

Notation 4.1. Throughout this chapter let G be a uniserial p-adic space group of dimension d and coclass r, with point group P, translation subgroup T, and extended uniserial series $\ldots > T_{-1} > T_0 = T > T_1 > \ldots$. In this chapter, from Section 4.3 onwards, we assume that p is an odd prime.

4.1 Some number theory

The aim of this section is to briefly recall the number theory required for this chapter. These results are standard and can be found in [42, 45, 69, 70].

4.1.1 p-adic numbers

The p-adic valuation of $\mathbb{Q}$ is the map $\nu_p : \mathbb{Q} \to \mathbb{Z} \cup \{\infty\}$ which is defined as follows.

$$\nu_p(n) = \begin{cases} v & \text{if } n \in \mathbb{Z} \setminus \{0\} \text{ and } p^v \mid n \text{ but } p^{v+1} \nmid n \\ \nu_p(a) - \nu_p(b) & \text{if } n = \frac{a}{b} \in \mathbb{Q} \text{ where } a, b \in \mathbb{Z} \setminus \{0\} \\ \infty & \text{if } n = 0. \end{cases}$$

In fact, recall from Section 3.1.4 that the p-adic valuation $\nu_p : \mathbb{Q} \to \mathbb{Z} \cup \{\infty\}$ can be defined by $\nu_p(0) = \infty$ and, for $x \neq 0$, by the formula

$$x = p^{\nu_p(x)} \frac{a}{b}, \quad p \nmid ab \text{ for some } a, b \in \mathbb{Z}.$$

The above definition produces a p-adic absolute value $|\cdot|_p$ on $\mathbb{Q}$ which is defined by $|x|_p = p^{-\nu_p(x)}$ if $x \neq 0$ and $|0|_p = 0$. The field of p-adic numbers $\mathbb{Q}_p$ is defined as the completion of $\mathbb{Q}$ under the p-adic absolute value. We note that $\mathbb{Q}_p$ consists of equivalence classes of Cauchy sequences. The following description is given from [42, Chapter 3]. Let us define

$$\mathcal{C}_p(\mathbb{Q}) = \{(x_n)_{n\in\mathbb{N}} \mid (x_n)_{n\in\mathbb{N}} \text{ Cauchy sequence in } \mathbb{Q} \text{ with respect to } |\cdot|_p\}$$

and

$$\mathcal{N}_p(\mathbb{Q}) = \{(x_n)_{n\in\mathbb{N}} \in \mathcal{C}_p(\mathbb{Q}) \mid \lim_{n\to\infty} |x_n|_p = 0\}.$$

It can be shown that $\mathcal{N}_p(\mathbb{Q})$ is a maximal ideal of $\mathcal{C}_p(\mathbb{Q})$ and the field of p-adic numbers can be defined by the quotient

$$\mathbb{Q}_p = \mathcal{C}_p(\mathbb{Q})/\mathcal{N}_p(\mathbb{Q}).$$

The p-adic absolute value can be extended to $\mathbb{Q}_p$ via $|x|_p = \lim_{n\to\infty} |x_n|_p$ where $(x_n)_{n\in\mathbb{N}}$ is a Cauchy sequence in $\mathbb{Q}_p$ representing x. It can also be shown that $\mathbb{Q}_p$ is complete with respect to $|\cdot|_p$. Every $x \in \mathbb{Q}_p$ can uniquely be written as

$$x = \sum_{n\geq n_0} b_n p^n, \quad b_n \in \{0, \ldots, p-1\} \text{ and } n_0 = \nu_p(x).$$

The ring of p-adic integers $\mathbb{Z}_p$ is the valuation ring $\{x \in \mathbb{Q}_p \mid |x|_p \leq 1\}$ and can be regarded as

$$\mathbb{Z}_p = \{\sum_{i=0}^{\infty} a_i p^i \mid 0 \leq a_i \leq p-1,\ a_i \in \mathbb{N}\}.$$

Note that

$$\mathbb{Q} \cap \mathbb{Z}_p = \{\frac{a}{b} \in \mathbb{Q} \mid p \nmid b\}$$

and for each $n \in \mathbb{N}$ we have $\mathbb{Z}_p/p^n\mathbb{Z}_p \cong \mathbb{Z}/p^n\mathbb{Z}$.

The group of p-adic units consists of the elements in $\mathbb{Z}_p$ which are invertible in $\mathbb{Z}_p$ and equals $\mathbb{Z}_p^\star = \{x \in \mathbb{Q}_p \mid |x|_p = 1\}$; we have $\mathbb{Q} \cap \mathbb{Z}_p^\star = \{a/b \in \mathbb{Q} \mid p \nmid ab\}$.

Using Hensel's Lemma, see [42, Section 3.3], it can be deduced that the only roots of unity in $\mathbb{Q}_2$ are $\{1, -1\}$; moreover if p is odd then the $(p-1)$-th roots of unity are contained in $\mathbb{Q}_p$, and these are the only roots of unity.

4.1.2 Cyclotomic fields

We refer to [69, Section II, Chapters 5 and 7] for the results mentioned in this section.

Let θ be a primitive p^s-th root of unity over $\mathbb{Q}_p$ for some $s \geq 1$. The p^s-th local cyclotomic field is defined as $\mathbb{Q}_p(\theta)$, that is,

$$\mathbb{Q}_p(\theta) \cong \mathbb{Q}_p[X]/(1 + X + \ldots + X^{p^s-1})\mathbb{Q}[X].$$

The field extension $\mathbb{Q}_p(\theta)/\mathbb{Q}_p$ is of degree $d_s = p^{s-1}(p-1)$ and $\mathbb{Q}_p(\theta)$ has a $\mathbb{Q}_p$-basis $\{1, \theta, \ldots, \theta^{d_s-1}\}$.

The p-adic absolute value on $\mathbb{Q}_p$ extends to $\mathbb{Q}_p(\theta)$ and, with respect to this absolute value, $\mathbb{Q}_p(\theta)$ is complete. The valuation ring of $\mathbb{Q}_p(\theta)$ is $\{x \in \mathbb{Q}_p(\theta) \mid |x|_p \leq 1\}$ and

equals

$$\mathbb{Z}_p[\theta] = \{\sum_{i=0}^{d_s-1} a_i\theta^i \mid a_i \in \mathbb{Z}_p\}.$$

The invertible elements in $\mathbb{Z}_p[\theta]$ are $\{x \in \mathbb{Q}_p(\theta) \mid |x|_p = 1\}$; we denote this group of units by

$$\mathcal{U}_{p^s} = (\mathbb{Z}_p[\theta]^\star, \cdot).$$

The element

$$\kappa = \theta - 1$$

is a prime in $\mathbb{Q}_p(\theta)$ and generates the unique maximal ideal

$$\mathfrak{p} = \{x \in \mathbb{Q}_p(\theta) \mid |x|_p < 1\}$$

in the principal ideal domain $\mathbb{Z}_p[\theta]$. For any $z \in \mathbb{Z}$ we define $\mathfrak{p}^z = \{\kappa^z t \mid t \in \mathbb{Z}_p[\theta]\}$. The ideals $\mathfrak{p}^0, \mathfrak{p}^1, \mathfrak{p}^2, \ldots$ are all the non-zero ideals of $\mathbb{Z}_p[\theta]$, and each quotient $\mathfrak{p}^j/\mathfrak{p}^{j+1}$ is isomorphic to $\mathbb{Z}/p\mathbb{Z}$.

The Galois group

$$G_\theta = \{\alpha \in \mathrm{Aut}(\mathbb{Q}_p(\theta)) \mid \alpha(x) = x \text{ for all } x \in \mathbb{Q}_p\}$$

is cyclic of order d_s and generated by an automorphism defined by $\theta \mapsto \theta^k$ for some primitive root $k \in \{2, \ldots p^s - 1\}$ modulo p^s. For any such k, the Galois automorphism defined by $\theta \mapsto \theta^k$ is denoted by σ_k.

We now recall the structure of the group of units $\mathcal{U}_{p^s}$. If $\omega \in \mathbb{Z}_p$ is a primitive $(p-1)$-th root of unity, then

$$\mathcal{U}_{p^s} = \langle\omega\rangle \times (1 + \mathfrak{p});$$

every $u \in \mathcal{U}_{p^s}$ can be written uniquely as $u = \omega^a(1+t)$ with $a \in \{0, \ldots, p-2\}$ and $t \in \mathfrak{p}$.

The group of i-th one-units with $i \geq 1$ is defined as $\mathcal{U}_{p^s}^{(i)} = 1 + \mathfrak{p}^i$.

4.2 Exterior square

Let V be the $\mathbb{Z}_p$-submodule of $T \otimes T$ generated by $\{a \otimes a \mid a \in T\}$ where T is a $\mathbb{Z}_p$-module. The exterior square of T is

$$T \wedge T = (T \otimes T)/V,$$

which is the $\mathbb{Z}_p$-module generated by the symbols $s \wedge t$ with $s, t \in T$ subject to the relations $(zs) \wedge t = s \wedge (zt) = z(s \wedge t)$, $(s+t) \wedge u = (s \wedge u) + (t \wedge u)$ and $s \wedge t = -(t \wedge s)$ for

all $s, t, u \in T$ and $z \in \mathbb{Z}_p$. We consider $T \wedge T$ as a $\mathbb{Z}_pP$-module where P acts diagonally on $T \wedge T$, and write $T_i \wedge T$ for the $\mathbb{Z}_pP$-submodule of $T \wedge T$ generated by all $s \wedge t$ with $s \in T_i$ and $t \in T$.

4.3 Twisted groups

In the following, let $\gamma : T \wedge T \to T$ be a $\mathbb{Z}_pP$-module homomorphism. Recall that T has $\mathbb{Z}_p$-rank d.

Lemma 4.2. *There exists $0 \leq j \leq k$ such that $\gamma(T \wedge T) = T_j$ and $\gamma(T_j \wedge T) = T_k$; in particular, $k \geq 2j - d$.*

Proof. Since γ is a $\mathbb{Z}_pP$-homomorphism, for any $a, b \in T$ and $g \in P$ we have that $\gamma(a \wedge b)^g = \gamma(a^g \wedge b^g) \in \gamma(T \wedge T)$. This shows that $\gamma(T \wedge T)$ is a P-invariant subgroup of T, hence by Lemma 3.8 we have $\gamma(T \wedge T) = T_j$ for some $j \geq 0$. By a similar argument we can show $\gamma(T_j \wedge T) = T_k$ for some $k \geq 0$. Clearly $k \geq j$ since $T_k = \gamma(T_j \wedge T) \subseteq \gamma(T \wedge T) = T_j$. For the last claim, write $T_j = p^y T_i$ with $0 \leq i \leq d - 1$ and note that $\gamma(T_j \wedge T) \leq p^y T_j \leq T_{2j-d}$. □

We now assume that

$$\gamma(T \wedge T) = T_j \quad \text{and} \quad \gamma(T_j \wedge T) = T_k.$$

If $m \in \{j, j + 1, \ldots, 2j - d\}$, then $T_k \leq T_m \leq T_j$, and so γ induces a well-defined surjective P-homomorphism $(T/T_j) \wedge (T/T_j) \to T_j/T_m$ which maps $(a + T_j \wedge b + T_j)$ to $\gamma(a \wedge b) + T_m$. For remainder of the chapter, let us fix these j, k and m.

The definition of $T_{\gamma,m}$ in the following proposition depends on the fact that p is odd, hence 2 is invertible in $\mathbb{Z}_p$.

Proposition 4.3. *Let $T_{\gamma,m} = (T/T_m, \circ_\gamma)$ where*

$$(a + T_m) \circ_\gamma (a + T_m) = a + b + \tfrac{1}{2}\gamma(a \wedge b) + T_m.$$

Then $T_{\gamma,m}$ is a group of order p^m with central derived subgroup T_j/T_m.

Proof. Since, $T_m \subseteq T_j$ and $\gamma(T_j \wedge T) = T_k \subseteq T_m$, the operation $\circ_\gamma$ is well defined. We now show that $T_{\gamma,m}$ is a group. Clearly $0 + T_m$ is the identity and $-a + T_m$ is the inverse

of $a + T_m$ for any $a \in T$. To show associativity, we note that $T_k \leq T_m$ and if $a, b, c \in T$ then

$$\begin{aligned} & ((a + T_m) \circ_\gamma (b + T_m)) \circ_\gamma (c + T_m) \\ = \; & ((a + b + \tfrac{1}{2}\gamma(a \wedge b)) + T_m) \circ (c + T_m) \\ = \; & (a + b + \tfrac{1}{2}\gamma(a \wedge b) + c + \tfrac{1}{2}\gamma((a + b + \tfrac{1}{2}\gamma(a \wedge b)) \wedge c)) + T_m \\ = \; & a + b + c + \tfrac{1}{2}\gamma(a \wedge b) + \tfrac{1}{2}\gamma((a + b) \wedge c) + T_m \\ = \; & a + b + c + \tfrac{1}{2}(\gamma(a \wedge b) + \gamma(a \wedge c) + \gamma(b \wedge c)) + T_m. \end{aligned}$$

Similarly we can show that

$$(a + T_m) \circ_\gamma ((b + T_m) \circ_\gamma (c + T_m)) = a + b + c + \tfrac{1}{2}(\gamma(b \wedge c) + \gamma(a \wedge b) + \gamma(a \wedge c)) + T_m.$$

Clearly $T_{\gamma,m}$ has order p^m and if $a, b \in T$ then

$$\begin{aligned} & [a + T_m, b + T_m] \\ = \; & (-a + T_m) \circ_\gamma (-b + T_m) \circ_\gamma (a + T_m) \circ_\gamma (b + T_m) \\ = \; & ((-a - b + \tfrac{1}{2}\gamma(-a \wedge -b)) + T_m) \circ_\gamma ((a + b + \tfrac{1}{2}\gamma(a \wedge b)) + T_m) \\ = \; & \gamma(a \wedge b) + T_m. \end{aligned}$$

Since the derived subgroup $T'_{\gamma,m}$ is generated by all such commutators and γ has image T_j, we deduce $T'_{\gamma,m} = T_j/T_m$. If $a \in T$ and $b \in T_j$, then $[a+T_m, b+T_m] = \gamma(a \wedge b) + T_m = 0 + T_m$, so T_j/T_m is central in $T_{\gamma,m}$. □

4.4 Skeleton groups

We continue using Notation 4.1 and assume that p is odd. Moreover, when considering a *twisted group* $T_{\gamma,m}$, we implicitly assume that all parameters are chosen appropriately, that is, if $\gamma(T \wedge T) = T_j$ and $\gamma(T_j \wedge T) = T_k$, then $j \leq m \leq 2j - d$.

4.4.1 The split case

We first consider the case when $G = P \ltimes T$ is split since this allows a direct construction. We consider a $\mathbb{Z}_p P$-homomorphism $\gamma : T \wedge T \to T$ and the associated twisted group

$$T_{\gamma,m} = (T/T_m, \circ_\gamma).$$

Since γ is a $\mathbb{Z}_p P$-homomorphism, we can now make the following definition.

Definition 4.4. Let $\gamma\colon T \wedge T \to T_j$ be a surjective $\mathbb{Z}_pP$-homomorphism and choose m such that $j \leq m \leq 2j - d$. The skeleton group defined by γ and m is

$$G_{\gamma,m} = P \ltimes T_{\gamma,m}$$

with multiplication $(g, a + T_m)(h, b + T_m) = (gh, a^h + b + \frac{1}{2}\gamma(a^h \wedge b) + T_m)$.

The definition of $G_{\gamma,m}$ depends on the choice of the translation subgroup, which is implicitly encoded in γ, but it is independent of the chosen complement P.

4.4.2 The general case

Now we consider the general case, that is, the extension G of P by T is not necessarily split. The approach here is to embed G into some split pro-p-group G^*, to construct skeleton groups for G^* as in Section 4.4.1, and then to translate these groups back to groups defined over G. We describe these three steps in the following.

(1) By Theorem 3.28, there exists a smallest integer $x \geq 0$ such that if $T^* = p^{-x}T$, then G can be embedded into the pro-p-group $G^* = GT^*$, where $G \cap T^* = T$ and G^* is a split extension of T^* by P. We note that G has coclass r. Now $x \leq r$ follows from Lemma 3.17 and Section 3.1.5, cf. the proof of [53, Theorem 11.3.9]. To abbreviate notation, for an integer j it will be convenient to define

$$j^* = j - 2xd; \tag{4.1}$$

recall that d is the dimension of G. In the following we write

$$G = P.T = \{(g, t) \mid g \in P, t \in T\} \quad \text{and} \quad G^* = P.T^* = \{(g, t) \mid g \in P, t \in T^*\}$$

for the underlying sets of G and G^*, respectively, so that the embedding given by $\phi\colon G \hookrightarrow G^*$ maps (g, t) to (g, t). Let P^* be a complement to T^* in G^*; since $P^* \subseteq P.T^*$, write

$$P^* = \{h_g \mid g \in P\} \quad \text{where each} \quad h_g = (g, t_g) \in P.T^*.$$

(2) Let $\gamma : T \wedge T \to T_j$ be a surjective $\mathbb{Z}_pP$-homomorphism with $\gamma(T_j \wedge T) = T_k$ and $j \geq 2xd$; recall that $k \geq 2j - d$. Multiplication by p^{-x} translates γ to a surjective $\mathbb{Z}_pP$-homomorphism $T^* \wedge T^* \to T_{j^*}$, which, by abuse of notation, is also denoted by γ. If m satisfies $j^* \leq m \leq 2j^* + (x - 1)d$, then $\gamma(T_{j^*} \wedge T^*) \leq T_m$, and we can

define the skeleton group $G^*_{\gamma,m}$ as in Section 4.4.1 by

$$G^*_{\gamma,m} = P^* \ltimes T^*_{\gamma,m}.$$

(3) Note that T_{j^*}/T_m is a normal subgroup of $G^*_{\gamma,m}$ with quotient group G^*/T_{j^*}; denote by π the associated natural projection. We now define $G_{P^*,\gamma,m}$ to be the full preimage under π of the embedding of G/T_{j^*} into G^*/T_{j^*} via ϕ.

Proposition 4.5. *Writing the elements of $P^* \ltimes T^*_{\gamma,m}$ as $(h_g, t + T_m)$, we have*

$$G_{P^*,\gamma,m} = \{(h_g, t - t_g + T_m) \mid g \in P, t \in T\} \subseteq P^* \ltimes T^*_{\gamma,m}.$$

Proof. By abuse of notation, ϕ yields an embedding $\phi\colon G/T_{j^*} \to G^*/T_{j^*}$ which maps $u = (g, t + T_{j^*}) \in P.(T/T_{j^*})$ to $\phi(u) = (h_g, t - t_g + T_{j^*}) \in P^* \ltimes T^*/T_{j^*}$; recall that each $(g, 0) \in P.T^*$ can be written as $(h_g, -t_g) \in P^* \ltimes T^*$. Thus the full preimage of $\phi(u)$ under π consists of all $(h_g, t + s - t_g) \in P^* \ltimes T/T_m$ with $s \in T_{j^*}$. It follows that $G_{P^*,\gamma,m}$ is indeed the set given in the proposition. □

Remark 4.6. We give a direct proof that the set in Proposition 4.5 is a subgroup of $G^*_{\gamma,m}$. If $g, k \in P$, then $h_{gk} = (gk, t_{gk})$ and $h_g h_k = (gk, t_g^k + t_k + \delta(g,k)) \in P^*$ where $\delta \in Z^2(P,T)$ is the 2-cocycle defining the extension G of T by P; in particular, $h_{gk} = h_g h_k$ and so $t_{gk} = t_g^k + t_k + \delta(g,k) \equiv t_g^k + t_k \bmod T$. This can be used to verify that the product in $P^* \ltimes T^*_{\gamma,m}$ of two elements in $G_{P^*,\gamma,m}$ lies indeed in $G_{P^*,\gamma,m}$. It follows from $t_g^{(g^{-1})} + t_{g^{-1}} = 0$ that $G_{P^*,\gamma,m}$ is closed under inversion.

In the following, let $x \geq 0$, $T^* = p^{-x}T$, P^*, and $h_g = (g, t_g) \in P^*$ for $g \in P$ be as above. Since $P \cong P^*$ and each $h_g \in P^*$ acts on T^* as $g \in P$, we can define:

Definition 4.7. Let $\gamma\colon T \wedge T \to T_j$ be a surjective $\mathbb{Z}_pP$-homomorphism such that $j^* = j - 2xd \geq 0$, and let m be such that $j^* \leq m \leq 2j^* + (x-1)d$. The skeleton group defined by γ and m and the chosen complement P^* is

$$G_{P^*,\gamma,m} = \{(g, t - t_g + T_m) \mid g \in P, t \in T\} \subseteq P \ltimes T^*_{\gamma,m}.$$

A group is a skeleton group if it is isomorphic to $G_{P^*,\gamma,m}$ for certain P^*, γ, and m.

The projection $G_{P^*,\gamma,m} \to P$ has kernel $\{(1, t + T_m) \mid t \in T\} \cong T_{\gamma,m}$ and is surjective, so $G_{P^*,\gamma,m}$ is an extension of $T_{\gamma,m}$ by P. Moreover, if G splits, then $T = T^*$ and we can choose $P = P^*$ and $t_g = 0$ for all $g \in P$; in this case $G_{P^*,\gamma,m} = P \ltimes T_{\gamma,m}$ as in Section 4.4.1. We also note the following, cf. [53, Lemma 8.4.11].

Remark 4.8. The projection from $G_{\gamma,m}$ onto $P^* \cong P$ is surjective with the kernel $\{(1, t + T_m) \mid t \in T\} \cong T_{\gamma,m}$. This shows that $G_{\gamma,m}$ is an extension of P by $T_{\gamma,m}$. In

particular if G splits over T, then $T^* = T$ and $G = P \ltimes T$, so we can choose $t_g = 0$ for all $g \in P$, and $G_{\gamma,m} = (\{(g, t + T_m) \mid t \in T, g \in P\}, \cdot_\gamma) = P \ltimes T_{\gamma,m}$. From the construction of skeleton group $G_{\gamma,m}$, it can be seen that $G_{\gamma,m}$ lies at depth $m - j$ in the branch with root $P \ltimes T/T_j$.

The following shows that the skeleton group $G_{P^*,\gamma,m}$ lies in the branch $\mathcal{B}_j$.

Corollary 4.9. *Let $j_0 = \max\{k, d + 1\}$ where $\gamma_{c+1}(G) = T_k$ and c is the nilpotency class of P. Let γ be a surjective $\mathbb{Z}_pP$-homomorphism $T \wedge T \to T_j$ with $j^* > j_0$, and choose m such that $j^* \leq m \leq 2j^* + (x - 1)d$. Then $G_{P^*,\gamma,m}$ has coclass r and G/T_{j^*} as a quotient. If $x = 0$, then $G_{P^*,\gamma,m}$ does not have G/T_{j^*+1} as a quotient.*

Proof. Since P acts uniserially on T, the group G/T_j has coclass r for all $j \geq j_0$. It follows from $\gamma(T^* \wedge T^*) \leq T_{j^*}$ and $\gamma(T_{j^*} \wedge T^*) \leq T_m$ that $N = T_{j^*}/T_m$ is a normal subgroup of $S = G_{P*,\gamma,m}$. Since $\iota\colon (g, t + T_{j^*}) \to (g, -t_g + t + T_{j^*})$ is an isomorphism between G/T_{j^*} and S/N, see Remark 4.6, the latter groups have coclass r by assumption. Thus, if G/T_{j^*} has order p^u, then $T_{j^*} = \gamma_{u-r+1}(G)$ and $\gamma_{u-r+1}(S) \leq N$. Note that S/N acts uniserially on N and $\gamma_{u-r+1}(S) \leq N$ is S/N-invariant. Thus, S has coclass r if $\gamma_{u-r+1}(S) = N$, which holds if $\gamma_{u-r+1}(S) \not\leq T_{j^*+1}/T_m$, see Lemma 3.8. To prove the latter, we first use ι to deduce that $\gamma_{u-r}(S/N) = T_{j^*-1}/T_{j^*}$. This allows us to choose $(1, t + T_m) \in \gamma_{u-r}(S)$ and $(g, -t_g + T_m) \in S$ with $t \in T_{j^*-1}$ and $t - t^g \notin T_{j^*+1}$, so that in S

$$[(g, -t_g)(1, t + T_m)] = (1, t - t^g - \tfrac{1}{2}\gamma(t^g \wedge t) + \gamma(t^g \wedge t_g) + T_m) \notin T_{j^*+1}/T_m;$$

note that $\frac{1}{2}\gamma(t^g \wedge t) + \gamma(t^g \wedge t_g) \in T_{j^*+1}$ since $T_{j^*-1} \leq pT$. Thus $\gamma_{u-r+1}(S) = N$. If $x = 0$, then the quotient of $T_{\gamma,m}$ by T_{j+1}/T_m is not abelian whereas G/T_{j+1} is abelian and thus the claim follows. □

4.4.3 Skeleton groups are constructible groups

Skeleton groups are motivated by the definition of constructible groups as in [53, Definition 8.4.9]. We first recall the latter from [53, Chapter 8] by first introducing results related to pull-backs and Baer sums, see [53, Section 2.2]. We finally show that every constructible group is a skeleton group and vice versa.

Definition 4.10. Let L, H and K be groups, and $\alpha : L \to K$ and $\beta : H \to K$ be homomorphisms; then the pull-back, (X, α', β') of (α, β) is the subgroup of $L \times H$ given by

$$X = \{(g, h) \mid g \in L, h \in H \text{ and } \alpha(g) = \beta(h)\},$$

together with the maps α', β' which are the projections from X into H and L respectively. In other words, the following is a commutative diagram,

$$\begin{array}{ccc} X & \xrightarrow{\beta'} & L \\ \downarrow{\scriptstyle \alpha'} & & \downarrow{\scriptstyle \alpha} \\ H & \xrightarrow{\beta} & K \end{array}$$

Lemma 4.11. *Let $\mathcal{E} \equiv 0 \longrightarrow A \xrightarrow{\alpha} E \xrightarrow{\pi} B \longrightarrow 1$ be an extension of an abelian group A by a group B. If $\phi : B_1 \to B$ is a homomorphism, then there exists an extension $\mathcal{E}\phi \equiv 0 \longrightarrow A \xrightarrow{\alpha'} E_1 \xrightarrow{\pi'} B_1 \longrightarrow 1$ and a homomorphism, $\phi' : E_1 \to E$ such that the following diagram commutes:*

$$\begin{array}{rcl} \mathcal{E}\phi & \equiv & 0 \longrightarrow A \xrightarrow{\alpha'} E_1 \xrightarrow{\pi'} B_1 \longrightarrow 1 \\ & & \quad\Vert \quad\quad \downarrow{\scriptstyle \phi'} \quad\quad \downarrow{\scriptstyle \phi} \\ \mathcal{E} & \equiv & 0 \longrightarrow A \xrightarrow{\alpha} E \xrightarrow{\pi} B \longrightarrow 1 \end{array}$$

If ϕ is surjective, then so is ϕ'.

Lemma 4.12. *Let $\mathcal{E} \equiv 0 \longrightarrow A \xrightarrow{\alpha} E \xrightarrow{\pi} B \longrightarrow 1$ be an extension of an abelian group A by a group B. If A_2 is a B-module and $\phi : A \to A_2$ is a B-module homomorphism, then there exists an extension $\phi\mathcal{E} \equiv 0 \longrightarrow A_2 \xrightarrow{\alpha''} E_2 \xrightarrow{\pi''} B \longrightarrow 1$ and a homomorphism, $\phi'' : E \to E_2$ such that the following diagram commutes:*

$$\begin{array}{rcl} \phi\mathcal{E} & \equiv & 0 \longrightarrow A_2 \xrightarrow{\alpha''} E_2 \xrightarrow{\pi''} B \longrightarrow 1 \\ & & \quad\uparrow{\scriptstyle \phi} \quad\quad \uparrow{\scriptstyle \phi''} \quad\quad \Vert \\ \mathcal{E} & \equiv & 0 \longrightarrow A \xrightarrow{\alpha} E \xrightarrow{\pi} B \longrightarrow 1 \end{array}$$

If ϕ is injective, then so is ϕ''.

Definition 4.13. Let A be an abelian group, and let

$$\mathcal{E} \equiv 0 \longrightarrow A \xrightarrow{\alpha} E \xrightarrow{\pi} B \longrightarrow 1$$

and

$$\mathcal{E}' \equiv 0 \longrightarrow A \xrightarrow{\beta} E_1 \xrightarrow{\rho} B_1 \longrightarrow 1$$

be two extensions inducing the same action of B on A; then the Baer sum $\mathcal{E} + \mathcal{E}'$ of the two extensions is constructed as follows. Let (S, π', ρ') be the pull-back of (π, ρ), and let $N = \{(\alpha(a), -\beta(a)) \mid a \in A\}$, which is a normal subgroup of S. Define $E^* = S/N$, and a surjection $\pi^* : E^* \to B$ by $(e, e')N \mapsto \pi(e)$ for all $(e, e') \in S$, and define an injection $\alpha^* : A \to E^*$ by $a \mapsto (\alpha(a), 0)N$. Then $\alpha^*(A)$ is the kernel of π^*. Now $\mathcal{E} + \mathcal{E}'$ is the extension $0 \longrightarrow A \xrightarrow{\alpha^*} E^* \xrightarrow{\pi^*} B \longrightarrow 1$.

The following definition is from [53, Section 8.1]. Recall that for any prime p, an abelian group H is p-divisible if for every $h \in H$, there exists $y \in H$ such that $py = h$, or equivalently, an abelian group H is p-divisible if and only if $pH = H$.

Definition 4.14. Let A and B be Q-modules for some group Q; for reasons that will become apparent later, we write A additively and B multiplicatively. If $\gamma \in \mathrm{Hom}_Q(\wedge^2 B, A)$ and the image of γ is 2-divisible, then the group $R(\gamma)$ is defined as follows. The underlying set of $R(\gamma)$ is the direct product of the sets B and A, and multiplication on $R(\gamma)$ is defined by

$$(b_1, a_1)(b_2, a_2) = (b_1 b_2, a_1 + a_2 + \frac{1}{2}\gamma(b_1 \wedge b_2))$$

for all $a_1, a_2 \in A$ and $b_1, b_2 \in B$. The realisation of γ is the extension given by the natural exact sequence

$$\mathcal{R}_\gamma \equiv 0 \longrightarrow A \longrightarrow R(\gamma) \longrightarrow B \longrightarrow 1.$$

We now recall the very first step to define constructible groups; see [53, Definition 8.4.3].

Definition 4.15. The following data will be used to construct a group G_γ.

a) An extension $\mathcal{E} \equiv 0 \longrightarrow B \xrightarrow{\mu} E \xrightarrow{\pi} Q \longrightarrow 1$ where B is abelian and Q is a finite p-group.

b) An Q-embedding θ of B in a Q-module B_0 with a given splitting τ of $\theta\mathcal{E}$.

c) An extension $\mathcal{D} \equiv 0 \longrightarrow A \xrightarrow{\nu} K \xrightarrow{\pi} E \longrightarrow 1$ where A is abelian of odd order and is centralised by $\mu(B)$, and so is a Q-module.

d) $\gamma \in \mathrm{Hom}_Q(\wedge^2 B_0, A)$.

The group G_γ is constructed as follows. From a) and b) there exists an embedding $\phi : E \to Q \ltimes B_0$ such that $\phi\mu = \eta\theta$ where $\eta : B_0 \to Q \ltimes B_0$ is the natural map. Now the homomorphism γ in d) gives rise to the following central Q-extension

$$\mathcal{R}_\gamma \equiv 0 \longrightarrow A \longrightarrow R(\gamma) \longrightarrow B \longrightarrow 1.$$

This gives rise to the extensions

$$\mathcal{F}_\gamma \equiv 0 \longrightarrow A \longrightarrow Q \ltimes R(\gamma) \longrightarrow Q \ltimes B_0 \longrightarrow 1$$

and

$$\mathcal{F}_\gamma\phi \equiv 0 \longrightarrow A \longrightarrow Y \longrightarrow E \longrightarrow 1,$$

and, using c), the group G_γ is defined by the Baer sum

$$(\mathcal{D} + \mathcal{F}_\gamma\phi) \equiv 0 \longrightarrow A \xrightarrow{\nu_\gamma} G_\gamma \xrightarrow{\rho_\gamma} E \longrightarrow 1.$$

We will now state the definition of constructible group as in [53, Definition 8.4.8]. Recall from Section 3.1.5 that if G is a pre-space group with a translation subgroup T and corresponding point group P then there is a split pre-space group G^* containing G with a translation subgroup T^* and corresponding point group P. We note from [53] that for an odd prime p the concept behind constructible group is to construct, from a space group G with G-module $U < V$ of its translation subgroup T, a new group out of G/U by 'twisting' the image T/U of T in such a way that the twisted version of T/U is a central extension of V/U by T/V.

Definition 4.16. Let G be a pre-space group with a translation subgroup T and corresponding point group P. Let $U < V$ be P-modules of T, and T^* be the minimal supergroup of T over which G splits, and let $\tau_0 : P \to T^*G$ be a splitting. Let $\alpha \in \mathrm{Hom}_P(\wedge^2 T, V)$ induce $\gamma \in \mathrm{Hom}_P(\wedge^2(T^*/V), V/U)$. Then the group (G, U, V, α) is defined to be the group G_γ constructed using Definition 4.15 where K, E, A, B, B_0, Q are respectively $G/U, G/V, V/U, T/V, T^*/V, P$ with γ as given here, and τ is the composite of τ_0 and the natural projection from T^*G to T^*G/V.

Definition 4.17. [53, Definition 8.4.9] A finite p-group of coclass r is called constructible if it is isomorphic to a group (G, U, V, α) as given in Definition 4.16 with G a uniserial p-adic space group of coclass at most r.

We now establish the following:

Proposition 4.18. *Every constructible group is a skeleton group, and every skeleton group for a uniserial p-adic space group is a constructible group.*

Proof. Let $G = P.T$ be a uniserial p-adic space group of coclass r, with point group P, translation subgroup T, and extended uniserial series with terms T_i, $i \in \mathbb{Z}$.

Let $G^* = P.T^* = P^* \ltimes T^*$ be as defined in Section 3.1.5, with embedding $\phi\colon G \to G^*$. By abuse of notation, for $i \geq 0$ we denote the induced embeddings $G/T_i \to G^*/T_i$ also by ϕ. Let $\alpha\colon T \wedge T \to T_j$ be a surjective $\mathbb{Z}_pP$-homomorphism, inducing a surjective $\mathbb{Z}_pP$-homomorphism $\gamma\colon (T^*/T_{j^*}) \wedge (T^*/T_{j^*}) \to T_{j^*}/T_m$ where $j^* = j - 2xd$ as in (4.1); this requires $\alpha(T_{j^*} \wedge T^*) \leq T_m$. Use this homomorphism γ to define

$$R(\gamma) = (T^*/T_{j^*} \times T_{j^*}/T_m, \circ_\gamma)$$

where $(a, c) \circ_\gamma (b, d) = (a + b, c + d + \frac{1}{2}\gamma(a \wedge b))$; note that $R(\gamma)$ is an extension

$$\mathcal{R}_\gamma \quad \equiv \quad 0 \to T_{j^*}/T_m \to R(\gamma) \to T^*/T_{j^*} \to 1$$

which has the same commutator structure as the twisted group $T^*_{\alpha,m}$ defined in Section 4.4.1. In fact, $T^*_{\alpha,m}$ can be defined by the Baer sum $\mathcal{R}_\gamma + \mathcal{E}$ where

$$\mathcal{E} \quad \equiv \quad 0 \to T_{j^*}/T_m \to T^*/T_m \to T^*/T_{j^*} \to 1$$

is the natural extension of T_{j^*}/T_m by T^*/T_{j^*} describing T^*/T_m. Since γ is compatible with the action of P, one can define an extension $\mathcal{F}_\gamma$ as follows, and then use ϕ and a pull-back construction to define a group Y via $\mathcal{F}_\gamma\phi$:

$$\begin{array}{rl} \mathcal{F}_\gamma \equiv & 0 \longrightarrow T_{j^*}/T_m \longrightarrow P^* \ltimes R(\gamma) \longrightarrow G^*/T_{j^*} \longrightarrow 1 \\ & \qquad\quad \| \qquad\quad \phi'\uparrow \qquad\quad \phi\uparrow \\ \mathcal{F}_\gamma\phi \equiv & 0 \longrightarrow T_{j^*}/T_m \longrightarrow Y \longrightarrow G/T_{j^*} \longrightarrow 1 \end{array}$$

In cohomological terms, if δ is the cohomology class defining $P^* \ltimes R(\gamma)$ as an extension of T_{j^*}/T_m by G^*/T_{j^*}, then the restriction of δ to $\phi(G/T_{j^*})$ describes $\phi'(Y)$ as an extension of T_{j^*}/T_m by $\phi(G/T_{j^*})$; now Y is the preimage of that extension under the embedding. Lastly, describe G/T_m as the extension

$$\mathcal{D} \quad \equiv \quad 0 \to T_{j^*}/T_m \to G/T_m \to G/T_{j^*} \to 1.$$

The constructible group G_γ is now defined via the Baer sum

$$\mathcal{D} + \mathcal{F}_\gamma\phi \quad \equiv \quad 0 \to T_{j^*}/T_m \to G_\gamma \to G/T_{j^*} \to 1.$$

This completes the description of constructible groups as given in [53, Section 8.4]; we now investigate this further.

If G splits over T, then the construction of $G^* = P^* \ltimes T = P.T = G$ amounts to choosing a complement P^*. The corresponding embedding $\phi\colon G \to G^*$ is an isomorphism, and working through the above details shows that the constructible group G_γ is isomorphic to the skeleton group $G_{\gamma,m} = P \ltimes T_{\gamma,m}$, as defined in Section 4.4.1. In particular, the isomorphism type of G_γ is independent of the chosen complement and embedding; moreover, starting with $G = P \ltimes T$, we can assume that ϕ is the identity, and so $G_{\gamma,m}$ can be defined via the Baer sum $\mathcal{D} + \mathcal{F}_\gamma$.

Now suppose that G does not split over T. To understand the group defined by $\mathcal{D}+\mathcal{F}_\gamma\phi$, we make a detour via $G^* = P^* \ltimes T^*$. As explained in the previous paragraph, the constructible group G^*_γ can be constructed as $G^*_{\gamma,m} = P^* \ltimes T^*_{\gamma,m}$, which is realised via the Baer sum $\tilde{\mathcal{D}} + \mathcal{F}_\gamma$, where

$$\tilde{\mathcal{D}} \equiv 0 \to T_{j^*}/T_m \to P^* \ltimes T^*/T_m \to P^* \ltimes T^*/T_{j^*} \to 1.$$

Note that $\mathcal{D} \equiv \tilde{\mathcal{D}}\phi$ and $\mathcal{D} + \mathcal{F}_\gamma\phi \equiv \tilde{\mathcal{D}}\phi + \mathcal{F}_\gamma\phi \equiv (\tilde{\mathcal{D}} + \mathcal{F}_\gamma)\phi$, see [53, Exercise 2.2(3)(iii)], so we have

$$\begin{array}{rcl} \tilde{\mathcal{D}} + \mathcal{F}_\gamma & \equiv & 0 \longrightarrow T_{j^*}/T_m \longrightarrow P^* \ltimes T^*_{\gamma,m} \xrightarrow{\pi} P^* \ltimes T^*/T_{j^*} \longrightarrow 1 \\ & & \quad\Vert \qquad\quad \phi''\uparrow \qquad\qquad \phi\uparrow \\ (\tilde{\mathcal{D}} + \mathcal{F}_\gamma)\phi & \equiv & 0 \longrightarrow T_{j^*}/T_m \longrightarrow G_\gamma \longrightarrow G/T_{j^*} \longrightarrow 1 \end{array}$$

In cohomological terms, if δ is the cohomology class defining $G^*_\gamma = P^* \ltimes T^*_{\gamma,m}$ as an extension of T_{j^*}/T_m by $G^*/T_{j^*} = P^* \ltimes T^*/T_{j^*}$, then the restriction of δ to $\phi(G/T_{j^*})$ describes $\phi''(G_\gamma)$ as an extension of T_{j^*}/T_m by $\phi(G/T_{j^*})$; now G_γ is the preimage of that extension under the embedding. In other words, $\phi''(G_\gamma) \cong G_\gamma$ is the full preimage under $\pi\colon G^*_\gamma \to G^*/T_{j^*}$ of the embedding of G/T_{j^*} into G^*/T_{j^*} via ϕ. This proves that G_γ is a skeleton group as defined in Section 4.4.2.

Conversely, the above construction also shows that every skeleton group (defined for a space group) is constructible. In fact, our construction of skeleton groups is motivated by an analysis of the definition of constructible groups. □

We argue that for split space groups, we can choose the embedding ϕ to be the identity, as done in the proof of Proposition 4.18. To see this we refer back to [53, Definition 8.4.3] and use the notation in the proof of Proposition 4.18. Suppose $G = P \ltimes T$ is split. Writing the elements of G as (g, t) with $g \in P, t \in T$ we choose a splitting $\tau : P \to G$, $(g, t) \mapsto h_g = (g, t_g)$ with $t_g \in T$ for each $g \in P$; its image is $\tilde{P} = \{h_g \mid g \in P\}$. If, in cohomological terms, G is defined by a 2-cocycle δ (in fact, a 2-coboundary since G is split), then $t_{gk} = t^k_g + t_k + \delta(g, k)$ for all $g, k \in P$. We now take the embedding $\phi : G/T_j \to \tilde{P} \ltimes T/T_j$ defined by

$$(g, t + T_j) \mapsto (h_g, t - t_g + T_m).$$

Note that, since G/T_j and $\tilde{P} \ltimes T/T_j$ have same order, ϕ is an isomorphism with inverse given by $(h_g, t + T_j) \mapsto (g, t + t_g + T_j)$. For a P-module homomorphism γ, the group $R(\gamma)$ has underlying set $T/T_j \times T_j/T_m$ and multiplication

$$(a + T_j, c + T_m)(b + T_j, d + T_m) = (a + c + T_j, b + d + \frac{1}{2}\gamma(a \wedge c) + T_m).$$

We now recall the following exact sequences.

$$\begin{array}{rcl} \mathcal{F}_\gamma & \equiv & 0 \longrightarrow T_j/T_m \xrightarrow{\alpha} \tilde{P} \ltimes R(\gamma) \xrightarrow{\beta} \tilde{P} \ltimes T/T_j \longrightarrow 1 \\ & & \quad\Vert \qquad\quad \phi'\uparrow \qquad\qquad \phi\uparrow \\ \mathcal{F}_\gamma\phi & \equiv & 0 \longrightarrow T_j/T_m \xrightarrow{\alpha'} Y \xrightarrow{\beta'} G/T_j \longrightarrow 1 \end{array}$$

where α and β are given by $(t+T_m) \mapsto (1,(0+T_j,t+T_m))$ and $(h_g,(a+T_j,b+T_m)) \mapsto (h_g,a+T_j)$ respectively for $g \in P, t \in T_j, a \in T, b \in T_j$. The group Y is constructed using the pull-back as described in the beginning of Section 4.4.3. Following the definition of pull-backs, as a set Y is given by

$$\{((h_g,(a+T_j,b+T_m)),(k,t+T_j)) \mid (h_g,a+T_j) = (h_k,t-t_k+T_j)\} \leq (\tilde{P} \ltimes R(\gamma)) \times (G/T_j).$$

Thus $Y = \{((h_g,(a+T_j,b+T_m)),(g,a+t_g+T_j)) \mid g \in P, a \in T, b \in T_j\}$, and so Y is indeed isomorphic to $\tilde{P} \ltimes R(\gamma)$; this means that ϕ' can be regarded as the identity. This allows us to take $\alpha' = \alpha$ and β' is defined by $(h_g,(a+T_j,b+T_m)) \mapsto (g,t_g+a+T_j)$. Now consider the exact sequence

$$\mathcal{D} \quad \equiv \quad 0 \to T_j/T_m \to G/T_m \to G/T_j \to 1$$

and take the Baer sum

$$\mathcal{D} + \mathcal{F}_\gamma\phi \quad \equiv \quad 0 \to T_j/T_m \to G_\gamma \to G/T_j \to 1.$$

To understand this Baer sum, we note that $G_\gamma = S/N$ where

$$S = \{((h_g,(a+T_j,b+T_m)),(g,t_g+a+s+T_m)) \mid g \in P, a \in T, b \in T_j, s \in T_j\}$$

and

$$N = \langle\{((1,(0+T_j,u+T_m)),(1,-u+T_m)) \mid u \in T_j\}\rangle.$$

Now we observe that the group $T_{\gamma,m}$ can be realised as the Baer sum of two exact sequences, one representing $R(\gamma)$ as an extension of T/T_j by T_j/T_m and the other representing T/T_m as an extension of T/T_j by T_j/T_m. Hence $T_{\gamma,m} \cong \tilde{S}/\tilde{N}$ where

$$\tilde{S} = \{((a+T_j,b+T_m),a+s+T_m) \mid a \in T, b, s \in T_j\}$$

and

$$\tilde{N} = \langle\{((0+T_j,u+T_m),-u+T_m) \mid u \in T_j\}\rangle \cong N.$$

Now consider $\widehat{P} = \{((h_g,(0+T_j,0+T_m)),(g,t_gT_m)) \mid g \in P\} \cong P$ and note that

$$\begin{aligned} & ((h_g,(a+T_j,b+T_m)),(g,t_g+a+s+T_m)) \\ = \quad & ((h_g,(0+T_j,0+T_m)),(g,t_gT_m))((1,(a+T_j,b+T_m)),(1,a+s+T_m)) \end{aligned}$$

for all $g \in P$, $a \in T$, and $s, b \in T_j$. Hence irrespective of the chosen embedding ϕ, we have

$$G_{\gamma,m} = G_\gamma = S/N = (\widetilde{P} \ltimes \tilde{S})/N = \widehat{P} \ltimes (\tilde{S}/N) = \tilde{P} \ltimes T_{\gamma,m} \cong P \ltimes T_{\gamma,m}.$$

Hence without loss of generality we may take the embedding ϕ to be identity.

As mentioned before, in [53] constructible groups are only defined for uniserial p-adic space groups. However, if $G_{\gamma,m}$ is a skeleton group for a uniserial p-adic pre-space group G, then there is a finite normal subgroup $H \trianglelefteq G_{\gamma,m}$, isomorphic to the hypercentre Z of G, such that $G_{\gamma,m}/H$ is a constructible group for the uniserial p-adic space group G/Z, see Lemma 3.11. In particular, [53, Theorem 11.3.9] can be formulated for skeleton groups.

Theorem 4.19. *Almost every finite p-group H of coclass r has a normal subgroup N such that H/N is a skeleton group and $|N| \leq p^{(p-1)p^{r-1}(7p^{r-1}+7r+4)}$.*

Remark 4.20. In conclusion, skeleton groups are important for two reasons:

- In contrast to an arbitrary p-group of coclass r, skeleton groups are easy to construct and to work with: they are "twisted" finite quotients of the associated pro-p-group, conveniently parametrised by certain $\mathbb{Z}_p P$-homomorphisms $T \wedge T \to T$.
- Theorem 4.19 shows that, with finitely many exceptions, every group in the graph $\mathcal{G}(p, r)$ has bounded distance to a skeleton group. This shows that skeleton groups in $\mathcal{G}(p, r)$ form indeed the "skeleton" of the graph.

Since understanding the skeleton subgraph of $\mathcal{G}(p, r)$ is a crucial and more feasible first step toward understanding the general structure of $\mathcal{G}(p, r)$, it is of interest to study skeleton groups. To determine the structure of the subgraph spanned by skeleton groups (and to possibly identify periodic patterns in the graph), it is important to decide when two homomorphisms parametrise isomorphic skeleton groups. We investigate this in the next chapter.

Chapter 5

Isomorphism Problem of Skeleton Groups

Let G be an infinite pro-p-group of coclass r and dimension d, with point group P and translation subgroup T; we assume that p is an odd prime. Throughout in this chapter, we assume that T is characteristic in G; this holds, for example, if G is a space group. We denote by

$$G^* = P.T^* = P^* \ltimes T^* \quad \text{with} \quad T^* = p^{-x}T$$

the minimal split supergroup, as discussed in Theorem 3.28. In particular, throughout this chapter, x is defined by this property. The results of this chapter appear in [22].

5.1 Preliminary results

Lemma 5.1. *Let $G_{\gamma,m}$ and $G_{\gamma',m}$ be skeleton groups defined with respect to P^* as in Definition 4.7. Let $\alpha \in \mathrm{Aut}(G)$ be such that*

$$\alpha(\gamma(t \wedge s)) \equiv \gamma'(\alpha(t) \wedge \alpha(s)) \bmod T_{m+2xd} \quad \textit{for all } s,t \in T. \tag{5.1}$$

a) *If G is split, then $G_{\gamma,m} \cong G_{\gamma',m}$.*

b) *If G is non-split and $G_{\gamma',m} \cong G_{\alpha(P^*),\gamma',m}$, then $G_{\gamma,m} \cong G_{\gamma',m}$.*

Proof. By assumption, $T \leq G$ is characteristic, so α induces automorphisms of T and $P \cong G/T$ which, by abuse of notation, are also denoted by α in the following.

a) Note that α maps $(g,t) \in P \ltimes T$ to $(\alpha(g), \phi(g) + \alpha(t))$ for some map $\phi : P \to T$. Then $G \to G$, $(g,t) \mapsto (\alpha(g), \alpha(t))$, is also an automorphism satisfying (5.1), hence we

assume $\phi = 0$ in the following. The next map is well-defined

$$\Phi : P \ltimes T_{\gamma,m} \to P \ltimes T_{\gamma',m}, \quad (g, t + T_m) \mapsto (\alpha(g), \alpha(t) + T_m);$$

together with (5.1), it follows that Φ is a group isomorphism:

$$\begin{aligned}
& \Phi((g, a + T_m) \circ_\gamma (h, b + T_m)) \\
= \; & \Phi(gh, a^h + b + \tfrac{1}{2}\gamma(a^h \wedge b) + T_m) \\
= \; & (\alpha_1(gh), \alpha(a^h) + \alpha(b) + \tfrac{1}{2}\alpha(\gamma(a^h \wedge b)) + T_m) \\
= \; & (\alpha(g)\alpha(h), \alpha(a)^{\alpha(h)} + \alpha(b) + \tfrac{1}{2}\gamma'(\alpha(a)^{\alpha(h)} \wedge \alpha(b)) + T_m) \\
= \; & \Phi((g, a + T_m)) \circ_{\gamma'} \Phi((h, b + T_m))
\end{aligned}$$

b) We extend α to an automorphism of G^*; now $\alpha(P^*)$ is also a complement to T^* in G^* as $\alpha(T^*) = T^*$. Write the elements of P^* and $\alpha(P^*)$ as h_g and k_g, respectively, with $g \in P$, such that α maps $(h_g, t) \in P^* \ltimes T^*$ to $(k_{\alpha(g)}, \alpha(t)) \in \alpha(P^*) \ltimes T^*$. Recall that

$$\begin{aligned}
G_{\gamma,m} &= \{(g, t - t_g + T_m) \mid g \in P, t \in T\}, \\
G_{\alpha(P^*),\gamma,m} &= \{(g, t - s_g + T_m) \mid g \in P, t \in T\},
\end{aligned}$$

where $s_g, t_g \in T^*$ are defined by expressing $(g, 0) \in P.T$ as $(h_g, -t_g) \in P^* \ltimes T^*$ and as $(k_g, -s_g) \in \alpha(P^*) \ltimes T^*$. As α maps $(h_g, -t_g)$ to $(k_{\alpha(g)}, -\alpha(t_g)) \in \alpha(P^*) \ltimes T^*$, this image element also lies in G since $\alpha(G) = G$. So we deduce $\alpha(t_g) \equiv s_{\alpha(g)} \bmod T$ for all $g \in P$. A direct calculation shows that the following is an isomorphism:

$$\Phi : G^*_{\gamma,m} \to G^*_{\gamma',m}, \quad (g, t + T_m) \mapsto (\alpha(g), \alpha(t) + T_m).$$

In particular, Φ maps $(g, t - t_g + T_m) \in G_{\gamma,m}$ to $(\alpha(g), \alpha(t) - \alpha(t_g) + T_m)$, and the latter lies in $G_{\alpha(P^*),\gamma',m}$ since $\alpha(t_g) \equiv s_{\alpha(g)} \bmod T$. Thus, Φ induces an isomorphism between $G_{\gamma,m}$ and $G_{\alpha(P^*),\gamma',m}$, and $G_{\alpha(P^*),\gamma',m} \cong G_{\gamma',m}$ by assumption. □

Remark 5.2. Lemma 5.1 is a modified version of the result given in [34, Lemma 3.3]. The modification is needed because the statement and proof given in [34] does not seem correct: for example, in the non-split case, [34, Lemma 3.3] states (5.1) with "mod T_m", whereas it must be "mod T_{m+2xd}".

An isomorphism between skeleton groups that arises from an automorphism of G (as described in Lemma 5.1) is called *orbit isomorphisms* in [34]; if two isomorphic skeleton group do not admit any orbit isomorphism, then any isomorphism is called *exceptional*, see [34, p. 1249]. It is shown in [34, p. 1269] that in $\mathcal{G}(3, 2)$ exceptional isomorphisms exist and that it can happen that $G^*_{\gamma,m} \cong G^*_{\gamma',m}$, but $G_{\gamma,m}$ and $G_{\gamma',m}$ are not isomorphic.

In [34] and [53] it is not discussed to what extent the isomorphism type of a skeleton group depends on the chosen translation subgroup T, point group P, and complement P^*. For example, if one fixes a complement P^*, is every skeleton group isomorphic to some $G_{P^*,\gamma,m}$? In fact, [34, Theorem 3.4] seems to imply that this is true because skeleton groups in [34] are defined with respect to a fixed complement. Unfortunately no justification is given, and to us it seems that the answer to this question is not easy in general. We concentrate on the split case in the following.

5.2 Isomorphism problem

In this section, we assume that G is split. We study twisted groups $T_{\gamma,m}$ and $T_{\gamma',m}$ with surjective homomorphisms $\gamma, \gamma' : T \wedge T \to T_j$; recall that $j \leq m \leq 2j - d$ by Definition 4.7. The next lemma shows how twisted groups are related to the abelian quotients of T.

Lemma 5.3. *Consider $T_{\gamma,m}$ and $T_{\gamma',m}$ with $\gamma, \gamma' : T \wedge T \to T_j$ surjective.*

a) *Every automorphism of T/T_m lifts to an automorphism of T.*

b) *If $\beta : T_{\gamma,m} \to T_{\gamma',m}$ is an isomorphism, then $\beta \in \mathrm{Aut}(T/T_m)$.*

c) *The groups $T_{\gamma,m}$ and $T_{\gamma',m}$ are isomorphic if and only if there is $\alpha \in \mathrm{Aut}(T)$ satisfying $\alpha(T_m) = T_m$ and (5.1) with $x = 0$.*

Proof. a) Let $\beta \in \mathrm{Aut}(T/T_m)$, let $\{t_1, \ldots, t_d\}$ be a (topological) generating set of T, and identify $\mathrm{Aut}(T) = \mathrm{GL}_d(\mathbb{Z}_p)$. Choose a $d \times d$ matrix $A = (a_{i,j})$ over $\mathbb{Z}_p$ such that each $\beta(t_j + T_m) = a_{j,1}t_1 + \ldots + a_{j,d}t_d + T_m$. If $m \geq d$, then $T_m \leq pT \leq T$ and so $A \bmod p$ describes the restriction of β to T/pT. This proves $p \nmid \det(A)$, so $\det(A)$ is a unit in $\mathbb{Z}_p$, and hence $A \in \mathrm{GL}_d(\mathbb{Z}_p)$ by [26, Theorem 11.30]. Clearly, A induces β. Suppose now $m < d$. In this case T/T_m is elementary abelian, so $T/T_m \cong C_p^m$ where C_p is the cyclic group of order p. Let $V = T/pT \cong C_p^d$ and $U \leq V$ such that $V/U \cong T/T_m$. We choose a basis $\{r_1, \ldots, r_d\}$ of V such that $\{r_{m+1}, \ldots, r_d\}$ is a basis of U. Let $\alpha \in \mathrm{Aut}(T/T_m)$ and choose a matrix $B \in \mathrm{GL}_m(\mathbb{Z}/p\mathbb{Z})$ that represents α with respect to $\{r_1 + U, \ldots, r_m + U\}$. Then $\hat{B} = \mathrm{diag}(B, I_{d-m}) \in \mathrm{GL}_d(\mathbb{Z}/p\mathbb{Z}) \cong \mathrm{Aut}(T/pT)$. As in the case $m \geq d$, we see that $\hat{B}$ lifts to an automorphism $\tilde{B}$ of T which clearly induces α.

b) Note that $T_{\gamma,m}$, $T_{\gamma',m}$, and T/T_m have the same underlying set. Let $\alpha : T \to T$ be a map such that $\beta(t + T_m) = \alpha(t) + T_m$ for all $t \in T$. Since β is an isomorphism and $[s + T_m, t + T_m] = \gamma(s \wedge t) + T_m$ in $T_{\gamma,m}$ for all $s, t \in T$, we deduce that $\alpha(\gamma(s \wedge t)) \equiv \gamma'(\alpha(s) \wedge \alpha(t)) \bmod T_m$. In the following let $e = s + t$ and $f = \frac{1}{2}\gamma(s \wedge t)$; note that $\gamma(e \wedge f) = 0$. Now $\alpha(s+t)+T_m = \alpha(s)+\alpha(t)+T_m$ follows from $\beta((s+T_m) \circ_\gamma (t+T_m)) =$

$\alpha(s)+\alpha(t)+\frac{1}{2}\alpha(\gamma(s\wedge t))+T_m$ and

$$\begin{aligned}\beta((s+T_m)\circ_\gamma(t+T_m)) &= \beta((e+T_m)\circ_\gamma(f+T_m))\\ &= (\alpha(e)+T_m)\circ_{\gamma'}(\alpha(f)+T_m)\\ &= \alpha(e)+\alpha(f)+\tfrac{1}{2}\gamma'(\alpha(e)\wedge\alpha(f))+T_m\\ &= \alpha(s+t)+\tfrac{1}{2}\alpha(\gamma(s\wedge t))+T_m.\end{aligned}$$

This implies $\beta(s+t+T_m)=\beta(s+T_m)+\beta(t+T_m)$ for all $s,t\in T$, as claimed.

c) If $\beta: T_{\gamma,m}\to T_{\gamma',m}$ is an isomorphism, then $\beta\in\mathrm{Aut}(T/T_m)$ by b), and therefore $\beta(t+T_m)=\alpha(t)+T_m$ for some $\alpha\in\mathrm{Aut}(T)$ with $\alpha(T_m)=T_m$ by a). Since β is an isomorphism, α satisfies (5.1) with $x=0$. Conversely, if α is as given in the lemma, then $\beta: T_{\gamma,m}\to T_{\gamma',m}$, $t+T_m\mapsto\alpha(t)+T_m$ is an isomorphism. □

The following proposition gives a partial converse of Lemma 5.1a).

Proposition 5.4. *An isomorphism $\phi: G_{\gamma,m}\to G_{\gamma',m}$ with $\phi(T_{\gamma,m})=T_{\gamma',m}$ induces an automorphism of $G/T_j=P\ltimes T/T_j$ defined by*

$$\beta:(g,t+T_j)\mapsto(\phi(g),\phi(g+T_j));$$

here we also write ϕ for the induced automorphisms of $P\cong G_{\gamma,m}/T_{\gamma,m}$ and T/T_j. If $j>d$ and β lifts to an automorphism α of G, then α satisfies (5.1) *with $x=0$.*

Proof. An isomorphism ϕ as in the proposition maps $(g,0),(1,t+T_m)\in P\ltimes T_{\gamma,m}$ to $(\phi(g),\phi'(g))$ and $(1,\Phi(t)+T_m)$, respectively, for some map $\phi': P\to T_{\gamma',m}$ and $\Phi\in\mathrm{Aut}(T)$ with $\Phi(\gamma(s\wedge t))\equiv\gamma'(\Phi(s)\wedge\Phi(t)) \bmod T_m$ for all $s,t\in T$, see the proof of Lemma 5.3. Since ϕ maps the derived subgroup T_j/T_m of $T_{\gamma,m}$ to that of $T_{\gamma',m}$, the map $t+T_j\mapsto\Phi(t)+T_j$ is an automorphism of T/T_j. Recall the definition of $\circ_\gamma$ from Proposition 4.3. Since ϕ is an isomorphism, evaluating the image of $(1,t+T_m)\circ_\gamma(g,0)$ implies $\Phi(t^g)\equiv\Phi(t)^{\phi(g)} \bmod T_j$ for all $g\in P$ and $t\in T$. Thus, $\beta:(g,t+T_j)\mapsto(\phi(g),\Phi(t)+T_j)$, is an automorphism of G/T_j; clearly, $\Phi(t)+T_j=\phi(t+T_j)$.

Now suppose β lifts to $\alpha\in\mathrm{Aut}(G)$, which maps (g,t) to $(\alpha(g),\alpha'(g)+\alpha(t))$ for some map $\alpha': P\to T$. Note that $\alpha'(P)\le T_j$ and $\alpha(t)\equiv\Phi(t) \bmod T_j$ for all $t\in T$ since β induces α. Recall that $j\le m\le 2j-d$ and write $j=yd+i$ with $i\in\{0,\dots,d-1\}$ and $y\ge 1$. Then $j\ge yd$ and $j+yd=2yd+i\ge 2j-d\ge m$, that is, $T_j\le p^yT$ and $p^yT_j\le T_m$. This shows that $\alpha(t)\equiv\Phi(t) \bmod T_m$ for all $t\in T_j$, and therefore α satisfies (5.1) with $x=0$. □

5.2.1 Lifting automorphisms

We continue with the assumption that $G = P \ltimes T$ is split and $T \leq G$ is characteristic. In view of the proof of Proposition 5.4, it is of interest to know when an automorphism of G/T_j (which can be assumed to have the form $(g, t + T_j) \mapsto (\alpha(g), \beta(t) + T_j)$ with $\alpha \in \mathrm{Aut}(P)$ and $\beta \in \mathrm{Aut}(T)$) lifts to an automorphism of G. Such automorphisms are closely related to *compatible pairs*, see [48, Page 55]: for $A \in \{T, T/T_j\}$ the group of compatible pairs $\mathrm{Comp}(P, A)$ consists of all $(\alpha, \beta) \in \mathrm{Aut}(P) \times \mathrm{Aut}(A)$ such that $\beta(a^g) = \beta(a)^{\alpha(g)}$ for all $g \in P$ and $a \in A$. It is easy to verify that every such pair yields an automorphism of $P \ltimes A$ via $(g, a) \mapsto (\alpha(g), \beta(a))$.

We now investigate when $(\alpha, \beta) \in \mathrm{Comp}(P, T/T_j)$ with $j \geq d$ can be lifted to an element in $\mathrm{Comp}(P, T)$. Here we consider the case $T_j = T_{yd} = p^y T$. Note that if $(\alpha, \beta) \in \mathrm{Comp}(P, A)$, then $\alpha \in \mathrm{Aut}(P)$ and $\beta \in \mathrm{Hom}_P(A, A_\alpha)$ where $A_\alpha = A$ is the P-module where $g \in P$ acts as $a \mapsto a^{\alpha(g)}$. Thus our question is: which elements of $\mathrm{Hom}_P(T/T_j, (T/T_j)_\alpha)$ lift to elements in $\mathrm{Hom}_P(T, T_\alpha)$? In the following we write $\mathbb{Z}_p^{a \times b}$ for the set of all $a \times b$ matrices over $\mathbb{Z}_p$.

Proposition 5.5. *Let $\alpha \in \mathrm{Aut}(P)$ and $T_{yd} = p^y T$ with $y \geq 1$. We can decompose*

$$\mathrm{Hom}_P(T/T_{yd}, (T/T_{yd})_\alpha) = L_{yd} \oplus N_{yd},$$

where $L_{yd} = \{t + T_{yd} \mapsto f(t) + T_{yd} \mid f \in \mathrm{Hom}_P(T, T_\alpha)\}$ are exactly the liftable homomorphisms, and the property $N_{yd} = 0$ or $N_{yd} \neq 0$ is independent of y. In particular, we have $N_{(u+1)d} = pN_{ud}$ for all large enough u.

Thus, *every* element in $\mathrm{Hom}_P(T/T_{yd}, (T/T_{yd})_\alpha)$ is liftable if and only if $N_{yd} = 0$; the detailed construction of N_{yd} is technical and only given in the proof.

Proof. Fix a basis of $T = \mathbb{Z}_p^d$ to identify $\mathrm{Aut}(T) = \mathrm{GL}_d(\mathbb{Z}_p)$ and $\mathrm{End}(T) = \mathbb{Z}_p^{d \times d}$. Let $P = \langle g_1, \ldots, g_m \rangle$ and let $\rho_1, \rho_2 : P \to \mathrm{GL}_d(\mathbb{Z}_p)$ be the two $\mathbb{Z}_p P$-module actions on T; write $T^{\{i\}}$ for the P-module T whose action is defined by ρ_i. Now define the $\mathbb{Z}_p$-linear map $\psi = \psi(\rho_1, \rho_2)$ from $\mathrm{End}(T)$ to $\mathbb{Z}_p^{d \times md}$ by the matrix

$$\psi(A) = \left[\; A\rho_1(g_1) - \rho_2(g_1)A \;\middle|\; \ldots \;\middle|\; A\rho_1(g_m) - \rho_2(g_m)A \; \right]$$

so that $\ker \psi = \mathrm{Hom}_P(T^{\{1\}}, T^{\{2\}})$, which is the group we are interested in.

Choosing the canonical $\mathbb{Z}_p$-basis of $\mathrm{End}(T) = \mathbb{Z}_p^{d \times d}$, we identify ψ with a $d^2 \times md^2$ matrix over $\mathbb{Z}_p$. Since $\mathbb{Z}_p$ is a principal ideal domain, there exist invertible matrices R and C

such the Smith-Normal-Form of ψ is

$$\mathrm{Snf}(\psi) = R\psi C = \left[\ \mathrm{diag}(\alpha_1, \ldots, \alpha_u, 0, \ldots, 0) \ \middle|\ 0\ \right] \in \mathbb{Z}_p^{d^2 \times md^2},$$

with $\alpha_1, \ldots, \alpha_u \neq 0$ and each $\alpha_i \mid \alpha_{i+1}$. Define $\mathfrak{m}(\psi) = (m_1, \ldots, m_u) \in \mathbb{Z}^u$ where each m_i is the largest p-power dividing α_i. Since the nonzero diagonal entries of $\mathrm{Snf}(\psi)$ are uniquely defined up to multiplication by elements of the unit group $\mathbb{Z}_p^*$,the vector $\mathfrak{m}(\psi)$ is uniquely defined by ψ.

Now define the same for $\bar{T} = T/p^yT$, that is, let $\bar{\psi} = (\bar{\rho}_1, \bar{\rho}_2)$, where each of the maps $\bar{\rho}_i : P \to \mathrm{GL}_d(\mathbb{Z}/p^y\mathbb{Z})$ is induced by ρ_i. In this case $\ker \bar{\psi} = \mathrm{Hom}_P(\bar{T}^{(1)}, \bar{T}^{(2)})$. Let $\mathrm{Snf}(\bar{\psi}) = \bar{R}\bar{\psi}\bar{C}$ with nonzero diagonal entries $\bar{\alpha}_1, \ldots, \bar{\alpha}_v$. Since $\mathrm{Snf}(\psi) \bmod p^y$ is also a Smith-Normal-Form of $\bar{\psi}$, we can assume that $\bar{R}\bar{\psi}\bar{C} = R\psi C \bmod p^y$.

Note that $\ker(R\psi C) = \langle e_{u+1}, \ldots, e_{d^2} \rangle$ where each e_i is the standard basis element with 1 in position i, thus

$$\mathrm{Hom}_P(T^{\{1\}}, T^{\{2\}}) = \ker \psi = \langle e_{u+1}R, \ldots, e_{d^2}R \rangle.$$

Similarly, $\alpha_i \bmod p^y \neq 0$ if and only if $y > m_i$, and so $\bar{R}\bar{\psi}\bar{C} = R\psi C \bmod p^y$ yields $\mathrm{Hom}_P(\bar{T}^{\{1\}}, \bar{T}^{\{2\}}) = \ker \bar{\psi} = L_{yd} \oplus N_{yd}$ where $L_{yd} = \langle e_{u+1}\bar{R}, \ldots, e_{d^2}\bar{R} \rangle$ and

$$N_{yd} = \langle p^{\max\{y-m_1,0\}} e_1 \bar{R}, \ldots, p^{\max\{y-m_u,0\}} e_u \bar{R} \rangle.$$

If each $m_i = 0$, then $N_{yd} = 0$ follows from $p^y\bar{R} = 0$. Conversely, suppose $N_{yd} = 0$. If there exists $m_i \geq y$, then $e_i\bar{R} \in N_{yd} \neq 0$, which is a contradiction, hence $y > m_i$ for all i. Since $\bar{R} = R \bmod p^y$ is invertible, $p \nmid \det(\bar{R})$ for all y, and so each $e_i\bar{R}$ has at least one entry not divisible by p. Since each $p^{y-m_i}e_i\bar{R} \in N_{yd} = 0$ by assumption, we deduce that each $m_i = 0$. The claim follows. □

5.2.2 Two special cases

We now discuss the isomorphism problem for special types of skeleton groups. Both the cases are motivated by [34] and generalises some results given there.

Cyclic point groups

We first consider space groups with cyclic point groups and show that in this case isomorphic skeleton groups always admit orbit isomorphisms. We start with a preliminary lemma.

Lemma 5.6. *Let $G = P \ltimes T$ be a uniserial p-adic space group where P has nilpotency class c and $\gamma_{c+1}(G) = T_k$. Let $\gamma, \gamma' : T \wedge T \to T_j$ with $j > \max\{k, d+1\}$ be surjective $\mathbb{Z}_p P$-module homomorphisms. If $C_P(T_k/T_j) = 1$, then every isomorphism $G_{\gamma,m} \to G_{\gamma',m}$ between skeleton groups maps $T_{\gamma,m}$ to $T_{\gamma',m}$.*

Proof. Let $S = G_{\gamma,m}$ and $N = T_j/T_m$. The proof of Corollary 4.9 shows $G/T_j \cong S/N$ and, if $|G/T_j| = p^u$, then $\gamma_{u-r+1}(S) = N$, where r is the coclass of G. Moreover, $T_k/T_j = \gamma_{c+1}(G/T_j) = \gamma_{c+1}(S/N)$, which yields $\gamma_{c+1}(S) = T_k/T_m$. Let C be the centraliser in S of $\gamma_{c+1}(S)/\gamma_{u-r+1}(S)$. By assumption, $C \cap P = 1$, so $C = T_{\gamma,m}$. □

Remark 5.7. At the end of the proof of [34, Lemma 5.8] it is claimed that a certain compatible pair of P and T/T_j lifts to a compatible pair of P and T. In view of Proposition 5.5 it is not clear to us why this is true. However, the statement of [34, Lemma 5.8] is covered by our Proposition 5.8.

Proposition 5.8. *Let $G = P.T$ be a uniserial p-adic space group with cyclic point group P. Let $G_{P^*,\gamma,m}$ and $G_{P^*,\gamma',m}$ be skeleton groups with $\gamma, \gamma' : T \wedge T \to T_j$ for some $j > d$. Every isomorphism between $G_{P^*,\gamma,m}$ and $G_{P^*,\gamma',m}$ is an orbit isomorphism, induced by some automorphism of G which satisfies* (5.1) *with $x = 0$.*

Proof. By [40, Lemma 11], for every $s \geq 1$ there is, up to isomorphism, a unique uniserial p-adic space group with cyclic point group of order p^s: We can assume that $G = P \ltimes T$ where $T = (\mathbb{Z}_p[\theta], +)$ for a primitive p^s-th root of unity θ over $\mathbb{Q}_p$, and $P = \langle \mu \rangle$ acts on T by multiplication by θ, see Example 3.15. The uniserial series of T has terms $T_i = (\theta - 1)^i T$ for all i, and each T_i is characteristic in G. In particular, $T_i = \gamma_{i+1}(G)$ for each $i \geq 1$, and so G has coclass s.

If $\alpha \in \mathrm{Aut}(G)$ satisfies (5.1) with $x = 0$, then $G_{\gamma,m} \cong G_{\gamma',m}$ by Lemma 5.1. Conversely, consider an isomorphism $\phi : G_{\gamma,m} \to G_{\gamma',m}$. We now apply Lemma 5.6: if $\mu^{(p^i)} \in P$ centralises T_1/T_j, then $(\theta^{(p^i)} - 1)t \in T_j$ for all $t \in T_1$, so $\theta^{p^i} - 1 \in T_{j-1}$. Since $T_j > pT$, this forces $\mu^{p^i} = 1$; it follows that $\phi(T_{\gamma,m}) = T_{\gamma',m}$. Proposition 5.4 now shows that ϕ induces an automorphism β of $G/T_j = P \ltimes T/T_j$ of the form $(\mu, t + T_j) \mapsto (\mu^k, \phi(t + T_j))$, where ϕ also denotes the induced automorphisms of P and T/T_j. Since $j > d$, Proposition 5.4 proves the claim once we have shown that β lifts to $\mathrm{Aut}(G)$. Recall that $t^{\phi(\mu)} = t^{(\mu^k)} = \theta^k t = \sigma_k(\theta)t$ for all $t \in T$. Write $\phi(1 + T_j) = v_0 + T_j$ for some $v_0 \in T$; note that $v_0 \in \mathcal{U}_{p^s}$ since otherwise ϕ would not be an automorphism of T/T_j. Together, if $i \geq 1$, then

$$\phi(\theta^i + T_j) = \phi(1^{(\mu^i)} + T_j) = \phi(1 + T_j)^{\phi(\mu^i)} = v_0 \sigma_k(\theta^i) + T_j;$$

this implies that $\phi(t + T_j) = v_0\sigma_k(t) + T_j$ for all $t \in T$. Now define $\Phi \in \mathrm{Aut}(T)$ by the map $t \mapsto v_0\sigma_k(t)$. Clearly, $\Phi(t^\mu) = \Phi(t)^{\phi(\mu)}$, and so $\alpha : (\mu, t) \mapsto (\phi(\mu), \Phi(t))$ is an automorphism of G. By construction, α induces β, so α is a lift of β. □

Some metacyclic point groups

The second case is motivated by [34, Theorem 6.8] and the gap we have identified in its proof, see Remark 5.13. As a slight generalisation, we consider $G = P \ltimes T$ for

$$P = \langle \mu, \sigma \rangle \quad \text{and} \quad T = (\mathbb{Z}_p[\theta], +)$$

where θ is a primitive p^s-th root of unity over $\mathbb{Q}_p$, and μ and σ are automorphisms of T such that $t^\mu = \theta t$ is multiplication by θ, and $t^\sigma = \sigma_v(t)$ is the Galois automorphism defined by $\theta \mapsto \theta^v$. We assume that $\theta^\sigma \neq \theta$ since otherwise P is cyclic; we also assume that P is a p-group. Note that T has dimension $d = p^{s-1}(p-1)$ and G is a uniserial p-adic space group, with uniserial series terms $T_j = (\theta - 1)^j T$ for all $j \geq 0$. Suppose $|\sigma| = p^i$ with $1 \leq i \leq s-1$, so that P has order p^{i+s} and nilpotency class $\lceil s/(s-i) \rceil \leq s$. Since the Galois group of $\mathbb{Q}_p(\theta)$ is cyclic and $|\sigma_{1+p^{s-i}}| = p^i$, we can assume $v = 1 + p^{s-i}$. Note that σ fixes $\eta = \theta^{(p^i)}$ and, in fact, $Z(P) = \langle \mu^{(p^i)} \rangle$ has order p^{s-i}. It follows from [2, Theorem 3.1] that $|\mathrm{Aut}(P)| = (p-1)p^{s+2i-1}$ if $2i \leq s$, and $|\mathrm{Aut}(P)| = (p-1)p^{2s-1}$ otherwise. The previous notation is retained in the remainder of this section. We note that in [34, Theorem 6.3] the case $(p, s, i) = (3, 2, 1)$ is considered, hence the following lemma applies.

Lemma 5.9. *If $2i \leq s$ then $\mathrm{Aut}(G)$ maps onto $\mathrm{Aut}(P)$.*

Proof. Recall from Section 4.1 that the generator σ_k of the Galois group of $\mathbb{Q}_p(\theta)$ induces automorphisms of G and P of order $p^{s-1}(p-1)$. Since $\langle \sigma_k \rangle \cap P = \langle \sigma \rangle$ and $|Z(P)| = p^{s-i}$, the order of $J = \langle \sigma_k, \mathrm{Inn}(P) \rangle \leq \mathrm{Aut}(P)$ is $(p-1)p^{s+i-1}$. Clearly, J is induced by automorphisms of G. Considering σ and μ as permutations of $\{1, \theta, \ldots, \theta^{p^s-1}\}$, both μ and $\sigma\mu$ are p^s-cycles, and $\mu^w = \sigma\mu$ for the permutation w which maps each θ^j to $\theta^{1+v+\ldots+v^{j-1}}$. Our claim is that $\langle w, \sigma_k, \mathrm{Inn}(P) \rangle = \mathrm{Aut}(P)$ is induced by $\mathrm{Aut}(G)$. We first prove $\sigma^w = \sigma$. Note that $w\sigma$ and σw send θ^j to $e_1 = \theta^{v+v^2+\ldots+v^j}$ and $e_2 = \theta^{1+v+\ldots+v^{jv-1}}$, respectively. Now $vj - 1 > j$, so $e_1 = e_2$ follows if $y = 1 + v^{j+1} + v^{j+2} + \ldots + v^{jv-1} \equiv 0 \bmod p^s$. Since $i \leq s/2$, we have $v^a \equiv 1 + ap^{s-i} \bmod p^s$ for all $a \geq 0$, thus $y \equiv j(v-1) + ((j+1) + (j+2) + \ldots + (jv-1))\, p^{s-i} \bmod p^s$, and $y \equiv 0 \bmod p^s$ follows from evaluating this sum. Thus, conjugation by w induces an automorphism α of P which maps μ and σ to $\sigma\mu$ and σ, respectively. Since $\mu^{(w^j)} = \sigma^j\mu$ for all j, this implies that $\langle w, \sigma_k, \mathrm{Inn}(P) \rangle$ has order $(p-1)p^{s+2i-1}$, and therefore equals $\mathrm{Aut}(P)$. We now show

that α is induced by an automorphism of G. Recall that w permutes $\{1, \theta, \ldots, \theta^{p^s-1}\}$. Since w maps each θ^j to $\theta^{1+v+\ldots+v^{j-1}}$, we have

$$(\theta^{jp^{s-1}})^w = \theta^{1+v+\ldots+v^{jp^{s-1}-1}} = \theta^{jp^{s-1}}$$

for all $0 \leq j \leq p-1$. Since T is generated by $\{1, \theta, \ldots, \theta^{p^s-1}\}$ subject to the relation $\theta^{p^{s-1}(p-1)} + \theta^{p^{s-1}(p-2)} + \ldots + \theta^{p^{s-1}} + 1 = 0$, this proves that w defines an automorphism β of T. By construction, (α, β) is a compatible pair of P and T, hence it defines an isomorphism of G inducing α. □

For the following lemma recall the definition of i, s, η from above.

Lemma 5.10. *Let $y \in \mathbb{Z}$, $\ell \in \{0, 1, \ldots, p^i - 1\}$, and $j > d$.*

a) *If $\theta^y \neq 1$, then $\theta^y - 1 \notin T_{p^{s-1}+1}$.*

b) *If $w = w_0 + \theta w_1 + \ldots + \theta^\ell w_\ell \in T_j$ with each $w_j \in \mathbb{Z}_p[\eta]$, then each $w_a \in T_{j-p^i+1}$.*

Proof. a) We can assume $1 \leq j < p^s$, and writing $j = cp^u$ with $p \nmid c$ and $u \leq s-1$ yields $\theta^i - 1 = (\theta^{(p^u)} - 1)(1 + \theta^{(p^u)} + \theta^{2(p^u)} + \ldots + \theta^{(c-1)(p^u)})$. The second factor is congruent c modulo T_1, hence lies in $T \setminus T_1$. By the binomial formula, the first factor satisfies $\theta^{(p^u)} - 1 \equiv (\theta - 1)^{(p^u)} \bmod pT$. Thus $\theta^j - 1 \in T_{p^u} \setminus T_{p^u+1}$.

b) Every $w \in T$ admits unique $w_0, \ldots, w_{p^i-1} \in \mathbb{Z}_p[\eta]$ such that

$$w = w_0 + \theta w_1 + \ldots + \theta^{p^i-1} w_{p^i-1}.$$

The proof of a) yields $\eta - 1 \in T_{p^i} \setminus T_{p^i-1}$, so $T_j = (\eta-1)^x T_y$ for some $0 \leq y \leq p^i - 1$ and we can write $w = (\eta-1)^x w'$ for some $w' \in T_y$. Decomposing w' as above implies that each $w_a = (\eta-1)^x w'_a \in T_{xp^i} \leq T_{j-p^i+1}$, as claimed. □

Definition 5.11. For $n \in \mathbb{Z}$ with $n \not\equiv 0, 1 \bmod p$ let $\nu_n : T \wedge T \to T$ be defined by

$$\nu_n(t \wedge s) = \sigma_n(t)\sigma_{1-n}(s) - \sigma_n(s)\sigma_{1-n}(t).$$

A $\mathbb{Z}_p P$-homomorphism $\gamma : T \wedge T \to T$ is called a *1-parameter homomorphism* if $\gamma = z\nu_n$ for some $z \in T$ and $n \in \mathbb{Z}$.

All skeleton groups in $\mathcal{G}(p, r)$ for $(p, r) \in \{(3, 1), (3, 2), (5, 1)\}$ are defined by 1-parameter homomorphisms. In these cases, a solution to the isomorphism problem of skeleton groups is within reach, cf. [34]. For skeleton groups defined by non-1-parameter homomorphisms, the isomorphism problem is much more complicated, even for p-groups of maximal class (cf. the analysis in [18, 20]). This is the reason why the next result focuses

on 1-parameter homomorphisms. This proposition closes the gap we have identified in the proof of [34, Theorem 6.8], see Remark 5.13.

Proposition 5.12. *Let $G = P \ltimes T$ be as above with $2i \leq s$. Let $G_{\gamma,m}$ and $G_{\gamma',m}$ be skeleton groups with $\gamma, \gamma' : T \wedge T \to T_j$ onto such that $d < j \leq m \leq 2j - d$. If γ' is a 1-parameter homomorphism and $G_{\gamma,m} \cong G_{\gamma',m}$, then there is also an orbit isomorphism, induced by some automorphism of G satisfying* (5.1) *with $x = 0$.*

Proof. Write $S = G_{\gamma,m}$. Let c be the nilpotency class of P, so $\gamma_{c+1}(S) = T_k/T_m$ with $k \leq s$ and $T_j/T_m = \gamma_{c+1+j-k}(S)$, cf. the proof of Lemma 5.6. Let C be the centraliser in S of T_k/T_j; we show that $P \cap C = 1$. If $c = \sigma^a\mu^b \in P \cap C$, then $\theta^b\sigma_{v^a}(t) - t \in T_j$ for all $t \in T_k$. For $t = (\theta - 1)^y$ with $k \leq y \leq j$ this yields $\theta^b(1 + \theta + \ldots + \theta^{v^a-1})^y - 1 \in T_{j-i}$. Subtracting the equations for $y = k$ and $y = k + 1$ eventually forces $\theta^{v^a-1} - 1 \in T_{j-k}$. Since $j - k > d - s \geq p^{s-1}$, Lemma 5.10a) yields $\theta^{v^a-1} = 1$, and so $c = \mu^b$. This implies $\theta^b - 1 \in T_{j-k}$, and $\theta^b = 1$ again by Lemma 5.10a). This proves $c = 1$, and so $P \cap C = 1$ and $C = T_{\gamma,m}$.

Thus, if $\phi : G_{\gamma,m} \to G_{\gamma',m}$ is an isomorphism, then $\phi(T_{\gamma,m}) = T_{\gamma',m}$. In particular, there exist a map $\phi' : P \to T$ and $\Phi \in \mathrm{Aut}(T)$ such that ϕ maps $(h, 0 + T_m)$ and $(1, t + T_m)$ to $(\phi(h), \phi'(h) + T_m)$ and $(1, \Phi(t) + T_m)$, respectively; here we identify ϕ with the induced automorphism of P. Now Proposition 5.4 shows that this yields an automorphism $\beta : (h, t + T_j) \mapsto (\phi(h), \Phi(t) + T_j)$ of G/T_j, with $\Phi(t^h) \equiv \Phi(t)^{\phi(h)} \bmod T_j$ for all $h \in P$ and $t \in T$.

By Lemma 5.9, the automorphism ϕ is induced by some $\alpha \in \mathrm{Aut}(G)$. Since $\alpha(T) = T$, we can assume that α maps (h, t) to $(\phi(h), \alpha(t))$ with $\alpha(t^h) = \alpha(t)^{\phi(h)}$ for all $h \in P$ and $t \in T$, which yields an automorphism $\beta_1 : (h, t + T_j) \mapsto (\phi(h), \alpha(t) + T_j)$ of G/T_j. Note that $\beta_2 = \beta \circ \beta_1^{-1}$ is an automorphism of G/T_j of the form $(h, t + T_j) \mapsto (h, \tau(t) + T_j)$ for some $\tau \in \mathrm{Aut}(T)$ with $\tau(t^h) \equiv \tau(t)^h \bmod T_j$ for all $h \in P$ and $t \in T$. Since $\mu \in P$ acts by multiplication by θ on T, it follows that $\tau(t) \equiv ut \bmod T_j$ for some unit $u \in \mathcal{U}_{p^s}$; since $\sigma \in P$, it follows that $\sigma(u) \equiv u \bmod T_j$. In conclusion, the automorphism $\beta = \beta_2 \circ \beta_1$ of G/T_j induced by the isomorphism ϕ is of the form

$$\beta : (h, t + T_j) \to (\phi(h), \Phi(t) + T_j) = (\phi(h), u\alpha(t) + T_j).$$

In general, $\sigma(u) \neq u$ and β cannot be lifted to $\mathrm{Aut}(G)$. Motivated by [34, Lemma 6.7], we now modify β in a suitable way. First, we examine the unit u.

Write $u = \sum_{k=0}^{p^i-1} \theta^k u_k$ with each $u_k \in \mathbb{Z}_p[\eta]$ fixed by σ. Now $\sigma(u) - u \in T_j$ translates to $\sum_{k=1}^{p^i-1} \theta^k u_k(\theta^{kp^{s-i}} - 1) \in T_j$, so $u_k(\theta^{kp^{s-i}} - 1) \in T_{j-p^i+1}$ for each $k \geq 1$ by Lemma 5.10. The proof of Lemma 5.10a) yields $\theta^{kp^{s-i}} - 1 \notin T_{p^{s-1}+1}$ for $0 < k < p^i$, so

$u_k \in T_{j-p^i-p^{s-1}+1} \leq T_{j-d}$ for $k \geq 1$. Since $j > d$ and u is a unit, this forces $u_0 \in T \setminus T_1$. Thus u_0 is a unit and $u = u_0 v$ for $v = 1 + (\sum_{k=1}^{p^i-1} \theta^k u_k) u_0^{-1} \in 1 + T_{j-d}$. Since $\sigma(u_0) = u_0$ and $\alpha(t^g) = \alpha(t)^{\phi(g)}$ for all $t \in T$ and $g \in P$, we obtain an automorphism

$$\beta' : G \to G, \quad (h, t) \mapsto (\phi(h), u_0 \alpha(t)).$$

We now prove that β' satisfies (5.1) with $x = 0$; then Lemma 5.1 proves the claim. By assumption $\gamma' = z\nu_n$ for some $z \in T$ and $n \in \mathbb{Z}$, which implies $\gamma'(us \wedge ut) = u\rho_n(u)\gamma'(s \wedge t)$ with $\rho_n(u) = u^{-1}\sigma_n(u)\sigma_{n-1}(u)$ for all $s, t \in T$. Since ϕ is an isomorphism, a direct calculation shows that

$$u\alpha(\gamma(t \wedge s)) \equiv \gamma'(u\alpha(t) \wedge u\alpha(s)) \equiv u\rho_n(u)\gamma'(\alpha(t) \wedge \alpha(s)) \bmod T_m.$$

Since $\rho_n : \mathcal{U}_{p^s} \to \mathcal{U}_{p^s}$ is a homomorphism, γ' has image T_j, the unit u satisfies $u = u_0 v$ with $v \in 1 + T_{j-d}$, and $m \leq 2j - d$, the above equivalence yields

$$u_0\alpha(\gamma(t \wedge s)) \equiv u_0\rho_n(u_0)\gamma'(\alpha(t) \wedge \alpha(s)) \equiv \gamma'(u_0\alpha(t) \wedge u_0\alpha(s)) \bmod T_m.$$

This proves that β' satisfies (5.1); as explained above, this completes the proof. □

As said above, when proving the above results we identified and corrected some gaps in [34]; the following remark provides details.

Remark 5.13. In [34, Theorem 6.8] the following situation is considered; we partly adapt the notation of that theorem. Let $G = G_{j-3}$ be a non-split uniserial 3-adic space group of coclass 2 with split supergroup $H = H_{j-3} = P \ltimes T$. We have $P = \langle \mu, \sigma_4 \rangle$ and $T = \mathbb{Z}_3[\theta]$ as above, for a primitive 9-th root of unity θ. In particular, $\mathrm{Aut}(H)$ maps onto $\mathrm{Aut}(P)$. Let $A = H_{j-3,\gamma,m}$ and $B = H_{j-3,\gamma',m}$ be skeleton groups for H, and let $\phi : A \to B$ be an isomorphism. In the proof of [34, Theorem 6.8] it is said that, since $\mathrm{Aut}(H)$ maps onto $\mathrm{Aut}(P)$, one can assume that ϕ acts as the identity on the common quotient P of A and B, respectively. We claim that this assumption cannot be made, for two reasons.

First, in GAP [39], we have constructed two such skeleton groups which are isomorphic, but which do not admit an isomorphism between them which acts as the identity on the common quotient P. These two skeleton groups $A = H_{j-3,\gamma_1,13}$ and $B = H_{j-3,\gamma_2,13}$ are constructed via 1-parameter homomorphisms $\gamma_1, \gamma_2 : T \wedge T \to T_9$ defined by $\gamma_i = t_i(\theta^3 - 1)^3\nu_2$ with $t_1 = -2 + 3\theta^3$ and $t_2 = 1 + \theta^3$, respectively. We constructed an explicit isomorphism ϕ between these skeleton groups, which acts on P as $\alpha : (\mu, \sigma_4) \mapsto (\sigma_4^2\mu^8, \sigma_4\mu^6)$, and we have verified there is no automorphism of B inducing α on P. Thus the claim in the proof of [34, Theorem 6.8] is not correct.

A second line of argument (not presented in the proof of [34, Theorem 6.8]) is to redefine B with respect to the point group $\phi(P) \leq B$. Then the isomorphism between A and B would act as the identity on the common quotient isomorphic to P. However, it is not clear whether this construction will allow us to lift the isomorphism ϕ to an automorphism of $H = P \ltimes T$, which is the ultimate aim in the proof of [34, Theorem 6.8].

We note that these problems in the proof of [34, Theorem 6.8] are solved with our slightly more general Proposition 5.12.

Chapter 6

Orbit Isomorphic Skeleton Groups

In this chapter, p is an odd prime. We use Notation 3.19 and consider a split space group $G = P \ltimes T$ of dimension d and coclass r, with point group P, translation subgroup T, and extended uniserial series $\ldots > T_{-1} > T_0 = T > T_1 > \ldots$. Let $\mathcal{T}_G$ be the coclass tree in $\mathcal{G}(p, r)$ defined by G; its branches are labelled such that $\mathcal{B}_j$ has root $G_j = P \ltimes T/T_j$. The shaved branch $\mathcal{B}_j[k]$ is the subgraph of $\mathcal{B}_j$ consisting of the groups of depth at most k in $\mathcal{B}_j$. For any $j \geq 1$, we write

$$H_j = \mathrm{Hom}_P(T \wedge T, T_j)$$

and

$$L_j = \{\gamma \in H_j \mid \gamma \text{ is surjective}\}.$$

Let $\gamma \in L_j$ with $\gamma(T_j \wedge T) = T_k$ where $k \geq 2j - d$. For every m with $j \leq m \leq 2j - d$ we have defined the skeleton group $G_{\gamma,m} = P \ltimes T_{\gamma,m}$, see Chapter 4. Recall that $G_{\gamma,m}$ lies at depth $m - j$ in $\mathcal{B}_j$. As before, whenever considering a skeleton group $G_{\gamma,m}$, we implicitly assume that all parameters are chosen appropriately, that is, if $\gamma(T \wedge T) = T_j$ and $\gamma(T_j \wedge T) = T_k$, then $j \leq m \leq 2j - d$.

The skeleton groups in $\mathcal{B}_j$ induce a subgraph $\mathcal{S}_j$ of depth $2j - d$. By $\mathcal{S}_j[k]$ we denote the subgraph of $\mathcal{S}_j$ consisting of all skeleton groups in depth at most k for $k \leq 2j - d$. In Chapter 5 we investigated the isomorphism problem of skeleton groups and showed in Lemma 5.1 that if two homomorphisms γ, γ' satisfy $\alpha \circ \gamma \equiv \gamma' \circ (\alpha \wedge \alpha) \bmod H_m$ for some $\alpha \in \mathrm{Aut}(G)$, then $G_{\gamma,m} \cong G_{\gamma',m}$. The converse is no always true, but holds in special cases, for example, for the skeleton groups of coclass 1. The latter has been investigated in [17, 19]. The next result follows directly from Lemma 5.1.

Lemma 6.1. *Every $\phi \in \mathrm{Aut}(G)$ acts on $\gamma \in H_j$ via $\gamma \mapsto \gamma^\phi$, defined by*

$$\gamma^\phi(t \wedge s) = \phi^{-1}(\gamma(\phi(t) \wedge \phi(s))). \tag{6.1}$$

If γ is surjective, then so is γ^ϕ.

The action defined in (6.1) induces an action of $\mathrm{Aut}(G)$ on L_j. Note that $\gamma \equiv \gamma' \bmod H_m$ if and only if $\gamma - \gamma' \in H_m$. For $V \leq \mathrm{Aut}(G)$, we write

$$\mathrm{Stab}_V(\gamma + H_m) = \{\alpha \in V \mid \gamma^\alpha \equiv \gamma \bmod H_m\}.$$

Now Lemma 5.1 can be rephrased as follows.

Lemma 6.2. *Let $\gamma, \gamma' \in L_j$. If there exists $\beta \in \mathrm{Aut}(G)$ such that $\gamma^\beta \equiv \gamma' \bmod H_m$ then $G_{\gamma,m} \cong G_{\gamma',m}$.*

Recall that two skeleton groups are orbit isomorphic if there is an isomorphism as in Lemma 6.2, induced by the automorphism group of the associated space group.

Lemma 6.2 is a partial solution to the isomorphism problem of split skeleton groups; a complete solution can be obtained in some special cases, see Chapter 5. However there are examples where the converse of Lemma 6.2 is not true, see [34].

Note that if the converse of Lemma 6.2 holds, the skeleton subgraph (in the coclass tree associated with G) is completely determined by the structure of G: the ingredients for constructing skeleton groups are P, T, and homomorphisms $T \wedge T \to T$, and their isomorphism problem can be solved by considering the action of $\mathrm{Aut}(G)$.

6.1 Periodicities in skeleton graph

In this section we study how the converse of Lemma 6.2 improves some known periodicity results; it generalises some results for $\mathcal{G}(p,1)$ obtained in [17, 19].

Hypothesis 6.3. *In this section we assume that G is chosen such if two skeleton groups (defined in $\mathcal{T}_G$) are isomorphic, then they are also orbit isomorphic.*

We have proved in Chapter 5 that Hypothesis 6.3 holds whenever G has a cyclic point group; this includes the prominent example $\mathcal{G}(p,1)$. Assuming Hypothesis 6.3, the condition given in Lemma 6.2 is in fact both necessary and sufficient for solving the isomorphism problem of skeleton groups.

The periodicity of type I, see Section 2.2, shows that for any fixed k and all large enough n, there is a graph isomorphism $\mathcal{B}_n[k] \to \mathcal{B}_{n+d}[k]$; recall that d is the dimension

of the space group G. As discussed in Section 2.2.1, this result was later improved by Dietrich [19] for groups of maximal class. This motivated us to investigate the periodicity of type I under Hypothesis 6.3. We establish the following improvement.

Theorem 6.4. *Under the assumption of Hypothesis 6.3 the following holds. For all large enough j, we have $\mathcal{S}_j \cong \mathcal{S}_{j+d}[j-d]$ as rooted trees; here d is the dimension of the associated space group.*

Proof. From Section 4.4 we find that for $6d < j \leq m \leq 2j-d$, a complete list of skeleton groups at depth $m-j$ in $\mathcal{B}_j$ is given by

$$S_{j,m} = \{G_{\gamma,m} \mid \gamma \in L_j\}.$$

Multiplication by p defines a bijection $L_j \to L_{j+d}$. Since $j+d \leq m+d \leq 2j \leq 2(j+d)-d$, we have

$$S_{j+d,m+d} = \{G_{p\gamma,m+d} \mid \gamma \in L_j\}.$$

Clearly $(p\gamma)^\alpha = p(\gamma^\alpha)$ for $\alpha \in \mathrm{Aut}(G)$. Hence in view of Hypothesis 6.3 we have the following using Lemmas 5.1 and 6.2.

$$G_{\gamma,m} \cong G_{\gamma',m} \iff G_{p\gamma,m+d} \cong G_{p\gamma',m+d}.$$

This proves the existence of a bijection between the isomorphism types of the skeleton groups at depth e in $\mathcal{B}_j$ and at depth e in $\mathcal{B}_{j+d}$, respectively, for all $e \leq j-d$. The parent of $G_{\gamma,m}$ in $\mathcal{B}_j$ is $G_{\gamma,m-1}$ for $m > j$; this also implies that the above bijection induces a graph isomorphism from $\mathcal{S}_j$ to $\mathcal{S}_{j+d}[j-d]$; recall that $\mathcal{S}_j$ has depth $j-d$. □

We now describe why Theorem 6.4 is a significant improvement over the periodicity of type I as described in [35]: It is shown in [35] that, for large enough j, one can embed $\mathcal{B}_j[e_j]$ into $\mathcal{B}_{j+d}$ where e_j is approximately $j/6d$. In contrast, Theorem 6.4 shows one can embed the *whole* skeleton tree $\mathcal{S}_j$ (of depth $j-d$) into $\mathcal{B}_{j+d}$, such that $\mathcal{S}_j \cong \mathcal{S}_{j+d}[j-d]$.

6.2 Skeleton groups with cyclic point group

Motivated by the skeleton groups of maximal class, see[20], we here investigate p-adic uniserial space groups with cyclic point groups. It follows from [40, Lemma 11] that every such space group is split and uniquely determined, up to isomorphism, by the size of its point group; thus, the following convention covers the general case of space groups with cyclic point groups.

Notation 6.5. We assume that $G = P \ltimes T$ is a split space group whose point group P is cyclic of order p^s, generated by g. If θ is a primitive p^s-th root of unity, then we can assume that $T = (\mathbb{Z}_p[\theta], +)$ whose uniserial series has terms $T_i = (\theta - 1)^i T = \mathfrak{p}^i$; see Chapter 3 for details. Recall that T has dimension $d_s = p^{s-1}(p-1)$. We denote the unit group of the ring $\mathbb{Z}_p[\theta]$ by $\mathcal{U}_{p^s}$, and write $\mathcal{U}_{p^s,i} = 1 + \mathfrak{p}^i$ for all $i > 0$, with $\mathcal{U}_{p^s,0} = \mathcal{U}_{p^s}$, see Section 4.1 for details.

The space group associated with the coclass tree of $\mathcal{G}(p, 1)$ is obtained by taking $s = 1$.

6.2.1 Homomorphisms from $T \wedge T$

To get a better understanding of skeleton groups it is important to study the set of parametrising homomorphisms. Let $K = \mathbb{Q}_p[\theta]$ and recall that $\sigma_a \in \mathrm{Aut}(K)$ is defined by $\theta \mapsto \theta^a$, see Section 4.1.2. The following is [53, Theorem 11.4.1].

Theorem 6.6. *For $a \not\equiv 0, 1 \bmod p$ define $\nu_a : K \wedge K \to K$ by*

$$\nu_a(x \wedge y) = \sigma_a(x)\sigma_{1-a}(y) - \sigma_a(y)\sigma_{1-a}(x). \tag{6.2}$$

Then $\{\nu_a \mid 2 \leq a \leq \frac{1}{2}(p^s - 1), a \not\equiv 0, 1 \bmod p\}$ is a K-basis of $\mathrm{Hom}_{\mathbb{Q}_p P}(K \wedge K, K)$.

Remark 6.7. The image of $T \wedge T$ under ν_a lies inside T, hence we can consider the restriction $\nu_a : T \wedge T \to T$ without any ambiguity.

We now concentrate on the structure of the homomorphisms from $T \wedge T$ to T. In the following theorem, we first find how $T \wedge T$ is generated as a $\mathbb{Z}_p P$-module; this is motivated by [53, Proposition 8.3.5]. Recall that $\theta + \ldots + \theta^{p^s-1} = -1$.

Theorem 6.8. *The $\mathbb{Z}_p P$-module $T \wedge T$ is the direct sum of a free $\mathbb{Z}_p P$-module of rank $\frac{1}{2}(p^s - 2p^{s-1} - 1)$ generated by $\{1 \wedge \theta^i \mid p^{s-1} + 1 \leq i \leq (p^s - 1)/2\}$ and a free $\mathbb{Z}_p$-module generated by $z = \sum_{0 \leq i < k < (p^s-1)} \theta^i \wedge \theta^k$.*

Proof. We know that $W = \{\theta^i \wedge \theta^k \mid 0 \leq i < k < d_s\}$ freely generates $T \wedge T$ as $\mathbb{Z}_p$-module. Further, $\theta^i \wedge \theta^k = (1 \wedge \theta^{k-i})^{g^i}$ and $1 \wedge \theta^k = -(1 \wedge \theta^{p^s-k})^{g^k}$ for $0 \leq i < k < p^s$. Since $p^s - x \leq (p^s - 1)/2$ whenever $x > (p^s - 1)/2$, we have that $T \wedge T$ is generated by $B' = \{1 \wedge \theta, \ldots, 1 \wedge \theta^{(p^s-1)/2}\}$ as a $\mathbb{Z}_p P$-module.

Now for each $p^{s-1} + 1 \leq i \leq (p^s - 1)/2$, define B_i as the 1-dimensional $\mathbb{Z}_p P$-submodule of $T \wedge T$ generated by $1 \wedge \theta^i$. Also define $B_1 = \{cz \mid c \in \mathbb{Z}_p\}$ which is a 1-dimensional $\mathbb{Z}_p$-submodule of $T \wedge T$. We observe that for $p^{s-1} + 1 \leq i \leq (p^s - 1)/2$, as a $\mathbb{Z}_p$-module of B_i is generated by

$$V_i = \{1 \wedge \theta^i, \theta \wedge \theta^{i+1}, \ldots, \theta^{d_s - i} \wedge \theta^{d_s}, 1 \wedge \theta^{d_s - i + 1}, \theta \wedge \theta^{d_s - i + 2}, \ldots, \theta^{i-1} \wedge \theta^{d_s}\}.$$

Let V be the union of all such V_i and let $B = V \cap W$ which is the subset of V omitting θ^{d_s}. Take a $\mathbb{Z}_p$-linear combination in V, say $x = \sum_{v\in V} a_v v$ and rewrite it as

$$x = \sum_{v\in B} a_v v + \sum_{m=1}^{d_s - p^{s-1}-1} b_m(\theta^m \wedge \theta^{d_s})$$

for some $b_m \in \mathbb{Z}_p$. Observe that $\theta^{np^{s-1}} \wedge \theta^m \in V_{|m-np^{s-1}|}$ for $1 \le m \le d_s - p^{s-1} - 1$ and $0 \le n \le p-2$ we have $|m - np^{s-1}| \in \{p^{s-1}+1, \ldots, (p^s-1)/2\}$. Suppose now $X_m = \{n \mid 0 \le n \le p-2, |m-np^{s-1}| \in \{1, 2, \ldots, p^{s-1}\}\}$ and consider the $\mathbb{Z}_p$-submodule $\hat{B} = \langle B\rangle_{\mathbb{Z}_p}$ generated by B. Thus we have

$$\theta^m \wedge \theta^{d_s} \equiv (-\theta^m) \wedge (\sum_{n\in X_m} \theta^n) \bmod \hat{B}. \tag{6.3}$$

If $x = 0$, we use (6.3) to deduce $\sum_{m=1}^{d_s-p^{s-1}-1} b_m(-\theta^m) \wedge (\sum_{n\in X_m} \theta^n) \in \hat{B}$, so each $b_m = 0$ and this implies $a_v = 0$ for all $v \in B$ since W is a free generating set. Hence $\hat{V} = \langle V\rangle_{\mathbb{Z}_p}$ is freely generated by V as $\mathbb{Z}_p$-module and hence $\hat{V}$ is freely generated by the set $\{1 \wedge \theta^i \mid p^{s-1}+1 \le i \le (p^s-1)/2\}$ as a $\mathbb{Z}_pP$-module.

Finally from the definition of $\hat{B}$, we have $\theta^i \wedge \theta^{i+n} \equiv 1 \wedge \theta^n \bmod \hat{B}$ for $n \in \{1, 2, \ldots, p^{s-1}\}$ and $0 \le i \le n-1$. Also, z can be written

$$z = \sum_{i=1}^{p^{s-1}} (1 \wedge \theta^i)^{1+g+\ldots+g^{p^{s-1}-i}} + \sum_{\substack{0\le i<k<(p^s-1)\\ k\ge p^{s-1}+1}} \theta^i \wedge \theta^k.$$

Hence $z \equiv (1 \wedge \theta^n) \bmod \hat{V}$ for $n \in \{1, 2, \ldots, p^{s-1}\}$. Recall that $T \wedge T$ is generated by $\{1 \wedge \theta, \ldots, 1 \wedge \theta^{p^s-1}, 1 \wedge \theta^{p^{s-1}+1}, \ldots, 1 \wedge \theta^{(p^s-1)/2}\}$ as a $\mathbb{Z}_pP$ module. Hence $\{z\} \cup V$ generates $T \wedge T$ as $\mathbb{Z}_p$-module. Also we note that $cz \notin \hat{V}$ for all $c \in T \setminus \{0\}$. Hence $\hat{V} \cap B_1 = \{0\}$. This completes the proof. □

Lemma 6.9. *The element z of Theorem 6.8 is fixed under the action of P.*

Proof. This follows from

$$\begin{aligned} z^g &= \sum_{0\le i<k<(p^s-1)} \theta^{i+1} \wedge \theta^{k+1} \\ &= \sum_{0\le i<k<(p^s-1)-1} \theta^{i+1} \wedge \theta^{k+1} + \sum_{1\le i\le(p^s-1)-1} \theta^i \wedge \theta^{(p^s-1)} \\ &= \sum_{1\le i<k<(p^s-1)} \theta^i \wedge \theta^k + (\sum_{1\le i\le p^s-2} \theta^i) \wedge \theta^{(p^s-1)} \end{aligned}$$

$$
\begin{aligned}
&= \sum_{1\le i<k<(p^s-1)} \theta^i \wedge \theta^k + (-1-\theta^{p^s-1}) \wedge \theta^{(p^s-1)} \\
&= \sum_{1\le i<k<(p^s-1)} \theta^i \wedge \theta^k + 1 \wedge (-\theta^{p^s-1}) \\
&= \sum_{1\le i<k<(p^s-1)} \theta^i \wedge \theta^k + 1 \wedge (\sum_{1\le i\le p^s-2} \theta^i) \\
&= \sum_{0\le i<k<(p^s-1)} \theta^i \wedge \theta^k \\
&= z
\end{aligned}
$$

□

Since both $T \wedge T$ and T are $\mathbb{Z}_p$-modules of finite rank, every homomorphism $T \wedge T \to T$ and $T \wedge T \to T/T_e$ (for any e) is a $\mathbb{Z}_p$-module homomorphism; see Remark 3.3. Since the only fixed point of T under the action of P is 0, Lemma 6.9 shows that every P-homomorphism $T \wedge T \to T$ must map z to 0. Therefore Theorem 6.8 shows that every P-homomorphism $T \wedge T \to T$ is uniquely determined by its values on $1 \wedge \theta^i$ for $i \in \{p^{s-1}+1, \ldots, (p^s-1)/2\}$. Since the elements in T/T_e fixed by $g \in P$ are precisely T_{e-1}/T_e, the image of z under a P-homomorphism $T \wedge T \to T/T_e$ lies in the subgroup generated by $\hat{z}_e = (\theta-1)^{e-1}+T_e$. The following results are motivated from [53, Chapter 8] where the case $s = 1$ has been discussed. We denote by $\delta_{i,k}$ the Kronecker delta with $\delta_{i,k} = 1$ if $i = k$ and $\delta_{i,k} = 0$ otherwise.

Definition 6.10. For $i, k \in \{p^{s-1}+1, \ldots, (p^s-1)/2\}$ and any $e > 0$, we define P-homomorphisms

$$f_k : T \wedge T \to T \quad \text{and} \quad \tilde{f}_k : T \wedge T \to T/T_e$$

by $f_k(1 \wedge \theta^i) = \delta_{i,k}$ and $f_k(z) = 0$, and $\tilde{f}_k = \pi \circ f_k$, where $\pi : T \to T/T_e$ is the projection. Let $\tilde{f}_1 : T \wedge T \to T/T_e$ be the P-homomorphism defined by $\tilde{f}_1(1 \wedge \theta^i) = 0$ and $\tilde{f}_1(z) = \hat{z}_e$.

Since $\mathbb{Z}_p[\theta]$ is abelian, $\mathrm{Hom}_P(T \wedge T, T)$ is a $\mathbb{Z}_p[\theta]$-module via $(f^c)(x) = cf(x)$ for all $c \in \mathbb{Z}_p[\theta]$, $x \in T \wedge T$ and $f \in \mathrm{Hom}_P(T \wedge T, T)$. The next two results are corollaries to Theorem 6.8.

Corollary 6.11. *As $\mathbb{Z}_p[\theta]$-module, H_0 is generated by $\{f_k \mid p^{s-1}+1 \le k \le (p^s-1)/2\}$.*

Corollary 6.12. $\mathrm{Hom}_P(T \wedge T, T/T_e)$ *is a direct sum of $\frac{1}{2}(p^s - 2p^{s-1} - 1)$ summands isomorphic to T/T_e, generated by $\tilde{f}_k$ for $p^{s-1}+1 \le k \le (p^s-1)/2$, and a summand of order p generated by $\tilde{f}_1$.*

Proof. The image of z under any homomorphism in $\mathrm{Hom}_P(T \wedge T, T/T_e)$ must be in the subgroup generated by $\hat{z}_e$. Thus using Theorem 6.11 we find that $\mathrm{Hom}_P(T \wedge T, T/T_e)$ is the direct sum of $\frac{1}{2}(p^s-2p^{s-1}-1)$ summands generated by $\tilde{f}_k$ for $p^{s-1}+1 \le k \le (p^s-1)/2$

and a summand generated by $\tilde{f}_1$. Finally, each of the subgroups generated by $\tilde{f}_k$ is isomorphic to T/T_e for $p^{s-1}+1 \leq k \leq (p^s-1)/2$ and the subgroup generated by $\tilde{f}_1$ is isomorphic to $T_{e-1}/T_e \cong C_p$. □

Denote $m_s = \frac{1}{2}(p^s - 2p^{s-1} - 1)$ and consider

$$\begin{aligned} \mathcal{I}_{p,s} &= \{a \in \mathbb{Z} \mid 2 \leq a \leq (p^s-1)/2, a \not\equiv 0, 1 \bmod p\}, \\ \mathcal{J}_{p,s} &= \{p^{s-1}+1, \ldots, (p^s-1)/2\}. \end{aligned}$$

From Theorem 6.10 and Definition 6.6 we can see that there are two different bases of H_0 which are indexed over different sets of size m_s, namely the bases are $\{\nu_k \mid k \in \mathcal{I}_{p,s}\}$ and $\{f_k \mid k \in \mathcal{J}_{p,s}\}$. Note that $\mathcal{I}_{p,s} \to \{1, 2, \ldots, m_s\} : n \mapsto n - 2\lfloor n/p \rfloor - 1$ and $\mathcal{J}_{p,s} \to \{1, 2, \ldots, m_s\} : n \mapsto n - p^{s-1}$ are indeed bijections. Both bases are useful for different purposes: the definition of $\{f_k \mid k \in \mathcal{J}_{p,s}\}$ is natural, whereas $\{\nu_k \mid k \in \mathcal{I}_{p,s}\}$ will be convenient when studying the action of the automorphism group (to solve the isomorphism problem for skeleton groups), see (6.8) below. The presence of two bases poses some notational difficulties; in order to reduce these technicalities, we adopt the following.

Notation 6.13. We relabel the ordered bases $(\nu_k)_{k \in \mathcal{I}_{p,s}}$ and $(f_k)_{k \in \mathcal{J}_{p,s}}$ as $(\overline{\nu}_k)_{k=1}^{m_s}$ and $(\overline{f}_k)_{k=1}^{m_s}$ respectively.

The following result follows from Corollary 6.11 and Theorem 6.6.

Lemma 6.14. *If $\gamma \in \mathrm{Hom}_P(T \wedge T, T)$ then*

a) *there exists a unique $(c_1, \ldots, c_{m_s}) \in T^{m_s}$ such that $\gamma = \sum_{a=1}^{m_s} c_a \overline{f}_a$,*

b) *there exists a unique $(b_1, \ldots, b_{m_s}) \in K^{m_s}$ such that $\gamma = \sum_{a=1}^{m_s} b_a \overline{\nu}_a$.*

Remark 6.15. Lemma 6.14 shows that there exists an invertible matrix $B \in \mathrm{GL}_{m_s}(K)$ which represents the change of bases for $\mathrm{Hom}_P(T \wedge T, T)$ from $\{\overline{f}_k \mid 1 \leq k \leq m_s\}$ to $\{\overline{\nu}_k \mid 1 \leq k \leq m_s\}$. If γ is uniquely represented as $\gamma = \sum_{a=1}^{m_s} c_a \overline{f}_a$ then $\gamma = \sum_{a=1}^{m_s} b_a \overline{\nu}_a$ where $\boldsymbol{b} = \boldsymbol{c}B$ with $\boldsymbol{c} = (c_1, \ldots, c_{m_s}) \in T^{m_s}$ and $\boldsymbol{b} = (b_1, \ldots, b_{m_s}) \in K^{m_s}$. For example if $s = 1$, then [20, Section 4.1] shows that $B = (\beta_{ij})_{m_1 \times m_1}$ is given by $\beta_{i,j} = \left(\theta^{i-2} - \theta^{3-i}\right)\left(\left(\theta^{i-2} - 1\right)\left(\theta^{3-i} - 1\right)\right)^{j-1}$.

Our next aim is to investigate the automorphism group of the space group.

6.2.2 The automorphism group

To determine the automorphism group of G, it is useful to exploit the extension structure of G. For this a cohomological argument can be used. We therefore first recall some

facts on cohomology groups; these are standard and can be found in [48, 80]. For any group H and an H-module N, the corresponding groups of 1-cocycles, 1-coboundaries, and the first cohomology group are defined as follows.

$$Z^1(H,N) = \{\gamma : H \to N \mid \gamma(gh) = \gamma(g)^h + \gamma(h) \text{ for all } g,h \in H\},$$
$$B^1(H,N) = \{\gamma \in Z^1(H,N) \mid \exists n \in N \text{ such that } \gamma(g) = n^g - n \text{ for all } g \in H\},$$
$$H^1(H,N) = Z^1(H,N)/B^1(H,N).$$

The next lemma describes the structure of $Z^1(P,T)$.

Lemma 6.16. *$Z^1(P,T) = \{\alpha_t \mid t \in T\}$ where $\alpha_t : P \to T$ is given by $\alpha_t(g^i) = \frac{\theta^i-1}{\theta-1}t$ for all $i \geq 0$.*

Proof. Suppose $\alpha \in Z^1(P,T)$ maps g to $t \in T$. By definition $\alpha(uv) = \alpha(u)^v + \alpha(v)$ for $u,v \in P$. Then inductively we can show that α maps g^i to $(1+\theta+\ldots+\theta^{i-1})t = \frac{\theta^i-1}{\theta-1}t$ for all $i \geq 0$. Hence every such α is equal to α_t for some $t \in T$. Conversely take $t \in T$ and consider α_t. Then $\alpha_t(g^b)^{g^a} + \alpha_t(g^a) = \frac{\theta^{b-1}-1}{\theta-1}\theta^a t + \frac{\theta^{a-1}-1}{\theta-1}t = \frac{\theta^{a+b}-1}{\theta-1}t = \alpha_t(g^{a+b})$ for all $1 \leq a,b \leq p^s-1$, So $\alpha_t \in Z^1(P,T)$. □

The proof of the following theorem is motivated by [34, Lemma 5.4]. Recall from Section 4.1 that the Galois group G_θ of $\mathbb{Q}_p(\theta)|\mathbb{Q}_p$ is cyclic of order d_s and is generated by σ_k for a primitive root k modulo p^s.

Theorem 6.17. *The automorphisms of G are $\phi(k,u,s) : G \to G$ defined by*

$$(g^i,t) \mapsto (g^{ik}, u\sigma_k(t) + u_{ik}s), \qquad (0 \leq i \leq p^s-1,\ t \in T) \tag{6.4}$$

where $k \in \{1,\ldots,d_s\}$ with $p \nmid k$, $s \in T, u \in \mathcal{U}_{p^s}$ and $u_j = \frac{\theta^j-1}{\theta-1}$ for all $j \geq 0$.

Proof. Since $G/T \cong P$ and T is characteristic in G, see Lemma 3.18, we can define a homomorphism $\lambda : \mathrm{Aut}(G) \to \mathrm{Aut}(P)$ mapping $\phi \mapsto \phi|_{G/T}$. Recall that the G_θ is generated by σ_k and σ_k induces an automorphism η_k of G mapping $(g^i,t) \mapsto (g^{ki}, \sigma_k(t))$. Hence the subgroup $\langle\eta_k\rangle$ (of $\mathrm{Aut}(G)$) maps onto $\mathrm{Aut}(P)$ under λ. We now determine the kernel of λ. Consider a restriction map $\zeta : \mathrm{Aut}(G) \to \mathrm{Aut}(T)$ mapping $\phi \mapsto \phi|_T$. If $\phi \in \ker(\lambda)$ then $\phi|_P = id_P$. Hence $\phi|_T$ is a P-module automorphism of T. Now T acts on T by natural ring multiplication. In that case any P-module automorphism of T is a T-module automorphism of T since g acts as multiplication by θ on T. So $\phi|_T$ is a T-module automorphism of T. But T is a cyclic T-module and multiplication by a unit is a T-module automorphism of T. Hence the group of T-module automorphisms of T is isomorphic to $\mathcal{U}_{p^s}$. Thus ζ maps $\ker(\lambda)$ into $\mathcal{U}_{p^s}$ and multiplication by a unit induces

an automorphism of G which lies in $\ker(\lambda)$. Hence ζ maps $\ker(\lambda)$ onto $\mathcal{U}_{p^s}$. Finally we find $\ker(\zeta) \cap \ker(\lambda)$. If $\phi \in \ker(\zeta) \cap \ker(\lambda)$ then ϕ fixes P and T point-wise. Hence $\phi \in \mathrm{Aut}(G)$ satisfies $\phi(g^i, 0) = (g^i, \phi_2(g))$ for some $\phi_2 \in Z^1(P, T)$. Thus by Lemma 6.16 there is $s \in T$ such that $\phi_2(g^i) = \frac{\theta^i - 1}{\theta - 1} s$ for all $i \geq 0$. Note that each $x \in T$ induces an automorphism of G mapping $(g^i, t) \mapsto (g^i, t + \frac{(\theta^i - 1)}{\theta - 1} x)$. Finally we recall that P is cyclic and every automorphism of P maps $g^i \mapsto g^{ik}$ for some $1 \leq k \leq d_s$ such that $p \nmid k$. □

Remark 6.18. a) The inverse of $\phi(k, u, s)$ is given by $\phi(l, \sigma_l(u)^{-1}, \sigma_l(u)^{-1} u_j s^{-1})$ where $k \equiv l^{-1} \bmod p^s$.

b) Let A_θ, A_u, and A_z denote the automorphisms of G induced by $G_\theta, \mathcal{U}_{p^s}$, and $Z^1(P, T)$ respectively, that is,

$$\begin{aligned} A_\theta &= \{\phi(k, 1, 0) \mid 1 \leq k \leq d_s, p \nmid k\} \cong G_\theta, \\ A_u &= \{\phi(1, u, 0) \mid u \in \mathcal{U}_{p^s}\} \cong \mathcal{U}_{p^s}, \\ A_z &= \{\phi(1, 1, \theta^i) \mid 0 \leq i \leq d_s - 1\} \cong Z^1(P, T). \end{aligned}$$

We have $\mathrm{Aut}(G) \cong (A_\theta \ltimes A_u) \ltimes A_z$. Below we sometimes identity $A_\theta = G_\theta$, etc.

The following lemma is immediate from the proof of Theorem 6.17. This result is analogous to [20, Lemma 3.2 (a)].

Lemma 6.19. *Let $\rho : \mathrm{Aut}(G) \to \mathrm{Aut}(T)$ be the natural restriction. The kernel of ρ is $A_z \cong Z^1(P, T)$. The image of ρ is $A_\theta \ltimes A_u$ restricted to T, that is, isomorphic to $G_\theta \ltimes \mathcal{U}_{p^s}$; a preimage of $(\sigma_z, u) \in G_\theta \ltimes \mathcal{U}_{p^s}$ under ρ is $\phi(z, u, 0)$.*

Recall from [53, Definition 3.1.3] that if H is a finite p-group with class n then for $i \in \{2, \ldots, n-2\}$, the 2-*step centraliser* K_i in H is the centraliser in H of $\gamma_i(H)/\gamma_{i+2}(H)$. Recall that $G_j = P \ltimes T/T_j$.

Lemma 6.20. *If $j \geq 4$, then $f \mapsto f|_{G_j}$ is a surjection from $\mathrm{Aut}(G)$ to $\mathrm{Aut}(G_j)$.*

Proof. Let $\alpha \in \mathrm{Aut}(G_j)$. We note that P is abelian and the 2-nd and 4-th term of the lower central series of G_j are T_1/T_j and T_3/T_j respectively. So the two step centraliser of G_j is $C_{G_j}(T_1/T_3) = T/T_j$. Hence T/T_j is characteristic in G_j. So $\alpha(g, 0 + T_j) = (g^l, a)$ for some $a \in T/T_j$ and $l \in \mathbb{Z}_p^*$. Suppose now for each $a \in T/T_j$ we choose and fix an element $\tau(a) \in T$ using a transversal $\tau : T/T_j \to T$ such that $\tau(a) + T_j = a$. We take an automorphism $\beta = \phi(l, 1, \theta\sigma_l(\tau(a)))|_{G_j}$, see Theorem 6.17, and observe that $\beta \circ \alpha^{-1}(g, 0 + T_j) = \beta(g^n, -a^{g^n}) = (g, \sigma_l(-\tau(a)^{g^n}) + \theta\sigma_l(\tau(a)) + T_j)$. Hence $\beta \circ \alpha^{-1}(g, 0 + T_j) = (g, 0 + T_j)$. Further it is evident that α has a preimage in $\mathrm{Aut}(G)$ if and only if $\beta \circ \alpha^{-1}$ has a preimage in $\mathrm{Aut}(G)$. Thus we can assume that $\alpha(g) = g$ and $\alpha(1 + T_j) = v + T_j$ for some $v \in T$. Then for $x \in \{0, \ldots, d_s - 1\}$ we have

$\alpha(g^x, 1+T_j) = \alpha(g^x, 0+T_j)\alpha(1, 1+T_j) = (g^x, v+T_j)$ and so $\alpha(1, \theta^x+T_j) = \alpha(g^{-x}, 1+T_j)\alpha(g^x, 0+T_j) = (g^{-x}, v+T_j)(g^x, 0+T_j) = (1, \theta^x v+T_j) = (1, (v+T_j)(\theta^x+T_j))$. So $\alpha|_{T/T_j}$ is the multiplication by $v+T_j$. But $\alpha|_{T/T_j} \in \mathrm{Aut}(T/T_j)$ and so $v \in \mathcal{U}_{p^s}$. Thus $\alpha(g^i, t+T_j) = (g^i, vt+T_j)$ for $t \in T$ and $0 \leq i \leq p^s-1$. Hence $\alpha = \phi(1, v, 0)|_{G_j}$. □

6.2.3 Orbit isomorphisms

Recall that $m_s = \frac{1}{2}(p^s - 2p^{s-1} - 1)$ and the skeleton subgraph of the branch $\mathcal{B}_j$ is denoted by $\mathcal{S}_j$. Let B be the base change matrix as given in Remark 6.15. Now Lemma 6.14 allows us to define the following.

Definition 6.21. If $\boldsymbol{c} = (c_1, \ldots, c_{m_s}) \in K^{m_s}$ and $\gamma = \sum_{a=1}^{m_s} c_a \overline{\nu}_a \in L_j$, then the skeleton group $G_{\gamma,m}$ defined by γ and m is denoted by $S_m(\boldsymbol{c})$.

In order to investigate orbit isomorphisms, one requires to study the orbits of the action of $\mathrm{Aut}(G)$ on L_j as defined in (6.1). From Definition 6.21 we can see that one can also parametrise the skeleton groups by the elements of K^{m_s}. Thus we first transfer the action (6.1) to the tuples that define skeleton groups. For $j \geq 1$ we define

$$\Theta_j = \{\boldsymbol{c} \in K^{m_s} \mid S_m(\boldsymbol{c}) \in \mathcal{S}_j \text{ for some } m \text{ with } j \leq m \leq 2j - d_s\}, \tag{6.5}$$

$$\Omega_j = \{(c_1, \ldots, c_{m_s})B^{-1} \mid c_i \in \mathfrak{p}^j \text{ for } 1 \leq i \leq m_s\} \tag{6.6}$$

and we consider the following homomorphisms defined for all $a \in \mathcal{I}_{p,s}$

$$\rho_a : \mathcal{U}_{p^s} \to \mathcal{U}_{p^s} \text{ defined by } u \mapsto u^{-1}\sigma_a(u)\sigma_{1-a}(u). \tag{6.7}$$

Lemma 6.17 and Remark 6.18 show that A_z acts trivially on L_j and hence the action of $\mathrm{Aut}(G)$ on L_j is same as the action of $A_\theta \ltimes A_u$ on L_j. In the following we rewrite this action in terms of the parameters from Θ_j. This is motivated by [20, Lemma 4.3].

An element $(\sigma_n, u) \in G_\theta \ltimes \mathcal{U}_{p^s}$ acts on $\boldsymbol{c} = (c_1, \ldots, c_{m_s}) \in \Theta_j$ via

$$\boldsymbol{c}^{(\sigma_n,u)} = (\rho_1(u^{-1})\sigma_n(c_1), \ldots, \rho_{m_s}(u^{-1})\sigma_n(c_{m_s})) \tag{6.8}$$

To see this we observe the following. Let $\boldsymbol{c} = (c_1, \ldots, c_{m_s}) \in \Theta_j$. Suppose

$$\gamma = \sum_{a=1}^{m_s} c_a \overline{\nu}_a \quad \text{and} \quad \gamma' = \sum_{a=1}^{m_s} \sigma_n(c_a)\rho_a(u^{-1})\overline{\nu}_a.$$

We note that $\phi(n,u,0)^{-1} = \phi(l,v,0)$ where $l \equiv n^{-1} \bmod p^s$ and take $v = \sigma_l(u^{-1})$. Then using (6.1) and (6.7), for all $t, s \in T$ we have

$$\begin{aligned}
\gamma^{\phi(n,u,0)^{-1}}(t \wedge s) &= \phi(n,u,0)(\gamma((v\sigma_l(t)) \wedge ((v\sigma_l(s)))) \\
&= \phi(n,u,0)(\sum_{a=1}^{m_s} c_a\overline{\nu}_a((v\sigma_l(t)) \wedge ((v\sigma_l(s)))) \\
&= \phi(n,u,0)(\sum_{a=1}^{m_s} c_a\sigma_a(v)\sigma_{1-a}(v)\overline{\nu}_a(\sigma_l(t) \wedge (\sigma_l(s))) \\
&= \sum_{a=1}^{m_s} \sigma_n(c_a)u\sigma_a(u^{-1})\sigma_{1-a}(u^{-1})\overline{\nu}_a(t \wedge s) \\
&= \sum_{a=1}^{m_s} \sigma_n(c_a)\rho_a(u^{-1})\overline{\nu}_a(t \wedge s) \\
&= \gamma'(t \wedge s).
\end{aligned}$$

Now $\boldsymbol{c} \in \Theta_j$ implies $S_m(\boldsymbol{c}) \in \mathcal{S}_j$. Then using (6.1) we get that $G_{\gamma' m} \in \mathcal{S}_j$, in other words $S_m(\boldsymbol{c}^{(\sigma_n,u)}) \in \mathcal{S}_j$, and therefore $\boldsymbol{c}^{(\sigma_n,u)} \in \Theta_j$.

Remark 6.22. The action defined in (6.8) induces an action on Ω_j and hence on the set of cosets Ω_j/Ω_{j+e} for all $e \geq 1$.

Now we rephrase Proposition 5.8 in terms of Θ_j and (6.8).

Theorem 6.23. *Let $j > d_s$ and choose m such that $j \leq m \leq 2j - d_s$. Suppose $\boldsymbol{c}, \boldsymbol{b} \in \Theta_j$. Then $S_m(\boldsymbol{c})$ and $S_m(\boldsymbol{b})$ are isomorphic if and only if $\boldsymbol{c} + \Omega_m$ and $\boldsymbol{b} + \Omega_m$ lie in the same orbit under the action of $G_\theta \ltimes \mathcal{U}_{p^s}$ on Ω_j/Ω_m.*

Proof. Let $\boldsymbol{c} = (c_1, \ldots, c_{m_s})$ and $\boldsymbol{b} = (b_1, \ldots, b_{m_s})$. Using Lemma 6.14, consider $\gamma = \sum_{a=1}^{m_s} c_a\overline{\nu}_a$ and $\gamma' = \sum_{a=1}^{m_s} b_a\overline{\nu}_a$. Since the point group is cyclic, we know from Lemma 6.2 that $S_m(\boldsymbol{c})$ and $S_m(\boldsymbol{b})$ are isomorphic if and only if there exists some automorphism ψ of G such that $(\gamma')^\psi \equiv \gamma \bmod H_m$. Now by Lemma 6.19 we can assume $\psi = \phi(n,u,0)$ for some n with $p \nmid n$ and $u \in \mathcal{U}_{p^s}$. The action of $\phi(n,u,0)$ corresponds to the action of $(\sigma_n, u) \in G_\theta \ltimes \mathcal{U}_{p^s}$ on Θ_j. Hence $S_m(\boldsymbol{c})$ and $S_m(\boldsymbol{b})$ are isomorphic if and only if for all $t, s \in T$

$$\sum_{a=1}^{m_s} (b_a - \sigma_n(c_a)\rho_a(u^{-1}))\overline{\nu}_a(t \wedge s) \in T_m. \tag{6.9}$$

Let $\alpha_a = b_a - \sigma_n(c_a)\rho_a(u^{-1})$ for $1 \leq a \leq m_s$ and $(\alpha_1, \ldots, \alpha_{m_s})B^{-1} = (\beta_1, \ldots, \beta_{m_s})$. Now using Remark 6.15 we see that (6.9) holds if and only if we have for all $t, s \in T$

$$\sum_{a=1}^{m_s} \beta_a\overline{f}_a(t \wedge s) \in T_m.$$

Note that $(\alpha_1, \ldots, \alpha_{m_s})B^{-1} = \boldsymbol{b}B^{-1} - \boldsymbol{c}^{(\sigma_n,u)}B^{-1}$. Thus from Definition 6.10 we conclude (6.9) holds if and only if $(\boldsymbol{b}B^{-1} - \boldsymbol{c}^{(\sigma_n,u)}B^{-1}) \in T_m$ that is $S_m(\boldsymbol{c})$ and $S_m(\boldsymbol{b})$ are isomorphic if and only if $\boldsymbol{c} + \Omega_m$ and $\boldsymbol{b} + \Omega_m$ lie in the same orbit under the action of $G_\theta \ltimes \mathcal{U}_{p^s}$. □

6.2.4 The one-parameter case

Definition 6.21 shows that skeleton groups can be parametrised by tuples in K^{m_s}. One interesting case is to consider all those homomorphisms that are parametrised by tuples having exactly one non-zero entry. Recall from Definition 5.11 that these are called one-parameter homomorphism and were first considered in [59] for maximal class groups; later they were studied in [34] for investigating $\mathcal{G}(3,2)$. Here we analyse these homomorphisms for odd primes and coclass r. We start with a preliminary lemma.

We define consider the subset $\mathcal{I}'_{p,s} = \{a \in \mathcal{I}_{p,s} \mid p \mid (2a-1)\}$, and write δ_a for the largest p-power dividing $2a-1$. For $a \in \mathcal{I}_{p,s}$, let

$$E_{a,j} = \{c\nu_a \mid c \in K\} \cap H_j.$$

In the following we consider skeleton groups defined by the one-parameter homomorphisms in $E_{a,j}$. The following result is a generalisation of [34, Lemma 5.3].

Lemma 6.24. *For $a \in \mathcal{I}_{p,s}$, the following hold.*

a) $E_{a,j} = \{c_a(\theta-1)^{j-\delta_a}\nu_a \mid c_a \in T\}$.

b) $E_{a,j} \setminus E_{a,j+1} = \{(\theta-1)^{j-\delta_a}u\nu_a \mid u \in \mathcal{U}_{p^s}\}$.

Proof. a) Since T is a P-module of rank d_s, the image of $T \wedge T$ under ν_a is generated by $\{\nu_a(\theta^{u_1} \wedge \theta^{u_2}) \mid 0 \le u_1 < u_2 \le d_s - 1\}$ for all $a \in \mathcal{I}_{p,s}$. If $u_1 > u_2$, say $u_1 = \epsilon + u_2$ with $\epsilon \ge 1$ then

$$\begin{aligned}
\nu_a(\theta^{u_1} \wedge \theta^{u_2}) &= \sigma_a(\theta^{u_1})\sigma_{1-a}(\theta^{u_2}) - \sigma_a(\theta^{u_2})\sigma_{1-a}(\theta^{u_1}) \\
&= \theta^{a(\epsilon+u_2)}\theta^{(1-a)u_2} - \theta^{au_2}\theta^{(1-a)(\epsilon+u_2)} \\
&= \theta^{a\epsilon+u_2} - \theta^{\epsilon+u_2-a\epsilon} \\
&= \theta^{\epsilon+u_2-a\epsilon}[\theta^{(2a-1)\epsilon} - 1].
\end{aligned}$$

Together with the proof of Lemma 5.10a), this implies that $\nu_a(T \wedge T)$ lies in T_{δ_a} but not in T_{δ_a+1}. Thus each $(\theta-1)^{j-\delta_a}\nu_a$ is in $E_{a,j}$. Now by Theorem 6.6 and the definition of $E_{a,j}$ we get that ν_a generates $E_{a,j}$ as T-module. Hence if $\gamma : T \wedge T \to T_j$ is a P-module homomorphism then there exists $c_a \in T$ such that $\gamma = c_a(\theta-1)^{j-\delta_a}\nu_a$.

b) This follows from the fact that $\mathfrak{p}^l \setminus \mathfrak{p}^{l+1} = (\theta-1)^l\mathcal{U}_{p^s}$ for all l. □

For suitably chosen j and m, the skeleton group $G_{c\nu_a,m}$ is called a one-parameter group defined by the parameter a. Lemma 6.24 shows that if $\gamma \in E_{a,j}$ and γ is surjective then γ can be written as $\gamma = (\theta-1)^{j-\delta_a} c\nu_a$ for some $c \in \mathcal{U}_{p^s}$. Recall that $\mathcal{U}_{p^s,i} = 1 + \mathfrak{p}^i$ for all $i \geq 0$ where $\mathcal{U}_{p^s} = \mathcal{U}_{p^s,0}$.

Lemma 6.25. *Let $a \in \mathcal{I}_{p,s}$ and $j > d_s$. If $c, c' \in \mathcal{U}_{p^s}$ are units, then the homomorphisms $(\theta-1)^{j-\delta_a} c\nu_a$ and $(\theta-1)^{j-\delta_a} c'\nu_a$ induce the same element in L_j if and only if $c \equiv c' \bmod \mathcal{U}_{p^s,n}$.*

Proof. Note that two homomorphisms γ and γ' induce isomorphic skeleton group in $\mathcal{S}_j$ at depth n if and only if $\gamma(t \wedge s) - \gamma'(t \wedge s) \in T_{j+n}$ for all $s, t \in T$. First we suppose $c \equiv c' \bmod \mathcal{U}_{p^s,n}$. Thus $c' = c(1+e)$ for some $e \in \mathfrak{p}^n$. Thus for any $s, t \in T$ we have $(\theta-1)^{j-\delta_a} c'\nu_a(t \wedge s) - (\theta-1)^{j-\delta_a} c\nu_a(t \wedge s) = e(\theta-1)^{j-\delta_a} c\nu_a(t \wedge s) \in T_{j+n}$ since $e \in \mathfrak{p}^n$. Converse is similar. □

Theorem 6.26. *Let $j > d_s$ and $n < j - d_s$. Then the isomorphism types of the one-parameter skeleton groups defined by the parameter $a \in \mathcal{I}_{p,s}$ at depth n in branch $\mathcal{B}_j$ correspond to the cosets $\mathcal{U}_{p^s}/\rho_a(\mathcal{U}_{p^s})\mathcal{U}_{p^s,n}$.*

Proof. From (6.5) and (6.6) one can observe that the elements in Ω_j induce homomorphisms that define skeleton groups in $\mathcal{B}_j$. Also Lemma 6.23 shows that the isomorphism types of skeleton groups at depth $n \leq j - d_s$ in branch $\mathcal{B}_j$ are in one-one correspondence with the orbits of the action of $G_\theta \ltimes \mathcal{U}_{p^s}$ on Ω_j/Ω_{j+n}. In view of Notation 6.13, elements of the following set define one-parameter skeleton groups defined by the parameter $a \in \mathcal{I}_{p,s}$

$$\Omega_{j,a} = \Omega_j \cap \{(c_1, \ldots, c_{m_s})B^{-1} \mid c_i = 0 \text{ if } i \neq a \text{ and } c_a \in (\theta-1)^{j-\delta_a}\mathcal{U}_{p^s}\}.$$

Note that the action of $G_\theta \ltimes \mathcal{U}_{p^s}$ on Ω_j/Ω_m induces an action on $\Omega_{j,a}/\Omega_{m,a}$ for all $m \geq j$. Hence the isomorphism types of the one-parameter skeleton groups defined by the parameter $a \in \mathcal{I}_{p,s}$ at depth $n \leq j - d_s$ in branch $\mathcal{B}_j$ are in an one-one correspondence with the orbits of the action of $G_\theta \ltimes \mathcal{U}_{p^s}$ on $\Omega_{j,a}/\Omega_{j+n,a}$. Using Lemma 6.25 wee see that the desired orbits of corresponds to the $G_\theta \ltimes \mathcal{U}_{p^s}$-orbits of $\mathcal{U}_{p^s}/\mathcal{U}_{p^s,n}$.

We consider $(1,u) \in G_\theta \ltimes \mathcal{U}_{p^s}$ and $c \in T$ and observe that

$$\begin{aligned}((\theta-1)^{j-\delta_a} c\nu_a)^{(1,u)}(t \wedge s) &= (\theta-1)^{j-\delta_a} uc\nu_a(tu^{-1} \wedge su^{-1}) \\ &= (\theta-1)^{j-\delta_a} c\sigma_a(u^{-1})\sigma_{1-a}(u^{-1})u\nu_a(t \wedge s) \\ &= \rho_a(u^{-1})(\theta-1)^{j-\delta_a} c\nu_a(t \wedge s).\end{aligned}$$

Thus the subgroup $\{1\} \ltimes \mathcal{U}_{p^s}$ of $G_\theta \ltimes \mathcal{U}_{p^s}$ acts on $\mathcal{U}_{p^s}/\mathcal{U}_{p^s,n}$ via multiplication by $\rho(\mathcal{U}_{p^s})$. Let us consider $\alpha(m,a) = (1+\theta+\ldots+\theta^{m-1})^{j-\delta_a}$ and observe that this is a unit since $m \neq d_s$. We now consider $(\sigma_k^l, 1) \in G_\theta \ltimes \mathcal{U}_{p^s}$ and $c \in T$ and observe that

$$\begin{aligned}((\theta-1)^{j-\delta_a}c\nu_a)^{(\sigma_k^l,1)}(t \wedge s) &= \sigma_k^l((\theta-1)^{j-\delta_a}c\nu_a(\sigma_k^{-l}(t) \wedge \sigma_k^{-l}(s))) \\ &= \alpha(k^l,a)\sigma_k^l(c)(\theta-1)^{j-\delta_a}\sigma_k^l(\sigma_k^{-l}(\nu_a(t \wedge s))) \\ &= \alpha(k^l,a)\sigma_k^l(c)(\theta-1)^{j-\delta_a}\nu_a(t \wedge s).\end{aligned}$$

Thus for a fixed $a \in \mathcal{I}_{p,s}$, we can consider an action of G_θ on $\mathcal{U}_{p^s}/\rho_a(\mathcal{U}_{p^s})$ defined by $(u\rho_a(\mathcal{U}_{p^s}))^{\sigma_k} = \sigma_k(u)\rho_a(\mathcal{U}_{p^s})$. Note that $\alpha(k^l,a)$ is a unit for $0 \leq l \leq d_s - 1$. Let $\gamma = (\theta-1)^{j-\delta_a}c\nu_a$, $\gamma' = ((\theta-1)^{j-\delta_a}c\nu_a)^{(\sigma_k^l,1)}$ and $\gamma'' = \sigma_k^l(c)(\theta-1)^{j-\delta_a}\nu_a$. Then for $j \leq m \leq 2j - d_s$, the skeleton groups $G_{\gamma,m}$ and $G_{\gamma',m}$ are isomorphic if and only if $G_{\gamma'',m}$ and $G_{\gamma,m}$ are isomorphic; this is because $G_{\gamma',m}$ and $G_{\gamma'',m}$ are isomorphic as $\alpha(k^l,a)$ is a unit and multiplication by a unit induces an automorphism of G. Thus the desired orbits correspond to the cosets $\mathcal{U}_{p^s}/\rho_a(\mathcal{U}_{p^s})\mathcal{U}_{p^s,n}$. □

6.2.5 Descendants of a skeleton group

Since the parent of $G_{\gamma,m+1}$ is $G_{\gamma,m}$ for $\gamma \in L_j$, the following is easy to see from Lemma 6.2. Recall that any isomorphism between skeleton groups in $\mathcal{T}_G$ is an orbit isomorphism.

Lemma 6.27. *Given $\gamma \in L_j$ and $j \leq m \leq 2j - d_s - 1$, a skeleton group $G_{\gamma',m+1}$ is an immediate descendant of $G_{\gamma,m}$ if and only if there exists $\alpha \in \mathrm{Aut}(G)$ such that $\gamma^\alpha \equiv \gamma' \bmod H_m$.*

Noting that if $\gamma \in L_j$ then there is $s,t \in T$ such that $\gamma(t \wedge s) \in T_j \setminus T_{j+1}$, the next result follows from Lemma 4.2.

Lemma 6.28. *Suppose $\gamma \in L_j$ and $\delta \in H_k$ for $k > j$ then $\gamma + \delta \in L_j$.*

The next lemma describes the descendants of a skeleton group.

Lemma 6.29. *Let $j \geq 0$ and $\gamma \in L_j$. Suppose $j < m \leq 2j - d_s - 1$ and $1 \leq k \leq 2j - d_s - m$. Consider the skeleton group $G_{\gamma,m}$ at depth $e = m - j$ in $\mathcal{B}_j$. Then*

a) *A skeleton group H is a descendant of $G_{\gamma,m}$ of distance k if and only if*

$$H \cong G_{\gamma+\delta,m+k}$$

for some $\delta \in H_{j+e}$.

b) *For $\delta_1, \delta_2 \in H_{j+e}$, two skeleton groups $G_{\gamma+\delta_1,j+e+k}$ and $G_{\gamma+\delta_2,j+e+k}$ are isomorphic if and only if there exists $\alpha \in \mathrm{Stab}_{\mathrm{Aut}(G)}(\gamma + H_{j+e})$ such that*

$$\delta_1^\alpha + \gamma^\alpha - \gamma \equiv \delta_2 \bmod H_{j+e+k}.$$

Proof. a) Note that $m = e + j$. Consider $\delta \in H_m$ and by Lemma 6.28 we get $\gamma + \delta \in L_j$. Now $(\gamma+\delta) \equiv \gamma \bmod H_m$ since $\delta \in L_m$. Thus for the identity automorphism $\mathrm{id} \in \mathrm{Aut(G)}$ we get $(\gamma+\delta)^{\mathrm{id}} \equiv \gamma \bmod H_m$. So by Lemma 6.27, we conclude that $G_{\gamma+\delta,m+k}$ is a k-step descendant of $G_{\gamma,m}$.

Conversely let $G_{\eta,m+k}$ be a k-step descendant of $G_{\gamma,m}$ for some $\eta \in L_j$. Then by Lemma 6.27 we find that there is $\alpha \in \mathrm{Aut}(G)$ such that $\eta^\alpha \equiv \gamma \bmod T_m$. This means $\eta^\alpha = \gamma + \delta$ for all $t, s \in T$ for some $\delta \in H_m$. Thus by Lemma 6.2 we conclude $G_{\eta,m+k} \cong G_{\eta^\alpha,m+k}$. Hence $G_{\eta,m+k} \cong G_{\gamma+\delta,m+k}$.

b) Consider $G_{\gamma+\delta_1,m+k} \cong G_{\gamma+\delta_2,m+k}$. Now by Lemma 6.2 there is $\alpha \in \mathrm{Aut}(G)$ such that $(\gamma+\delta_1)^\alpha \equiv \gamma + \delta_2 \bmod H_{m+k}$ and hence $\delta_1^\alpha + \gamma^\alpha - \gamma \equiv \delta_2 \bmod H_{j+e+k}$. Now $\delta_1, \delta_2 \in L_m$ and $T_{m+k} \leq T_m$. So $\gamma^\alpha \equiv \gamma \bmod H_m$ which is same as saying $\alpha \in \mathrm{Stab}_{\mathrm{Aut}(G)}(\gamma + H_m)$. The converse is straightforward by using Lemma 6.2. □

Remark 6.30. Each $\gamma \in L_j$ can uniquely be written as $\gamma = (\theta - 1)^j F$ where $F \in L_0$. Hence every $F \in L_0$ induces a skeleton group $G_{(\theta-1)^j F,m}$ at depth $e = m - j$ in the branch $\mathcal{B}_j$ where $j \leq m \leq 2j - d_s$. Also note that multiplication by any unit induces an automorphism of G. Hence $\mathrm{Stab}_{\mathcal{U}_{p^s}}(\gamma + H_m) = \mathrm{Stab}_{\mathcal{U}_{p^s}}(F + H_{m-j})$.

Motivated by Lemma 6.29 and [17, Section 9.1] we define the following.

Definition 6.31. For $\alpha \in \mathrm{Aut}(G)$, $F \in H_0$, $g \in H_n$ and $e \geq n \geq 0$ we write

$$(g + H_e)_\alpha = g^\alpha + (F^\alpha - F) + H_e. \tag{6.10}$$

Note that (6.10) defines an *affine action*; it is a group action if and only if $F^\alpha \equiv F \bmod H_e$. However, we have $(g + H_e)_{(\alpha\circ\beta)} = ((g + H_e)_\alpha)_\beta$ and $(g + H_e)_{\mathrm{id}} = (g + H_e)$.

Lemma 6.32. *Suppose $\gamma \in L_j$. Choose m and k such that $j < m \leq 2j - d_s - 1$ and $1 \leq k \leq 2j - d_s - m$. Let $\mathfrak{M}_{\gamma,m,k}$ be the set of $\mathrm{Stab}_{\mathrm{Aut}(G)}(\gamma + H_m)$-representative of $\{g + H_{m+k} \mid g \in H_m\}$ under the affine action as in the Definition 6.31. Then the k-step descendants of $G_{\gamma,m}$, up to isomorphism, are given by*

$$\{G_{\gamma+\eta,m+k} \mid \eta \in \mathfrak{M}_{\gamma,m,k}\}.$$

Proof. By Lemma 6.29, the list of k-step descendants of $G_{\gamma,m}$ is given by

$$\{G_{\gamma+\delta,m+k} \mid \delta \in H_m\}$$

and for $\delta_1, \delta_2 \in H_m$, two skeleton groups $G_{\gamma+\delta_1,m+k}$ and $G_{\gamma+\delta_2,m+k}$ from this list are isomorphic if and only if there exists $\alpha \in \mathrm{Stab}_{\mathrm{Aut}(G)}(\gamma + H_m)$ such that $\delta_1^\alpha + \gamma^\alpha - \gamma \equiv \delta_2 \bmod H_{j+e+k}$. By assumption $\gamma = (\theta-1)^j F$ where $F \in L_0$ and hence $G_{\gamma+\delta_1,m+k}$ and $G_{\gamma+\delta_2,m+k}$ are isomorphic if and only if there exists $\alpha \in \mathrm{Stab}_{\mathrm{Aut}(G)}(\gamma + H_m)$ such that $(\delta_2 + H_m) \equiv \delta_1^\alpha + \gamma^\alpha - \gamma \bmod H_{m+k}$ which is equivalent saying $(\delta_2 + H_m)_\alpha \equiv \delta_1$ under the action defined in (6.10) for $\gamma \in L_j$. The claim follows. $\{G_{\gamma+\eta,m+k} \mid \eta \in \mathfrak{M}_{\gamma,m,k}\}$. □

6.2.6 The maximal class case

In this section we consider $\mathcal{G}(p,1)$. This is studied in detail in [17–20, 53, 56–59]. We are particularly interested in the descendants of a skeleton group. The case $p \equiv 5 \bmod 6$ is discussed in [18]. We here consider other primes. In view of Notation 6.5, we here take $s = 1$ so that θ is a primitive p-th root of unity. Then $T = (\mathbb{Z}_p[\theta], +)$ has $\mathbb{Z}_p$-rank $d = d_s = p-1$. The associated space group with the coclass tree of $\mathcal{G}(p,1)$ has point group P which is cyclic of order p, see [19].

We briefly recall some number theory from [18, section 5.1]. A detailed account of these results can also be found in [59, Section 2] and [69, Satz II.15.5]. Let $\mathcal{I}_{p,1} = \{2, \ldots, d/2\}$ as in Section 6.2.1 and denote $\mathcal{I} = \mathcal{I}_{p,1}$. It is also known that for $i \geq 2$, there exists $\mathbb{Z}_p$-module isomorphisms between T_i and $\mathcal{U}_{p,i}$ which are defined by the usual power series of the exponential and logarithm mapping

$$\exp : T_i \to \mathcal{U}_{p,i} \quad \text{and} \quad \log : \mathcal{U}_{p,i} \to T_i$$

with $\exp^{-1} = \log$. For simplicity when the prime p is clear from the context, we denote $\mathcal{U}_p = \mathcal{U}$ and $\mathcal{U}_{p,i} = \mathcal{U}^{(i)}$ for all $i \geq 0$. From (6.7), recall the definition of ρ_a for every $a \in \mathcal{I}$:

$$\rho_a : \mathcal{U} \to \mathcal{U} \text{ defined by } u \mapsto u^{-1}\sigma_a(u)\sigma_{1-a}(u).$$

Using log, the restriction of $\rho_a : \mathcal{U} \to \mathcal{U}$ to $\mathcal{U}^{(2)} = 1 + T_2$ induces the following $\mathbb{Q}_p(\theta)$-linear map,

$$\tau_a : T_2 \to T_2, \quad z \mapsto -z + \sigma_a(z) + \sigma_{1-a}(z). \tag{6.11}$$

As before we take $\omega \in \mathbb{Z}_p$ to be a primitive $(p-1)$-th root of unity. The following can be found in [18, 53].

Lemma 6.33. *There exist $v_3, \ldots, v_{p+1} \in T_1$ with $v_k \in T_{k-1} \setminus T_k$ for all k such that, for all $a \in \mathcal{I}$, the following holds. If $a \equiv \omega^i \bmod p$ and $1 - a \equiv \omega^j \bmod p$, then v_k is an eigenvector of τ_a with eigenvalue $\omega_{a,k} = \omega^{ik} + \omega^{jk} - 1$. The images of $v_3, \ldots, v_{p+1}$ under*

exp *map generate* $\mathcal{U}^{(2)}$ *as a* $\mathbb{Z}_p$*-module. If* $p \equiv 5 \bmod 6$*, then* $\omega_{a,k} \neq 0$ *for all* a *and* k*. If* $p \equiv 1 \bmod 6$*, then* $\omega_{a,k} = 0$ *for some* a *and* k*.*

So for integers a and k, if $\omega_{a,k} \neq 0$ then there exists a largest integer $p_{a,k}$ with $\omega_{a,k} \equiv 0 \bmod p^{p_{a,k}}$, and from [20] we define $v_{a,k,e} = \max\{\lceil (e-k+1)/d \rceil - p_{a,k}, 0\}$ for all $e \geq 0$. For $a \in \mathcal{I}$ we define

$$N(a) = \{k \in \mathbb{Z} \mid 3 \leq k \leq p+1, \omega_{a,k} \neq 0\}. \tag{6.12}$$

The following lemma is motivated by [18, Lemma 5.3], which only takes account for primes $p \equiv 5 \bmod 6$. We relax this condition and consider all odd primes.

Lemma 6.34. *Let* $a \in \mathcal{I}$*. Suppose* $u \in \mathcal{U}^{(2)}$ *is such that* $u = \prod_{k \in N(a)} \exp(v_k)^{a_k}$*, then* $\rho_a(u) \in \mathcal{U}^{(e)}$ *if and only if* $p^{v_{a,k,e}}$ *divides* a_k *for all* $k \in N(a)$*.*

Proof. Recall that $\omega_{a,k}$ is the eigenvalue of τ_a corresponding to v_k. Then using log and exp, it is easy to observe that $\rho_a(u) = \prod_{k \in N(a)} \exp(v_k)^{a_k \omega_{a,k}}$. Note that $\omega_{a,k} \neq 0$ and $v_k \in T_{k-1} \setminus T_k$ for all $k \in N(a)$. Hence from the definition of $\omega_{a,k}$ (as in Lemma 6.33) we find that $\rho_a(u) \in \mathcal{U}^{(e)}$ if and only if $\exp(v_k)^{a_k \omega_{a,k}} \in \mathcal{U}^{(e)}$ for all $k \in N(a)$. Using log, this is equivalent to saying $a_k \omega_{a,k} v_k \in T_e$ for all $k \in N(a)$. Now recall that $v_k \in T_{k-1} \setminus T_k$ and $pT_i = T_{i+d}$. Thus $a_k \omega_{a,k} v_k \in T_e$ if and only if $a_k \omega_{a,k} \in T_{e-k+1}$ which is equivalent to saying $a_k \in T_{e-k+1-dp_{a,k}}$ for all $k \in N(a)$ since $p^{p_{a,k}}$ is the highest power of p which divides $\omega_{a,k}$. This is true if and only if $p^{v_{a,k,e}}$ divides a_k since $pT_i = T_{i+d}$. □

Recall the definition of ν_a from (6.2) :

$$\nu_a : K \wedge K \to K, \quad x \wedge y \mapsto \sigma_a(x)\sigma_{1-a}(y) - \sigma_a(y)\sigma_{1-a}(x).$$

The following result, from Lemma 6.14, describes the structure of $\mathrm{Hom}_P(T \wedge T)$. See also [18, Lemma 4.4].

Lemma 6.35. *Every* P*-homomorphism* $f : T \wedge T \to T$ *can be written uniquely as*

$$f = c_2\nu_2 + \ldots + c_{d/2}\nu_{d/2} \quad \textit{with} \quad c_2, \ldots, c_{d/2} \in T_{-(p-3)^2/4}.$$

If f *is surjective, then* $c_a \notin T$ *for at least one* $a \in \mathcal{I}$*.*

Recall that $u \in \mathcal{U}$ acts on $f = \sum_{a \in \mathcal{I}} c_a \nu_a \in H_0$ via

$$f^u = \sum_{a \in \mathcal{I}} \rho_a(u^{-1}) c_a \nu_a. \tag{6.13}$$

We recall from Section 4.1.2 that the group of units $\mathcal{U}$ can be decomposed as

$$\mathcal{U} = \langle\omega\rangle \times \langle\theta\rangle \times \mathcal{U}^{(2)}.$$

Note that if $a \in \mathcal{I}$ then $\rho_a(\theta) = 1$ and $\rho_a(\omega) = \omega$. So in view of (6.13), we now investigate the action of $\mathcal{U}^{(2)}$. We note that for every $u = \prod_{k=3}^{p+1} \exp(v_k)^{a_k} \in \mathcal{U}^{(2)}$ and $a \in \mathcal{I}$ we can write $u = \mathcal{N}_a(u)\mathcal{M}_a(u)$ where

$$\mathcal{N}_a(u) = \prod_{k \in N(a)} \exp(v_k)^{a_k} \quad \text{and} \quad \mathcal{M}_a(u) = \prod_{k \notin N(a)} \exp(v_k)^{a_k}.$$

Since $\rho_a(u) = \prod_{k=3}^{p+1} \exp(v_k)^{a_k \omega_{a,k}}$ for $a \in \mathcal{I}$, if $u \in \mathcal{U}$ then

$$\rho_a(u) = \rho_a(\mathcal{N}_a(u)).$$

For $f = \sum_{a \in \mathcal{I}} c_a \nu_a \in L_0$ and $u \in \mathcal{U}$, we get

$$f^u = \sum_{a \in \mathcal{I}} \rho_a(\mathcal{N}_a(u^{-1}))c_a\nu_a.$$

We now recall the following result from [18, Theorem 5.1]. For any group A, we denote the group of p-th power by $A^{[p]}$.

Theorem 6.36. *Let $p \equiv 5 \bmod 6$ and $f \in L_0$. Then there exists $e_0 \geq 0$ such that if $e \geq e_0$ then*

$$\mathrm{Stab}_{\mathcal{U}^{(2)}}(f + H_e)^{[p]} = \mathrm{Stab}_{\mathcal{U}^{(2)}}(f + H_{e+d_s})$$

and $\mathrm{Stab}_{\mathcal{U}^{(2)}}(f + H_e)$ centralises H_i/H_{i+3d_s} for all $i \geq 0$.

In [18] the case $p \equiv 5 \bmod 6$ has been studied while the case $p \equiv 1 \bmod 6$ is still open. In the following sections we consider the latter case in more detail. In general, the common observation is that for groups deep enough in a branch, the d_s-step parent often is a period parent, Theorem 6.36 is one such example. But computer experiments also show that there are cases where this is not true, and the question is whether this is a general fact or only an anomaly because those explicit examples involve groups of too small order. Our results in the following sections show that this is not an anomaly. The crucial difference between primes $p \equiv 5 \bmod 6$ and $p \equiv 1 \bmod 6$ is that in the latter case we have $\omega_{a,k} = 0$ for some k and a, while $\omega_{a,k} \neq 0$ for all a and k in the former case.

6.2.7 Periodic parents of skeleton groups in $\mathcal{G}(7,1)$

Consider the coclass graph $\mathcal{G}(p,1)$. We first recall a few definitions. Let k be an integer and define the k-step descendant tree $\mathcal{D}_k(H)$ of a group H in $\mathcal{B}_n$ as the subtree of $\mathcal{B}_n$ induced by the descendants of distance at most k from H. The following conjecture states one of the possibly ways describe these trees, see [18]. For any $n \geq 0$, let $e_p(n) = n-2p+8$ if $p \geq 7$ and $e_5(n) = n-4$.

Conjecture 6.37. *There is an integer $n_0 = n_0(p)$ such that, for every group K in $\mathcal{G}(p,1)$ at depth $e_p(n)$ in $\mathcal{B}_{n+p-1}$ with $n \geq n_0$, there exists a group H at depth $e_p(n-p+1)$ in $\mathcal{B}_{n+p-1}$ with $\mathcal{D}_{p-1}(K) \cong \mathcal{D}_{p-1}(H)$.*

Such a group H is a periodic parent of K. The conjecture is still open and there is only some partial evidence supporting it. The main difficulty is to find the correct periodic parent. Computer experiments for $p = 5, 7, 11$ suggest that the periodic parent can be chosen to be the $(p-1)$-step parent, that is, the unique ancestor at distance $p-1$. In fact the following is proved in [18, Theorem 1.2].

Theorem 6.38. *Let $p \equiv 5 \bmod 6$. There is an integer $n_0 = n_0(p)$ such that, for all $n \geq n_0$, the following holds. Let K be a group at depth $e_p(n)$ in $\mathcal{B}_{n+d}$ having immediate descendants and let H be the d-step parent of K. If the automorphism group of H is a p-group, then H is a periodic parent of K.*

From the proof of Theorem 6.38, as in [18], one can see that there are many number theoretic results used in the proof which are specifically true for $p \equiv 5 \bmod 6$, one such result is given in Theorem 6.36. Later in Lemma 6.40 we show that if $p = 7$ then the statement of Theorem 6.36 is not true. The aim of this section is to consider $p = 7$ and investigate the statement of Theorem 6.38 by relaxing the condition $p \equiv 5 \bmod 6$.

In the remainder of this section, let $p = 7$, that is, θ is a primitive 7-th root of unity and T is a $\mathbb{Z}_7$-module of dimension $d = 6$. The point group P is cyclic of order 7. Moreover, $\mathcal{I} = \{2, 3\}$ and ω is a 6-th root of unity; we choose $\omega \equiv 5 \bmod 7$. Then for $a = 2$ we have $a \equiv \omega^4 \bmod 7$ and $1 - a \equiv \omega^3 \bmod 7$. Similarly for $a = 3$ we get $a \equiv \omega^5 \bmod 7$ and $1 - a \equiv \omega \bmod 7$. Recall from Lemma 6.33 that if $a \equiv \omega^i \bmod p$ and $1 - a \equiv \omega^j \bmod p$, then v_k is an eigenvector of τ_a with eigenvalue $\omega_{a,k} = \omega^{ik} + \omega^{jk} - 1$ for $k \in \{3, \ldots, 8\}$. Using a straightforward computation we can list the eigenvalues of τ_a as

$a \downarrow, k \rightarrow$	3	4	5	6	7	8
2	-1	$-\omega$	$3\omega^2 - 2\omega$	1	$2\omega^2 - 3\omega$	ω^2
3	-3	-2	0	1	0	-2

Hence τ_2 has no zero eigenvalue whereas τ_3 has two zero eigenvalues for $k = 5, 7$. As a result, for any $u \in \mathcal{U}^{(2)}$, we can see that $\mathcal{N}_2(u) = u$. It is also easy to see that $p_{2,k} = 0$ if $k \neq 7$ and $p_{2,7} = 1$. Also $p_{3,k} = 0$ for $k \neq 5, 7$. We exploit the above facts in the following results.

Notation 6.39. For the rest of this chapter, for $n \geq 1$, we consider the homomorphisms

$$h_n = (\theta - 1)^n \nu_2 + (\theta - 1)^{-1} \nu_3.$$

We show that certain skeleton groups (parametrised by h_n) and their 6-step parents have non-isomorphic descendant trees. We first show that Theorem 6.36 is not true for $p = 7$.

Lemma 6.40. *If $n \geq 1$ then $h_n \in L_0$ and*

$$\mathrm{Stab}_{\mathcal{U}^{(2)}}(h_n + H_{n+2})^{[p]} \neq \mathrm{Stab}_{\mathcal{U}^{(2)}}(h_n + H_{n+2+d}).$$

Proof. By Lemma 6.35 we deduce $h_n \in L_0$. It is thus enough to find $u \in \mathrm{Stab}_{\mathcal{U}^{(2)}}(h_n + H_{n+2+d})$ such that there does not exist any $v \in \mathcal{U}^{(2)}$ with $u = v^p$. We aim to find integers x and y such that $u = \exp(v_7)^x \exp(v_5)^y$ is such an element of $\mathrm{Stab}_{\mathcal{U}^{(2)}}(h_n + H_{n+2+d})$. Now $\rho_3(u) = 1$. So $h_n^u - h = (\rho_2(u) - 1)(\theta - 1)^n \nu_2$. By Lemma 6.35 we find that if $(\rho_2(u) - 1) \in T_4$ then $u \in \mathrm{Stab}_{\mathcal{U}^{(2)}}(h_n + H_{n+2+d})$. We now show that $\rho_2(u) \in \mathcal{U}^{(4)}$. Now by Lemma 6.34, we find $\rho_2(u) \in \mathcal{U}^{(4)}$ if and only if $p^{v_{2,7,4}}$ divides x and $p^{v_{2,5,4}}$ divides y. Recall that $p_{2,7} = 1, p_{2,5} = 0$ and $v_{a,k,e} = \max\{\lceil (e - k + 1)/d \rceil - p_{a,k}, 0\}$ that is $v_{2,7,4} = v_{2,5,4} = 0$. So we choose x, y such that $7 \nmid x, y$. Recall that the images of $v_3, \ldots, v_8$ under exp map generate $\mathcal{U}^{(2)}$ as a $\mathbb{Z}_p$-module. So if there is $v \in \mathcal{U}^{(2)}$ such that $v^p = \exp(v_7)^x \exp(v_5)^y$ then p must divide both x and y. Hence by our choice of x and y, there does not exist any $v \in \mathcal{U}^{(2)}$ with $u = v^p$. This completes the proof. □

Corollary 6.41. *Let $n \geq 1$ and $e = n + 2$. Then there exist $g \in H_{e+d}$ and*

$$v \in \mathrm{Stab}_{\mathcal{U}^{(2)}}(h_n + H_{e+d}) \setminus \mathrm{Stab}_{\mathcal{U}^{(2)}}(h_n + H_e)^{[p]}$$

such that $(g + H_{e+d+1})_v \neq (g + H_{e+d+1})_{u^p}$ for all $u \in \mathrm{Stab}_{\mathcal{U}^{(2)}}(h_n + H_{e+d})$.

Proof. Take $g = (\theta - 1)^{e+d} h_n$. By the proof of Lemma 6.40, we can choose the element $v = \exp(v_7)^y \exp(v_5)^x$ with integers $x, y \geq 1$ not divisible by 7. Let $\alpha = ((\theta - 1)^{e+d} + 1)$. Then from (6.10) we have

$$(g + H_{e+d+1})_v = (\theta - 1)^n (\alpha \rho_2(v^{-1}) - 1) + (\theta - 1)^{-1} (\alpha \rho_3(v^{-1}) - 1).$$

Suppose, for a contradiction that $(g+H_{e+d+1})_v = (g+H_{e+d+1})_{u^p}$ for some unit u from $\mathrm{Stab}_{\mathcal{U}^{(2)}}(h_n + H_{e+d})$. Then we find that

$$\alpha((\theta-1)^n(\rho_2(v^{-1})-\rho_2(u^{-p}))+(\theta-1)^{-1}(\rho_3(v^{-1})-\rho_3(u^{-p}))) \in H_{e+d+1}.$$

Since α is a unit, we have $(\rho_2(v^{-1})-\rho_2(u^{-p}))+(\theta-1)^{-1}(\rho_3(v^{-1})-\rho_3(u^{-p}))) \in H_{e+d+1}$ which means $(\theta-1)^{-e-d-1}(\rho_2(v^{-1})-\rho_2(u^{-p}))+(\theta-1)^{-1}(\rho_3(v^{-1})-\rho_3(u^{-p}))) \in H_0$. So from Lemma 6.35 we get $(\theta-1)^{-9}(\rho_2(v^{-1})-\rho_2(u^{-p})) \in T_{-4}$. Hence we find that $(\rho_2(v^{-1})-\rho_2(u^{-p})) \in T_5$. So $(\rho_2(vu^{-p})-1) \in T_5$ since $\rho_2(u^p)$ is a unit. And hence $\rho_2(vu^{-p}) \in \mathcal{U}^{(5)}$. Write $u = \prod_{k=3}^{8}\exp(v_k)^{a_k}$. Now by Lemma 6.34 we get $p^{v_{2,5,5}}$ divides $x - 7a_5$ where $v_{2,5,5} = \max\{\lceil(5-5+1)/6\rceil - 0, 0\} = 1$ which is a contradiction since 7 does not divide x. □

We now find a family of skeleton groups in $\mathcal{G}(7,1)$ whose automorphism groups are 7-groups.

Lemma 6.42. *Let $n = 3+6z$ with $z \geq 1$. Then the automorphism group of $G_{(\theta-1)^j h_n, j+n+2}$ is a 7-group for $j \in (18+6\mathbb{Z}) \setminus (15+42\mathbb{Z})$.*

Proof. Using Remark 6.15 we have

$$B = \begin{pmatrix} \theta^2(1-\theta^4) & (\theta^3-1)u_1 \\ \theta^3(1-\theta^2) & (\theta^3-1)u_2 \end{pmatrix}$$

where $u_1 = \theta + 2\theta^2 + 2\theta^3 + 2\theta^4 + \theta^5$ and $u_2 = \theta + 3\theta^2 + 4\theta^3 + 3\theta^4 + \theta^5$ are both units. We now take

$$c_1 = (\theta-1)^n, \quad c_2 = (\theta-1)^{-1}, \quad q_1 = (\theta-1)^j c_1, \quad q_2 = (\theta-1)^j c_2.$$

So if $f = q_1\nu_2 + q_2\nu_3$ then $H = G_{f,j+e}$ is a skeleton group at depth e in branch $\mathcal{B}_j$. Note that the Galois group of $\mathbb{Q}_7(\theta)$ is generated by σ_3 which has order 6. Also note that $\sigma_3^2 = \sigma_2$ has order 3 and $\sigma_3^3 = \sigma_6$ has order 2. Recall that the point group is cyclic and hence Hypothesis 6.3 is true here. So from [20, Section 5] we conclude that $\mathrm{Aut}(H)$ is a p-group if and only if there does not exist $w_i \in \mathcal{U}$ such that $(q_1,q_2)^{(\sigma_i,w_i)} \equiv (q_1,q_2) \bmod \Omega_{j+e}$ for all $i = 2,3,6$ where the action is as defined in (6.8). Using (6.6), this is true if and only if $((q_1,q_2)^{(\sigma_i,w)} - (q_1,q_2))B \notin T_{j+e} \times T_{j+e}$ for all $w \in \mathcal{U}$ and $i = 2,3,6$. Now we take $e = n+2$ and note that $(\theta^i - 1) = (\theta-1)z_i$ for $i = 2,3,6$ where $z_2 = 1+\theta$, $z_3 = 1+\theta+\theta^2$ and $z_6 = 1+\theta+\theta^2+\theta^4+\theta^5 = -\theta^6$. Following the definition of B, a straightforward computation shows that if $((q_1,q_2)^{(\sigma_i,w_i)} - (q_1,q_2))B \in T_{j+e} \times T_{j+e}$

for some $w_i \in \mathcal{U}$ then

$$(\theta-1)^n\theta^2(1-\theta^4)(z_i^{j+n}\rho_2(w_i^{-1})-1)+(\theta-1)^{-1}\theta^3(1-\theta^2)(z_i^{j-1}\rho_3(w_i^{-1})-1)\in T_{n+2}$$

for $i=2,3,6$. Now we have $(\theta-1)^n(1-\theta^4)\in T_{n+1}$ which shows $(z_i^{j-1}\rho_3(w_i^{-1})-1)\in T_{n+1}$. If $\rho_3(w_i^{-1})\in\mathcal{U}_1$ then let $\rho_3(w_i^{-1})=1+t$ for some $t\in T_1$ and $i=2,3,6$. So for $n\geq 0$ we get $z_i^{j-1}-1=t'-tz^{j-1}\in T_1$ for some $t'\in T_{n+1}$. Note that $z_i^{18+6z-1}-1$ is of the form $a\theta(1+\theta^5)+b\theta^2(1+\theta^3)+c\theta^3(1+\theta)$ for $i=2,3,6$ and $z\geq 1$ where $a,b,c\in\mathbb{Z}_p$ are obtained via binomial theorem. So $z_i^{18+6z-1}-1\notin T_1$ for all $z\geq 1$ and $i=2,3$. Since z_6 is a 6-th root of unity, we can observe that $z_6^{j-1}-1\notin T_1$ unless $j=15+42k$ for some $k\geq 1$ as in such cases $z_6^{j-1}-1=0$. Thus $w_i\notin\mathcal{U}_1$ for all $i=2,3,6$ unless $j=15+7k$ for some $k\geq 1$ such that $6\mid k$.
Finally if $\rho_3(w_i^{-1})=1+s$ for $s\in T\setminus T_1$ then $z_i^{18+6z-1}(1+s)-1\notin T_1$ which shows there is no $w_i\in\mathcal{U}$ such that $(z_i^{j-1}\rho_3(w_i^{-1})-1)\in T_{n+1}$ unless $j=15+42k$ for some $k\geq 1$. Hence $\mathrm{Aut}(H)$ is a p-group unless $j=15+42k$ for some $k\geq 1$. □

We finally find a family of skeleton groups in $\mathcal{G}(7,1)$ whose 6-step parents are *not* periodic parents. Let $F_{18+6z}=(\theta-1)^{18+6z}h_{3+6z}$ and $e(18+6z)=5+6z$ for $z\geq 0$.

Theorem 6.43. *Using the notation of the above paragraph, for any $j=18+6z$ with $z\geq 0$, the skeleton groups $G_{F_j,j+e(j)}$ and $G_{F_j,j+e(j)+6}$ have different number of immediate descendants if $j\in(18+6\mathbb{Z})\setminus(15+42\mathbb{Z})$.*

Proof. Let $j=18+6z$ and take $e=n+2$ where $n=3+6z$. Take $\gamma=F_{18+6z}$. Let $m=j+e$ and $\mathfrak{M}_{h_n,m,1}$ be the set of $\mathrm{Stab}_{\mathrm{Aut}(G)}((\theta-1)^jh_n+H_m)$-orbit representatives of $\{g+H_{m+1}\mid g\in H_m\}$ under the action as in Definition 6.31. Then by Lemma 6.32, the immediate descendants, up to isomorphism, of the skeleton group $G_{\gamma,j+e}$ are given by

$$\{G_{\gamma+\eta,j+e+1}\mid\eta\in\mathfrak{M}_{h_n,m,1}\}.$$

By Lemma 6.42 we see that the automorphism group of the skeleton group $G_{\gamma,j+e}$ is a p-group unless unless $j=15+42k$ for some $k\geq 1$. Hence by Remark 6.30, the immediate descendants, up to isomorphism, of the skeleton groups $G_{\gamma,j+e}$ and $G_{\gamma,j+e+6}$ are in one-one correspondence with $\mathfrak{M}'_{h_n,e,1}$ and $\mathfrak{M}'_{h_n,e+6,1}$ respectively where $\mathfrak{M}'_{h_n,e,1}$ is the set of $\mathrm{Stab}_{\mathcal{U}^{(2)}}(h_n+H_e)$-orbit representative of $\{g+H_{e+1}\mid g\in H_e\}$.

Take $v=\exp(v_7)^y\exp(v_5)^x$ for some integers $x,y\geq 1$ such that $7\nmid x,y$. Let us take $g=(\theta-1)^{e+d}h_n$. Suppose for a contradiction, say $(p^{-1}g+H_{e+1})$ and $(p^{-1}g+H_{e+1})_v$ are in same orbit under the action of $\mathrm{Stab}_{\mathcal{U}^{(2)}}(h_n+H_e)$. Then using (6.10) we have $(p^{-1}g+H_{e+1})_u=(p^{-1}g+H_{e+1})_v$ for some $u\in\mathrm{Stab}_{\mathcal{U}^{(2)}}(h_n+H_e)$. A straightforward

computation shows that $g^u - g^v \in H_{e+d+1}$ which means

$$(\theta-1)^{n+e+d}(\rho_2(u^{-1})-\rho_2(v^{-1}))\nu_2 + (\theta-1)^{-1+e+d}(\rho_3(u^{-1})-\rho_3(v^{-1}))\nu_3 \in H_{e+d+1}.$$

Thus

$$(\theta-1)^{n-1}(\rho_2(u^{-1})-\rho_2(v^{-1}))\nu_2 + (\theta-1)^{-2}(\rho_3(u^{-1})-\rho_3(v^{-1}))\nu_3 \in H_0.$$

By Lemma 6.35 we have $(\rho_2(u^{-1})-\rho_2(v^{-1})) \in T_{-3+n}$ and $(\rho_3(u^{-1})-\rho_3(v^{-1})) \in T_{-2}$. We can choose large p-power of u^{-1} (and with abuse of notation we write the power as u^{-p}) such that we have $(\rho_2(u^{-p})-\rho_2(v^{-1})) \in T_{-3+n}$ and $(\rho_3(u^{-p})-\rho_3(v^{-1})) \in T_{-2}$. Hence we have $(\theta-1)^{n-1}(\rho_2(u^{-p})-\rho_2(v^{-1})) \in T_{-4}$ and $(\theta-1)^{-2}(\rho_3(u^{-p})-\rho_3(v^{-1})) \in T_{-4}$. So by Lemma 6.35,

$$(\theta-1)^{n-1}(\rho_2(u^{-p})-\rho_2(v^{-1}))\nu_2 + (\theta-1)^{-2}(\rho_3(u^{-p})-\rho_3(v^{-1}))\nu_3 \in H_0$$

that is,

$$(\theta-1)^{n+e+d}(\rho_2(u^{-p})-\rho_2(v^{-1}))\nu_2 + (\theta-1)^{-1+e+d}(\rho_3(u^{-p})-\rho_3(v^{-1}))\nu_3 \in H_{e+d+1}.$$

This means $(g+H_{e+d+1})_{u^p} = (g+H_{e+d+1})_v$ which is not possible by Corollary 6.41. This shows that $(p^{-1}g+H_{e+1})$ and $(p^{-1}g+H_{e+1})^v$ are never in the same orbit under the action of $\mathrm{Stab}_{\mathcal{U}^{(2)}}(h_n+H_e)$ whereas $(g+H_{e+d+1})$ and $(g+H_{e+d+1})^v$ are in same orbit under the action of $\mathrm{Stab}_{\mathcal{U}^{(2)}}(h_n+H_{e+d})$ as $v \in \mathrm{Stab}_{\mathcal{U}^{(2)}}(h_n+H_{e+d})$. Hence $|\mathfrak{M}'_{h_n,e,1}| \neq |\mathfrak{M}'_{h_n,e+d,1}|$. Thus the skeleton groups $G_{F_j,j+e(j)}$ and $G_{F_j,j+e(j)+6}$ have different number of immediate descendants. □

The main idea of Theorem 6.38 is the observation that in many instances the d-step parent is a periodic parent; Theorem 6.38 considers this set up for groups at depth $e_p(n)$ because this is the depth that plays a role in the periodicity of type 1, see Section 2.2. At the same time, the condition $p \equiv 5 \bmod 6$ also played a crucial role in proving Theorem 6.38. In Theorem 6.43 we relaxed this condition by considering $\mathcal{G}(7,1)$ and showed that there are pairs of groups at different depths, one being the 6-step parent of the other, where both groups have a 7-group as automorphism group, but non-isomorphic descendent trees. This shows that, in general, one cannot expect that the d-step parent always has an isomorphic descendant tree. Note from [18, Theorem 1.1], in $\mathcal{G}(7,1)$, the depth of the branch $\mathcal{B}_n$ is at most $n+3$ and the depth of the skeleton subgraph $\mathcal{S}_n$ is $n-6$. So if $n = 18+6z$ for some $z \geq 1$ then the depth of $\mathcal{S}_n$ is $12+6z$. The examples given in Theorem 6.43 are the skeleton groups at depth $11+6z$ in the branch $\mathcal{B}_{18+6z}$ for $z \geq 1$. This shows that these examples are occurring deep in the branches.

Chapter 7

Uniserial p-adic Space Groups

Recall from Chapters 2 and 3 that each coclass tree in a coclass graph defines a pro-p-group via the inverse limit of its mainline groups. Each such infinite pro-p-group has a finite hypercenter and the hypercentral quotient is a uniserial p-adic space group of coclass at most r, see Corollary 3.17. We know that infinite pro-p-groups of coclass r, up to isomorphism, are in a one-one correspondence with the coclass trees of $\mathcal{G}(p, r)$ and the mainline groups can be realised as the quotient of the associated pro-p-group. Hence the uniserial p-adic space groups of coclass at most r are significant to study the structure of $\mathcal{G}(p, r)$. For odd primes, a constructive classification of these space groups is given by Eick [30]. For prime $p = 2$, this is still open; see Chapter 3 for a brief discussion. It is the aim of this chapter to provide the necessary theoretical insight to determine and construct the uniserial 2-adic space groups of fixed coclass. We will continue using the notation mentioned in Section 1.2. In particular:

Notation 7.1. For the rest of this chapter, we will abbreviate "uniserial p-adic space group" by "space group".

7.1 Background

Let G be a space group of dimension d. Recall from Chapter 3 that G is an extension of its (characteristic) translation subgroup $T \cong \mathbb{Z}_p^d$ by a point group P acting faithfully and uniserially on T.

Space groups were first investigated by Leedham-Green and Newman in [60] for odd primes and in [55, 73] for $p = 2$. However these results were not conclusive towards any constructive classification. Later, for odd primes, Eick [30] has introduced a variety of results towards a classification of space groups. The case of prime 2 remained mostly

open, but has been partially investigated in the diploma thesis [44]. The case of *quaternion point groups* was not considered in [44]. The aim of this Chapter is to fill this gap. We set some notation first and begin with two definitions.

Notation 7.2. Suppose $R \in \{\mathbb{Q}_p, \mathbb{Z}_p, \mathbb{Q}, \mathbb{Z}\}$. For any positive integer d, let $M_d(R)$ denote the ring of $d \times d$ matrices over R. If $U \leq \mathrm{GL}(d, R)$ then we write $R[U]$ for the subalgebra of $M_d(R)$ generated by U, and define $E_R(U) = C_{M_d(R)}(U)$ and

$$C_R(U) = C_{\mathrm{GL}(d,R)}(U) \quad \text{and} \quad N_R(U) = N_{\mathrm{GL}(d,R)}(U).$$

Definition 7.3. Let $g \otimes h$ denote the Kronecker product of two matrices g and h. Suppose $R \in \{\mathbb{Q}_p, \mathbb{Z}_p, \mathbb{Q}, \mathbb{Z}\}$ and denote by $\mathrm{Sym}(q)$ the symmetric group on q points. By I_n we denote the identity matrix of size $n \times n$.

a) For $M \subseteq M_d(R)$, let $I_q \otimes M = \{I_q \otimes g \mid g \in M\}$.

b) For $M \subseteq \mathrm{Sym}(q)$, let $M \otimes I_d = \{\bar{g} \otimes I_d \mid g \in M\}$, where $\bar{g}$ is the permutation matrix (acting on columns) corresponding to g.

Definition 7.4. A finite p-group is uniserial if there is an embedding into $\mathrm{GL}(d, \mathbb{Z}_p)$ for some $d > 1$ such that its image acts uniserially on the natural module $\mathbb{Z}_p^d$.

Preliminary results and notations required for this chapter are given in Chapter 3. We now briefly recall from [30] how space groups are determined for odd primes. The case $p = 2$ will be considered from Section 7.4 onwards. For $s \geq 1$, we write

$$d_s = \begin{cases} p^{s-1}(p-1) & (p \text{ odd}) \\ 2^s & (p = 2). \end{cases}$$

Since every space group is an extension of its translation subgroup by a point group, it will be necessary to study the corresponding cohomology groups (which paramatrise group extensions). If H is a group and N is an H-module, then the group of corresponding 2-cocycles is

$$\begin{aligned} Z^2(H,N) \;=\; \{\gamma : H \times H \to N \mid \gamma(h,k) + \gamma(l,hk) = \gamma(lh,k) + \gamma(l,h)^k, \\ \gamma(1,h) = \gamma(h,1) = 1 \text{ for all } h,k,l \in H\}; \end{aligned}$$

the corresponding subgroup of 2-coboundaries is

$$\begin{aligned} B^2(H,N) \;=\; \{\gamma \in Z^2(H,N) \mid \text{ there exists } \delta : H \to N \text{ with} \\ \gamma(k,h) = \delta(kh) - \delta(k)^h - \delta(h)\}. \end{aligned}$$

The quotient group is known as the cohomology group

$$H^2(H,N) = Z^2(H,N)/B^2(H,N).$$

The normaliser of a point group $U \leq \mathrm{GL}(d,\mathbb{Z}_p)$ can be used to determine the isomorphism types of extensions of $T = (\mathbb{Z}_p^d, +)$ by U. We briefly recall this process from [30, 69, 70, 88]. First note that $\mathrm{Aut}(T) \cong \mathrm{GL}(d,\mathbb{Z}_p)$ and, by Remark 3.3, every automorphism of T is $\mathbb{Z}_p$-linear. Recall from Section 5.2.1 that for any $U \leq \mathrm{GL}(d,\mathbb{Z}_p)$, the group of compatible pairs of U and T is defined as

$$\mathrm{Comp}(U,T) = \{(\beta,\gamma) \in \mathrm{Aut}(U) \times \mathrm{Aut}(T) \mid (t^g)^\gamma = (t^\gamma)^{g^\beta} \text{ for } t \in T, g \in U\};$$

it acts on $Z^2(U,T)$ via $\delta \mapsto \delta^{(\beta,\gamma)}$, where the latter is defined by

$$\delta^{(\beta,\gamma)}(u,v) = \delta(u^{\beta^{-1}}, v^{\beta^{-1}})^\gamma. \tag{7.1}$$

Moreover, this action leaves $B^2(U,T)$ invariant, hence there is an induced action on $H^2(U,T)$. It is well-known that the orbits of this action classify all extensions of T by U up to *strong isomorphism*, see [30, Section 4]; moreover, if U acts uniserially on T, then T is a characteristic translation subgroup in any such extension; this implies the following.

Theorem 7.5. *If $U \leq \mathrm{GL}(d,\mathbb{Z}_p)$ is uniserial, then the isomorphism types of extensions of T by U correspond to the $\mathrm{Comp}(U,T)$-orbits of elements in $H^2(U,T)$.*

Since $U \leq \mathrm{GL}(d,\mathbb{Z}_p)$ acts faithfully on T, it follows from [48, p. 78] that there is an isomorphism

$$N_{\mathbb{Z}_p}(U) \to \mathrm{Comp}(U,T), \quad g \mapsto (\kappa_{(g^{-1})}, g),$$

where κ_g is the automorphism of U via conjugation by g. Thus from (7.1) we see that, for any uniserial point group $U \leq \mathrm{GL}(d,\mathbb{Z}_p)$, the element $g \in N_{\mathbb{Z}_p}(U)$ acts on $\delta \in Z^2(U,T)$ via $\delta \mapsto \delta^g$, where the latter is defined by

$$\delta^g(u,v) = \delta(u^{g^{-1}}, v^{g^{-1}})^g. \tag{7.2}$$

In conclusion, the next result follows, cf. [30, Theorem 27].

Theorem 7.6. *If $U \leq \mathrm{GL}(d_s,\mathbb{Z}_p)$ is, then the isomorphism types of extensions of T by U correspond to the $N_{\mathbb{Z}_p}(U)$-orbits of elements in $H^2(U,T)$.*

We conclude this section with the notion of Bravais groups since this is one of the main tools in [30] used in the classification of space groups for odd primes.

Definition 7.7. Let $(K, R) \in \{(\mathbb{Q}, \mathbb{Z}), (\mathbb{Q}_p, \mathbb{Z}_p)\}$ and let $G \leq \mathrm{GL}(n, R)$ be finite.

a) The invariant form of G is $\mathcal{F}_K(G) = \{m \in M_n(K) \mid g^\intercal m g = m \text{ for all } g \in G\}$.

b) The Bravais group of G is $B_R(G) = \{g \in \mathrm{GL}(n, R) \mid g^\intercal m g = m \text{ for all } g \in \mathcal{F}_K(G)\}$; we also write $B(G) = B_{\mathbb{Z}}(G)$.

The following can be found in [30, Lemmas 21 and 22].

Lemma 7.8. *If $G, H \leq \mathrm{GL}(n, \mathbb{Z})$ are finite, then the following hold.*

a) *If there is an invertible $f \in \mathcal{F}_K(G)$, then $\mathcal{F}_K(G) = f E_K(G)$,*

b) *$G \leq B(G)$ and $\mathcal{F}_K(G) = \mathcal{F}_K(B(G))$,*

c) *$N_{\mathbb{Z}_2}(G) \leq N_{\mathbb{Z}_2}(B(G))$,*

d) *$B(G) \leq B(H)$ if $G \leq H$.*

In the next sections we briefly describe the algorithm in [30] for odd primes. Later in Section 7.4, when we discuss the case $p = 2$, it will be easy to identify the main differences. The algorithm for odd primes proceeds in two steps: First, the construction of point groups and second, the construction of extensions. The first step depends on some deep results on the structure of point groups. The second step involves results on 2-cohomology and dimension shifting. We briefly describe these steps in the following. All the results and definitions mentioned in Sections 7.2 and 7.3 are from [30].

7.2 Point groups (case $p > 2$)

In this section, p denotes an odd prime; recall that $d_j = p^{j-1}(p-1)$ for all $j \geq 1$. We briefly discuss how the point groups of the uniserial p-adic space groups can be determined; we refer to Section 3.1.3 for preliminary results. In particular recall from Theorem 3.24 that if p is odd then any uniserial point group U is conjugate in $\mathrm{GL}(d_s, \mathbb{Q}_p)$ to a subgroup of $\mathrm{GL}(d_s, \mathbb{Z})$. This is elaborated in the following discussion.

Definition 7.9. Let m_1 be the companion matrix of $1 + x + \ldots + x^{p-1}$ and for $j \geq 2$ define iteratively,

$$m_j = \begin{pmatrix} 0 & I_{d_{j-1}} & 0 & \ldots & 0 \\ 0 & 0 & I_{d_{j-1}} & & 0 \\ \vdots & & \ddots & \ddots & \\ 0 & 0 & \ldots & 0 & I_{d_{j-1}} \\ m_{j-1} & 0 & \ldots & 0 & 0 \end{pmatrix} \in \mathrm{GL}(d_j, \mathbb{Z})$$

and let $M_j = \langle m_j \rangle \leq \mathrm{GL}(d_j, \mathbb{Z})$ for all $j \geq 1$.

The next result is [30, Lemma 6].

Lemma 7.10. *Let $K \in \{\mathbb{Q}, \mathbb{Q}_p\}$. Then $C_K(M_j) = K[M_j] \setminus \{0\}$ and $N_K(M_j) = A_j \ltimes C_K(M_j)$ for some cyclic $A_j \leq \mathrm{GL}(d_j, \mathbb{Z})$ of order d_j.*

Let P be the p-cycle $(1 \dots p) \in \mathrm{Sym}(p)$ and recall from [49, III.15.3] that the i-fold wreath product

$$P_i = P \wr \dots \wr P$$

is a Sylow p-subgroup of $\mathrm{Sym}(p^i)$; it is known that $N_{\mathrm{Sym}(p^i)}(P_i) = K_i \ltimes P_i$ for some abelian K_i of order $(p-1)^i$, see [30, Lemma 7].

In the following we fix an integer $s \geq 1$ and start with [30, Definition 8].

Definition 7.11. For $i \in \{0, \dots, s-1\}$ and $R \in \{\mathbb{Q}, \mathbb{Z}, \mathbb{Q}_p, \mathbb{Z}_p\}$, we define the following.

a) $W_i(s) = M_{s-i} \wr P_i \leq \mathrm{GL}(d_s, \mathbb{Z})$ and $W(s) = W_{s-1}(s)$.

b) $N_i(s) = ((I_{p^i} \otimes A_{s-i}) \times (K_i \otimes I_{d_{s-i}})) \ltimes W_i(s)$ and $N(s) = N_{s-1}(s)$, where A_{s-i} and K_i are defined as above.

Each $N_i(s)$ is a finite subgroup of $\mathrm{GL}(d_s, \mathbb{Z})$; it will be useful to describe the normaliser of $W_i(s)$. The next result is [30, Lemma 12].

Lemma 7.12. *Let $K \in \{\mathbb{Q}, \mathbb{Q}_p\}$ and $R \in \{\mathbb{Z}, \mathbb{Z}_p\}$. The following hold for all $i \in \{0, \dots, s-1\}$.*

a) $C_K(W_i(s)) = (I_{p^i} \otimes K[M_{s-i}]) \setminus \{0\}$.

b) $N_K(W_i(s)) = C_K(W_i(s))N_i(s)$.

c) $N_R(W_i(s)) = C_R(W_i(s))N_i(s)$.

Note that the base group of $W_i(s)$ is a direct product of p^i copies of the cyclic group M_{s-i}. Since $W(s)$ is a s-fold wreath product of cyclic groups, it has a natural generating set of s elements namely $g_1, \dots, g_s$, where g_s corresponds to m_1 in the base group. As a result, $Z(W_i(s)) = I_{p^i} \otimes M_{s-i}$, see [30, p. 627]. The next result is [30, Lemma 10].

Lemma 7.13. *We have $W_0(s) < W_1(s) < \dots < W_{s-1}(s) = W(s)$; each $W_i(s)$ is uniserial and generated by $i+1$ elements $g_1, \dots, g_i, g_{i+1}g_{i+2} \cdots g_s$.*

This result already determines s uniserial subgroups of dimension d_s; the next theorem shows that those subgroups are sufficient to construct all uniserial space groups up to conjugacy. For $k \in \{1, \dots, s\}$ let

$$V_k(s) = W(s)'\langle g_1, \dots, g_{k-1}, g_{k+1}, \dots, g_s \rangle \leq W(s).$$

The next result is [30, Theorem 18].

Theorem 7.14. *Let $U \leq \mathrm{GL}(d_s, \mathbb{Z}_p)$ be finite.*

a) *If U is uniserial, then U is conjugate in $\mathrm{GL}(d_s, \mathbb{Q}_p)$ to a subgroup of $W(s)$.*

b) *If $U \leq W(s)$, then U is uniserial if and only if $U \not\leq V_k(s)$ for $k \in \{1, \ldots, s\}$.*

The next theorem summarises how to construct all uniserial point groups of dimension d_s up to conjugacy in $\mathrm{GL}(d_s, \mathbb{Q}_p)$. The next theorem is a result from [30, p. 631].

Theorem 7.15. *Recall the construction of $N(s) \leq \mathrm{GL}(d_s, \mathbb{Z})$, see Definition 7.11; the following hold.*

a) *If $U \leq W(s)$ is uniserial, then $|Z(U)| = p^k$ for some $k \leq s$ and $Z(U)$ is conjugate in $N(s)$ to $Z(W_{s-k}(s))$.*

b) *Two uniserial subgroups of $U_1, U_2 \leq W(s)$ are conjugate in $\mathrm{GL}(d_s, \mathbb{Q}_p)$ if and only if they are conjugate in $N(s)$.*

c) *In order to find the $\mathrm{GL}(d_s, \mathbb{Q}_p)$-conjugacy classes of uniserial groups, it is sufficient to consider the $N(s)$-classes of the uniserial groups $U \leq W(s)$ with $Z(U) = Z(W_i(s))$ for each $i \in \{0, \ldots, s-1\}$.*

7.3 Construction of extensions ($p > 2$)

We continue with the assumption that p is an odd prime. In this section, $U \leq \mathrm{GL}(d_s, \mathbb{Z}_p)$ is uniserial with natural module $T = \mathbb{Z}_p^{d_s}$. By Theorem 7.15 we can assume $U \leq W(s)$. We now discuss how to determine, up to isomorphism, the extensions of T by U; see [30, Section 4]. Recall that $N_{\mathbb{Z}_p}(U)$ acts on $Z^2(U, T)$ as described in (7.2).

7.3.1 Dimension shifting and coclass

In view of Theorem 7.6, we want to determine the $N_{\mathbb{Z}_p}(U)$-orbits in $H^2(U, T)$. In [30], this is done via *dimension shifting*: this technique relates $H^2(U, T)$ with some 1-cohomology group, which simplifies the computations.

Let $V = \mathbb{Q}_p^{d_s}$ so that $T \leq V$. By Theorem 7.15, we can assume that $Z(U) = Z(W_i(s))$ for some $i \in \{0, 1, \ldots, s-1\}$. By $\mathrm{Fix}_{Z(U)}(V/T)$ we denote the set of fixed points in V/T under the action of $Z(U)$. The next theorem is [30, Theorem 28].

Theorem 7.16. *If $U \leq W(s)$ is uniserial and $Z(U) = Z(W_i(s))$, then $F = \mathrm{Fix}_{Z(U)}(V/T)$ is elementary abelian of rank p^i and $H^2(U, T) \cong H^1(U/Z(U), F)$.*

The action of $N_{\mathbb{Z}_p}(U)$ on $H^2(U, T)$ is translated to an action on $H^1(U/Z(U), F)$ via an explicit isomorphism $H^2(U, T) \to H^1(U/Z(U), F)$; it follows from [30, Theorem 28]

that $g \in N_{\mathbb{Z}_p}(U)$ acts on $\delta \in Z^1(U/Z(U), F)$ via $\delta \mapsto \delta^g$, where the latter is defined by $\delta^g(u) = \delta(u^{g^{-1}})^g$; this induces an action on $H^1(U/Z(U), F)$.

In order to read off coclass of an extension defined by cohomology class in $H^2(U/Z(U), F)$, we need the following result from [30, Theorem 30] and [54, Theorem 3.5].

Theorem 7.17. *Let $U \leq \mathrm{GL}(d_s, \mathbb{Z}_p)$ be uniserial of order p^m with $Z(U) = Z(W_i(s))$; write $F = \mathrm{Fix}_{Z(U)}(V/T)$. There exists a unique series*

$$1 = F(0) < \ldots < F(p^i) = F$$

of U-invariant subgroups. Let $Z(k)$ be the image of $Z^1(U/Z(U), F(k))$ in $H^1(U/Z(U), F)$ and let G be the extension of T by U defined by some cohomology class $\gamma \in H^1(U/Z(U), F)$, via the correspondence $H^1(U/Z(U), F) \cong H^2(U, F)$ as in Theorem 7.16. If j is the smallest index such that $\gamma \in Z(j)$, then G is a space group of coclass $m - j$.

Theorem 7.16 shows that $F = \mathrm{Fix}_{Z(U)}(V/T)$ is an $\mathbb{F}_p$-space of dimension p^i. If $u_1, \ldots, u_t$ is a generating set for U, then we can identify $H^1(U/Z(U), F)$ with a subspace H of F^t via the embedding $\delta \mapsto (\delta(u_1), \ldots, \delta(u_t))$. This identification is used in the following result, which is from [30, Theorems 25 and 34].

Theorem 7.18. *If $U \leq W(s)$ is uniserial with $Z(U) = Z(W_i(s))$, then*

$$N_{\mathbb{Z}_p}(U) = C_{\mathbb{Z}_p}(W_i(s)) N_{N_i(s)}(U)$$

and $C_{\mathbb{Z}_p}(W_i(s))$ acts as the group of scalar matrices on $H^1(U/Z(U), \mathrm{Fix}_{Z(U)}(V/T))$.

We conclude this section with a brief description of the classification algorithm for odd primes; we refer to [30] for more background information. To construct all uniserial p-adic space groups of dimension d_s, up to isomorphism, one first determines all uniserial point groups in $W(s)$ up to $N(s)$-conjugacy (see Theorem 7.15). For each such point group U, one needs to compute the $N_{\mathbb{Z}_p}(U)$-orbits in $H^2(U, T)$, see Theorem 7.6. This computation is simplified by Theorem 7.16 which shows that it is sufficient to determine the $N_{\mathbb{Z}_p}(U)$-orbits in $H^1(U/Z(U), F)$. Theorem 7.18 explains that $C_{\mathbb{Z}_p}(W_i(s))$ acts as scalars on $H^1(U/Z(U), F)$ and that the final step is to fuse those $C_{\mathbb{Z}_p}(W_i(s))$-orbits under the action of $N_{\mathbb{Z}_p}(U)$; the latter group is constructed using a *lattice subgroup algorithm*, and fusion of orbits can be achieved with an orbit-stabiliser algorithm, see [30, Section 5.1] for computational details. We note that Bravais groups play a crucial role in determining the various normalisers computationally, see [30, Section 3.3.3].

In order to determine the uniserial points groups of 2-adic space groups, we first find the largest point group in Theorem 7.19, and then determine which subgroups are uniserial. For any such uniserial U, we describe the centraliser $C_{\mathbb{Z}_2}(U)$ and normaliser $N_{\mathbb{Z}_2}(U)$ in

Section 7.4.3. Unlike in the odd prime case, we were not able to use Bravais groups. In Section 7.5, we find all non-isomorphic extensions of the natural $\mathbb{Z}_p$-module $T = \mathbb{Z}_p^d$ by these uniserial point groups. In view of Theorem 7.6, this can be done by determining the orbits of the action of the normalisers on $H^2(U, T)$. In Theorem 7.35, we provide a dimension shifting argument for prime 2, which allows us to consider a 1-cohomology group instead of $H^2(U, T)$.

7.4 Point groups ($p = 2$)

We first recall the following theorem from [55, Lemma 1.1]. This result will also show that Theorem 3.24 is not true for $p = 2$. In the following let $W_Q(2) = Q_{16}$, the quaternion group of order 16, and inductively define $W_Q(i+1)$ as the wreath product of $W_Q(i)$ by a cyclic group of order 2 for $i \geq 2$.

Theorem 7.19. *If $s \geq 2$ and $U \leq \mathrm{GL}(2^s, \mathbb{Z}_2)$ is a uniserial point group, then U is conjugate in $\mathrm{GL}(2^s, \mathbb{Q}_2)$ to a subgroup of $\mathrm{GL}(2^s, \mathbb{Z})$ or to a subgroup of $W_Q(s)$.*

In order to determine, up to conjugacy, the uniserial point groups for prime 2, we need to consider two cases: the groups that are conjugate to subgroups of $\mathrm{GL}(2^s, \mathbb{Z})$, called *integral point groups*, and the subgroups of $W_Q(s)$ which are not conjugate to subgroups of $\mathrm{GL}(2^s, \mathbb{Z})$, called *quaternion point groups*. The integral point groups are discussed in [44] and those behave similarly to the point groups in the odd prime case. It is the existence of the quaternion point groups which makes the determination of the 2-adic space groups challenging. We concentrate on those point groups in the remainder of this chapter.

7.4.1 Quaternion point groups

Our first objective is to get a matrix representation of the group $W_Q(s)$. Using [55, Section 4], in the following we assume that Q_{16} is given by its 4-dimensional representation $\langle x, y \rangle \leq \mathrm{GL}(4, \mathbb{C})$, where

$$x = \frac{1}{\sqrt{-39}} \begin{pmatrix} 3 & 1 & 2 & 5 \\ 1 & 2 & 5 & -3 \\ 2 & 5 & -3 & -1 \\ 5 & -3 & -1 & -2 \end{pmatrix} \quad \text{and} \quad y = \frac{1}{\sqrt{-39}} \begin{pmatrix} 5 & -3 & -1 & -2 \\ -3 & -1 & -2 & -5 \\ -1 & -2 & -5 & 3 \\ -2 & -5 & 3 & 1 \end{pmatrix}.$$

The element $\alpha = yx$ will be used frequently; note that

$$\alpha = \begin{pmatrix} 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} \in \mathrm{GL}(4, \mathbb{Z}).$$

Remark 7.20. We will show below that x, y can be considered as elements in $\mathrm{GL}(4, \mathbb{Z}_2)$, hence the generators of $W_Q(s)$ with $s \geq 3$ can be defined as $\{g_1, g_2, \ldots, g_s\}$ where each g_i is a $2^s \times 2^s$ matrix defined by $g_{s-1} = \mathrm{diag}(y, I_{2^s-4})$ and $g_s = \mathrm{diag}(x, I_{2^s-4})$, and for $i \in \{1, \ldots, s-2\}$, by

$$g_i = \begin{pmatrix} X_i & 0 \\ 0 & I_{2^s-2^{s-i+1}} \end{pmatrix} \quad \text{where} \quad X_i = \begin{pmatrix} 0 & I_{2^{s-i}} \\ I_{2^{s-i}} & 0 \end{pmatrix}.$$

The next lemma shows that each g_i can be regarded as a matrix in $\mathrm{GL}(2^s, \mathbb{Z}_2)$; in particular, for computational purposes, these generators can be constructed over the algebraic number field $\mathbb{Q}(\sqrt{-39})$.

Lemma 7.21. *If b is an integer with $b \equiv -1 \bmod 8$, then $e^2 = -b$ for some $e \in \mathbb{Z}_2^*$.*

Proof. If e is a square root of $-b$ in $\mathbb{Z}_2$ then $e \equiv 1 \bmod 2$; thus we need to show that there exists $f \in \mathbb{Z}_2$ such that $e = 1 + 2f$ and $(1+2f)^2 = -b$. Note that $(1+2f)^2 = -b$ implies $1 + 4f^2 + 4f = -b$, that is, f satisfies $4f^2 + 4f = -(b+1)$ and $f^2 + f \equiv 0 \bmod 2$ as $(b+1)/4 \equiv 0 \bmod 2$. Now consider the polynomial $x^2 + x$ which only has simple roots in $\mathbb{Q}_2$. By Hensel's Lemma, see [42, Pages 68 and 72], there is a root f of $x^2 + x$ in $\mathbb{Z}_2$. Now $e = 1 + 2f \in \mathbb{Z}_2$ is a root of $-b$. Note that any such root is a unit in $\mathbb{Z}_2$. □

Theorem 7.19, together with Lemma 7.21, demonstrates the main difference between the odd and even prime case. In contrast to Theorem 3.24 (which hold only for $p > 2$), Theorem 7.19 shows that uniserial point groups for $p = 2$ can be conjugate to a subgroup of $W_Q(s) \leq \mathrm{GL}(2^s, \mathbb{Z}_2)$.

7.4.2 Uniserial subgroups of $W_Q(s)$

In this section we will identify the uniserial subgroups of $W_Q(s)$; for this we consider the following subgroups as defined in [55, p. 420].

Definition 7.22. For $s \geq 2$ and $i \in \{0, 1, \ldots, s-1\}$ define the subgroup

$$W_Q^{(i)}(s) = \langle g_1, g_2, \ldots, g_i, g_{i+1} g_{i+2} \cdots g_s \rangle \leq W_Q(s);$$

note that $W_Q^{(s-1)}(s) = W_Q(s)$.

We give more details on those generators. If x, y and α are as in Section 7.4.1, then a direct calculation shows that for $i \leq s-2$ we have

$$g_{i+1}g_{i+2}\cdots g_s = \begin{pmatrix} \beta_{s-i} & \\ & I_{2^s-2^{s-i}} \end{pmatrix} \in \mathrm{GL}(2^s, \mathbb{Z}).$$

where $\beta_2 = \alpha$ and for $s - i \geq 3$,

$$\beta_{s-i} = \begin{pmatrix} & & & & I_{2^{s-i-1}} \\ & & & I_{2^{s-i-2}} & \\ & & \iddots & & \\ & I_4 & & & \\ \alpha & & & & \end{pmatrix} \in \mathrm{GL}(2^{s-i}.\mathbb{Z})$$

An immediate consequence is the following.

Lemma 7.23. *If $i \in \{1, \ldots, s-2\}$, then*

$$W_Q^{(i)}(s) = C_{s,i} \wr P_i$$

where $P_i = \langle g_1, \ldots, g_i \rangle$ is isomorphic to the i-fold wreath product of cyclic groups of order 2, and

$$C_{s,i} = \langle g_{i+1}g_{i+2}\cdots g_s \rangle$$

is cyclic of order 2^{s-i+1}.

We now focus on the structure of $W_Q^{(i)}(s)$. The next remark summarises a few observation; those follows similarly to the odd prime case [30].

Remark 7.24. The following hold.

a) If $i < s-1$, then the base group of $W_Q^{(i)}(s)$ is a direct product of p^i copies of $C_{s,i}$, and [80, Exercise 1.6(14)] shows that the centre of $W_Q^{(i)}(s)$ is the diagonal subgroup

$$Z(W_Q^{(i)}(s)) = I_{2^i} \otimes \langle \beta_{s-i} \rangle.$$

Note that $Z(Q_{16}) = \langle -I_4 \rangle$, and and induction on s shows $Z(W_Q(s)) = I_{2^s-4} \otimes \langle -I_4 \rangle$.

b) There is a subgroup series $W_Q^{(0)}(s) < W_Q^{(1)}(s) < \ldots < W_Q^{(s-1)}(s) = W_Q(s)$.

c) Each $W_Q^{(i)}(s) \leq \mathrm{GL}(2^s, \mathbb{Z}_2)$, and $W_Q^{(i)}(s) \leq \mathrm{GL}(2^i, \mathbb{Z})$ if and only if $i < s-1$.

d) We have $Q_{16} \cap \mathrm{GL}(4, \mathbb{Z}) = \langle \alpha \rangle$; thus, it follows that $U \leq W_Q(s)$ is a subgroup of $\mathrm{GL}(2^s, \mathbb{Z})$ if and only if $U \leq W_Q^{(s-2)}(s)$.

e) We have $C_{W_Q(s)}(Z(W_Q^{(i)}(s))) = W_Q^{(i)}(s)$ for all $i \leq s-1$.

The next result on base groups of wreath products follows from [71, Theorem 9.12].

Lemma 7.25. *The base group of $W_Q^{(i)}(s)$ is characteristic in $W_Q^{(i)}(s)$ for all i and s.*

The uniserial subgroups of $W_Q(s)$ are characterised by the following result, see [60, Theorem 2]. Recall from Section 6.2.2 that if H is finite p-group with class n, then for $i \in \{2, \ldots, n-2\}$, the 2-step centraliser K_i in H is defined to be the centraliser in H of $\gamma_i(H)/\gamma_{i+2}(H)$. It follows from [53, Definition 4.2.3 and Theorem 10.3.2] that the set $\{H_1, \ldots, H_s\}$ of 2-step centralisers in $W_Q(s)$ is exactly the set $\{V_{Q,1}(s), \ldots, V_{Q,s}(s)\}$ where each

$$V_{Q,k}(s) = W_Q(s)'\langle g_1, \ldots, g_{k-1}, g_{k+1}, \ldots, g_s\rangle \leq W_Q(s).$$

Parts a) and b) of the next result are from [60, p. 199]; part c) follows from b) and the fact that $W_Q^{(0)}(s)$ is not contained in any 2-step centraliser.

Theorem 7.26. *Fix $s \geq 2$.*

a) *A subgroup $U \leq W_Q(s)$ is uniserial if and only if U is not contained in any of the 2-step centralisers of $W_Q(s)$.*

b) *A subgroup $U \leq W_Q(s)$ is uniserial if and only if $U \not\leq V_{Q,k}(s)$ for all $k \in \{1, \ldots, s\}$.*

c) *The groups $W_Q^{(i)}(s)$ are uniserial for all $i \in \{0, \ldots, s-1\}$.*

Our next aim is to determine the normaliser of $W_Q(s)$ in $\mathrm{GL}(2^s, \mathbb{Z})$. In the odd prime case, normalisers were constructed using Bravais groups; this was possible because $B_{\mathbb{Z}}(G)$ is finite for finite $G \leq \mathrm{GL}(d_s, \mathbb{Z})$, see [30]. For $p = 2$, however, computer approximations of $B_{\mathbb{Z}_2}(G)$ suggest that the latter group is infinite when G is a quaternion point group. Below we adopt a different approach to construct normalisers. Recall from Lemma 7.23 that P_i is isomorphic to the i-th fold wreath product of $P = \langle (1,2)\rangle$.

7.4.3 Centralisers and normalisers

Recall that the groups $W_Q^{(i)}(s)$ can be realised as matrix groups of degree 2^s over $\mathbb{Z}_2$ for $i \in \{0, \ldots, s-1\}$. In this section, we determine the centralisers and the normalisers of these groups in $\mathrm{GL}(2^s, \mathbb{Z}_2)$. Normalisers are required to determine the extensions of $\mathbb{Z}_2^{2^s}$ by the uniserial point groups, up to isomorphism, see Theorem 7.6. We use several techniques to determine the normalisers of $W_Q(s)$ for $s \geq 2$. Lemma 7.21 shows if we set $\lambda = \sqrt{-39}$ then λx and λy have integer entries; both have determinant 1521. For $s \geq 2$, we define

$$\mathfrak{C}_s = C_{\mathbb{Z}_2}(W_Q(s)) \quad \text{and} \quad \mathfrak{N}_s = N_{\mathbb{Z}_2}(W_Q(s)).$$

The following matrices are necessary to describe the normalisers.

$$L = \begin{pmatrix} 0 & 1 & 0 & -1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ -1 & 0 & 1 & 0 \end{pmatrix} \quad \text{and} \quad M = \begin{pmatrix} 3 & 0 & 2 & 0 \\ 0 & -2 & 0 & 3 \\ 2 & 0 & -3 & 0 \\ 0 & 3 & 0 & 2 \end{pmatrix}.$$

Note that $\det(M) = 169$ and $\det(L) = 4$, so $M \in \mathrm{GL}(4, \mathbb{Z}_2)$.

Lemma 7.27. *We have* $\mathfrak{C}_2 = \{c_1 I_4 + c_2 L \mid c_1 \in \mathbb{Z}_2^* \text{ and } c_2 \in \mathbb{Z}_2\}$.

Proof. Let $H = \{c_1 I_4 + c_2 L \mid c_2 \in \mathbb{Z}_2, c_1 \in \mathbb{Z}_2^*\}$. A straightforward computation shows that if $c_1 I_4 + c_2 L \in H$, then $\det(c_1 I_4 + c_2 L) \equiv c_1^4 \bmod 2$ is a unit in $\mathbb{Z}_2$. It is easy to check that $Lx = xL$ and $Ly = yL$, hence $H \leq \mathfrak{C}_2$. For the converse, let $A \in \mathfrak{C}_2$ and write $A = (a_{ij})$ with each $a_{ij} \in \mathbb{Z}_2$. From $Ax = xA$ and $Ay = yA$ we will get a system of linear equations in the entries of A with coefficients in $\mathbb{Z}_2$. A direct computation shows that a $\mathbb{Q}(\lambda)$-basis of the solution space of the matrix of this system is $\{L, I_4\}$, hence $\mathfrak{C}_2 \leq \{c_1 I_4 + c_2 L \mid c_1, c_2 \in \mathbb{Q}(a)\} \cap \mathrm{GL}(4, \mathbb{Z}_2)$. Since for any $c_1, c_2 \in \mathbb{Q}(a)$ the entries in $c_1 I_4 + c_2 L$ are either c_1 or c_2 or $-c_2$, we deduce $\mathfrak{C}_2 \leq \{c_1 I_4 + c_2 L \mid c_1, c_2 \in \mathbb{Z}_2\} \cap \mathrm{GL}(4, \mathbb{Z}_2)$. As before, $\det(c_1 I_4 + c_2 L) \equiv c_1^4 \bmod 2$, so $c_1 I_4 + c_2 L \in \mathrm{GL}(4, \mathbb{Z}_2)$ if and only if $c_1 \in \mathbb{Z}_2^*$. □

Lemma 7.28. *We have* $\mathfrak{C}_s = I_{2^{s-2}} \otimes \mathfrak{C}_2$ *for* $s \geq 2$.

Proof. We prove the result by induction on s. The case $s = 2$ holds trivially. Now assume the statement of the lemma holds for $s - 1$ for some $s \geq 3$. Let $A \in H$ where $H = I_{2^{s-2}} \otimes \mathfrak{C}_2 = \{I_{2^{s-2}} \otimes g \mid g \in \mathfrak{C}_2\} \leq \mathrm{GL}(2^s, \mathbb{Z}_2)$. From the definition of H it is easy to see that $Ag_i = g_i A$ for $i \in \{1, \ldots, s\}$, hence $H \leq \mathfrak{C}_s$. We now consider $A \in \mathfrak{C}_s$ and write $A = \left(\begin{smallmatrix} A_1 & A_2 \\ A_3 & A_4 \end{smallmatrix}\right)$ where each $A_i \in M_{2^{s-1}}(\mathbb{Z}_2)$. Since A commutes with both g_{s-1} and g_s then a direct computation shows that A_1 commutes with both g'_{s-1} and g'_{s-2}, where $g'_1, \ldots, g'_{s-1}$ are the corresponding generators in $W_Q(s-1)$. Additionally, $A_2 = A_3 = 0$. Moreover $A_1 = A_4$ follows from $Ag_1 = g_1 A$, that is $A = \left(\begin{smallmatrix} A_1 & 0 \\ 0 & A_1 \end{smallmatrix}\right)$ with $A_1 \in \mathrm{GL}(2^{s-1}, \mathbb{Z}_2)$ and hence $A_1 \in \mathfrak{C}_{s-1}$. Thus $\mathfrak{C}_s = I_2 \otimes \mathfrak{C}_{s-1}$. Now the induction hypothesis shows that $\mathfrak{C}_s = I_{2^{s-2}} \otimes \mathfrak{C}_2$. This completes the proof. □

Now we consider the normaliser $\mathfrak{N}_s = N_{\mathbb{Z}_2}(W_Q(s))$; again we start with $s = 2$.

Lemma 7.29. *We have* $\mathfrak{N}_2 = \langle Q_{16}, M, \mathfrak{C}_2 \rangle$.

Proof. Recall that $Q_{16} = \langle x, y \rangle$. We denote by κ_M the automorphism of Q_{16} via conjugation by M. A straightforward computation shows that $\kappa_M(x) = x$ and $\kappa_M(y) = xyx$. The group $J = \langle \mathrm{Inn}(Q_{16}), \kappa_M \rangle$ has order 16 and index 2 in $\mathrm{Aut}(Q_{16})$. In particular, we

have $\langle J, \sigma\rangle = \mathrm{Aut}(Q_{16}$ where σ is the automorphism of Q_{16} that swaps the generators x and y. Recall from Section 7.4.1 that $\alpha = yx \in \mathrm{GL}(4,\mathbb{Z})$ and the subgroup $\langle\alpha\rangle$ is characteristic in Q_{16} of size 8. It turns out that $\sigma(\alpha) = \alpha^7$. Clearly $H = \langle Q_{16}, m, \mathfrak{C}_2\rangle$ lies in $\mathfrak{N}_2$ and H induces the subgroup J of $\mathrm{Aut}(Q_{16})$. We now show that $\mathfrak{N}_2 = H$. Suppose for a contradiction, this is not true, that is there is some element in $\mathfrak{N}_2 \setminus H$ and so $\mathfrak{N}_2$ induces $\mathrm{Aut}(Q_{16})$; recall that J has index 2 in $\mathrm{Aut}(Q_{16})$. Now $\sigma \in \mathrm{Aut}(Q_{16})$ and thus there must be some $A \in \mathfrak{N}_2$ inducing σ. Since $\sigma(\alpha) = \alpha^7$, we have $\alpha^A = \alpha^7$. This implies that A has the following structure

$$A = A(z) = \begin{pmatrix} a & b & c & d \\ b & c & d & -a \\ c & d & -a & -b \\ d & -a & -b & -c \end{pmatrix} \quad \text{for some} \quad z = (a,b,c,d) \in \mathbb{Z}_2^4.$$

Since A induces σ, we also have $Ax - yA = 0$. This yields a system of linear equations in the entries of the matrix A with coefficients in $\mathbb{Z}_2$. A direct computation shows that the null space of the matrix of this system over $\mathbb{Q}_2(\lambda)$ has a basis $\{b_1, b_2\}$ with respect to (a,b,c,d) where $b_1 = (62/11, 13/11, 1, 0)$ and $b_2 = (-13/11, -10/11, 0, 1)$. So for any $c_1, c_1 \in \mathbb{Q}(a)$ we have $c_1b_1 + c_2b_2 = ((62c_1 - 13c_2)/11, (13c_1 - 10c_2)/11, c_1, c_2)$. This shows that $A(z)$ is defined over $\mathbb{Z}_2$ if and only if $z = c_1b_1 + c_2b_2$ with $c_1, c_2 \in \mathbb{Z}_2$. Moreover if $A = A(z)$ for some $z = c_1b_1 + c_2b_2 = (a,b,c,d)$, then a direct computation shows that $\det(A) \equiv a^4 + b^4 + c^4 + d^4 \bmod 2$ and hence

$$\begin{aligned}\det(A) = {} & 53202/14641c_2^4 - 596856/14641c_2^3c_1 + 3999216/14641c_2^2c_1^2 \\ & -12480936/14641c_2c_1^3 + 14819538/14641c_1^4 \equiv 0 \bmod 2.\end{aligned}$$

Note that 14641 is odd but all the numerators in the terms of the above sum are even. This shows that $\det(A(z)) \notin \mathbb{Z}_2^*$ for any choice of $z \in \mathbb{Z}_2^4$, contradicts $A \in \mathrm{GL}(4,\mathbb{Z}_2)$. So there is no element in $\mathfrak{N}_2 \setminus H$, hence $\mathfrak{N}_2 = H$. □

The following lemma will be used to determine the structure of $\mathfrak{N}_s$ for $s \geq 3$.

Lemma 7.30. *If $G \leq \mathrm{GL}(d,\mathbb{Q}_2)$ acts irreducibly on the natural module $\mathbb{Q}_2^d$, then $G \wr P_i \leq \mathrm{GL}(2^n d, \mathbb{Q}_2)$ acts irreducibly on $\mathbb{Q}_2^{2^n d}$ for every $i \geq 0$.*

Proof. Write $G_i = G \wr P_i$ with natural module $V_i = \mathbb{Q}_2^{2^n d}$. We prove the claim by induction on i, the base case $i = 0$ being true by assumption. Now consider $i \geq 1$ and assume the claim is true for G_{i-1}. Note that we can decompose

$$G_i = G_{i-1} \wr C_2 = \langle\sigma\rangle \ltimes (H_1 \times H_2) \quad \text{and} \quad V_i = U_1 \oplus U_2,$$

where each $H_j \cong G_{i-1}$ acts irreducibly on $U_j \cong V_{i-1}$ and σ is an involution swapping U_1 and U_2. Now consider a non-trivial submodule $U \leq V_i$ and write $u \in U$ as $u = u_1 + u_2$ with each $u_j \in U_j$. Since U is invariant under σ, there must be some $u \in U$ with $u_1, u_2 \neq 0$. Since H_1 acts irreducibly on U_1, there is $h \in H_1$ with $u_1^h \neq u_1$, hence $u - u^h = u_1 - u_1^h \in U_1 \setminus \{0\}$; since U is a submodule, it follows that $U_1 \leq U$; analogously, we deduce $U_2 \leq U$, hence $U = V_i$. This proves that G_i acts irreducibly. □

We now determine the structure of $\mathfrak{N}_s$ for $s \geq 3$.

Lemma 7.31. *We have $\mathfrak{N}_s = \mathfrak{N}_2 \wr P_{s-2}$ for $s \geq 2$.*

Proof. We use induction on s. The case $s = 2$ holds trivially and recall the structure of $\mathfrak{N}_2$ from Lemma 7.29. Now we assume that the claim is true for some $s - 1$ with $s \geq 3$. From the proof of Lemma 7.30 we take $W_Q(s) = \langle \sigma \rangle \times (W_Q(s-1) \times W_Q(s-1))$. So $W_Q(s)$ acts on the natural G-module $V = {\mathbb{Q}_2}^{2^s}$ and decompose $V = V_1 \oplus V_2$, where each $V_i \cong {\mathbb{Q}_2}^{2^{s-1}}$ and the base group of $W_Q(s)$ acts as $W_Q(s-1)$ on each V_i. We know that $Q_{16} = \langle x, y \rangle$ acts irreducibly on $\mathbb{Q}_2^4$, see [55, page 418]. So by applying Lemma 7.30 inductively we deduce that $W_Q(s)$ acts irreducibly on V. Note that the base group of $W_Q(s)$ is characteristic in $W_Q(s)$, see Lemma 7.25. By a similar argument as in the proof of Lemma 7.30, we deduce that for any $g \in N_{\mathbb{Q}_2}(W_Q(s))$, the unique decomposition of V^g into $W_Q(s-1) \times W_Q(s-1)$ invariant subspaces is $V_1 \oplus V_2$; in other words, $\{V_1^g, V_2^g\} = \{V_1, V_2\}$. Hence g permutes $\{V_1, V_2\}$ and thus there is a homomorphism $\phi : N_{\mathbb{Q}_2}(W_Q(s)) \to \mathrm{Sym}(2)$. Now we recall that $\sigma \in N_{\mathbb{Q}_2}(W_Q(s))$ also permutes $\{V_1, V_2\}$. Hence $N_{\mathbb{Q}_2}(W_Q(s)) = \langle \sigma \rangle \ltimes \ker(\phi) = N_{\mathbb{Q}_2}(W_Q(s-1)) \wr C_2$ as $\ker(\phi) = N_{\mathbb{Q}_2}(W_Q(s-1)) \times N_{\mathbb{Q}_2}(W_Q(s-1))$. Now $\mathfrak{N}_s = N_{\mathbb{Q}_2}(W_Q(s)) \cap \mathrm{GL}(2^s, \mathbb{Z}_2) = (N_{\mathbb{Q}_2}(W_Q(s-1)) \wr C_2) \cap \mathrm{GL}(2^s, \mathbb{Z}_2) = \mathfrak{N}_{s-1} \wr C_2$, and the induction hypothesis shows that $\mathfrak{N}_s = (\mathfrak{N}_2 \wr P_{s-3}) \wr C_2 = \mathfrak{N}_2 \wr P_{s-2}$. □

We now determine the normaliser of $W_Q^{(i)}(s)$ for all $s \geq 2$ and $i \in \{0, \ldots, s-2\}$; the following proof is using ideas from [44, Satz 46].

Lemma 7.32. *Consider $s \geq 2$ and $i \in \{0, \ldots, s-2\}$. Then*

$$N_{\mathbb{Q}_2}(W_Q^{(i)}(s)) = C_{\mathbb{Q}_2}(W_Q^{(i)}(s)) N_Q^{(i)}(s)$$

where $C_{\mathbb{Q}_2}(W_Q^{(i)}(s)) = I_{2^i} \otimes (\mathbb{Q}_2[C_{s,i}] \setminus \{0\})$, and $N_Q^{(i)}(s) = (I_{2^i} \otimes L_{s-i}) \ltimes W_Q^{(i)}(s)$ for some cyclic $L_{s-i} \leq \mathrm{GL}(2^{s-i}, \mathbb{Z})$ order 2^{s-i}.

Proof. First, we note that $C_{\mathbb{Q}_2}(W_Q^{(i)}(s)) = I_{2^i} \otimes (\mathbb{Q}_2[C_{s,i}] \setminus \{0\})$ follows from [44, Satz 39]. Recall that $W_Q^{(i)}(s) = C_{s,i} \wr P_i$. Clearly $C_{\mathbb{Q}_2}(W_Q^{(i)}(s)) N_Q^{(i)}(s)$ normalises $W_Q^{(i)}(s)$. Recall the structure of $C_{s,i}$ from Lemma 7.23. It remains to show that $N_{\mathbb{Q}_2}(W_Q^{(i)}(s)) \leq$

$C_{\mathbb{Q}_2}(W_Q^{(i)}(s))N_Q^{(i)}(s)$. The base group $B = C_{s,i} \times \ldots \times C_{s,i}$ of $W_Q^{(i)}(s)$ is characteristic by Lemma 7.25. Using [30, Lemma 6] and [44, Satz 42], we have $N_{\mathbb{Q}_2}(C_{s,i}) = L_i \ltimes C_{\mathbb{Q}_2}(C_{s,i})$, where $L_i \in \mathrm{GL}(2^i, \mathbb{Z})$ is cyclic of order 2^i. Thus $N_{\mathbb{Q}_2}(W_Q^{(i)}(s)) \leq N_{\mathbb{Q}_2}(B)$ with

$$N_{\mathbb{Q}_2}(B) = N_{\mathbb{Q}_2}(C_{s,i}) \wr S_{2^i} = (L_{s-i} \ltimes (C_{\mathbb{Q}_2}(C_{s,i}))) \wr S_{2^i}.$$

Note from [30] that $N_{S_{2^i}}(P_i) = P_i$ and so $N_{\mathbb{Q}_2}(W_Q^{(i)}(s)) \leq (L_{s-i} \ltimes C_{\mathbb{Q}_2}(C_{s,i})) \wr P_i$; let H be the base group of this wreath product. It follows that if $h \in H$, then $h \in N_{\mathbb{Q}_2}(W_Q^{(i)}(s))$ if and only if $m^h \leq W_Q^{(i)}(s)$ for all $m \in P_i$. We now claim that if $h \in H \setminus B$, then $h \in N_{\mathbb{Q}_2}(W_Q^{(i)}(s))$ if and only if $h \equiv (I_{2^i} \otimes A) \bmod B$ for some $A \in L_{s-i} \ltimes C_{\mathbb{Q}_2}(C_{s,i})$; by the previous sentence, we have to show that $P_i^h \leq W_Q^{(i)}(s)$ if and only if $h \equiv (I_{2^i} \otimes A) \bmod B$ for some $A \in L_{s-i} \ltimes C_{\mathbb{Q}_2}(C_{s,i})$. To see this, suppose $h \in H \setminus B$ is not congruent $I_{2^i} \otimes A$ modulo B; we show that $P_i^h \not\leq W_Q^{(i)}(s)$. By assumption, there are distinct blocks U and V in h and a permutation matrix $m \in P_i$ such that $U^{-1}V \notin C_{s,i}$ and a permutation matrix $m \in P_i$ such that

$$m^h = \begin{bmatrix} \ddots & & & & \\ & 0 & & U^{-1}V & \\ & & \ddots & & \\ & V^{-1}U & & 0 & \\ & & & & \ddots \end{bmatrix};$$

in particular, $m^h \notin W_Q^{(i)}(s) = C_{s,i} \wr P_i$; this shows that $P_1^h \not\leq W_Q^{(i)}(s)$ as claimed. Conversely, if $h = I_{2^i} \otimes A$ for some $A \in L_{s-i} \ltimes C_{\mathbb{Q}_2}(C_{s,i})$, then $P_1^h \leq W_Q^{(i)}(s)$ follows. This proves the claim, and it follows that

$$N_{\mathbb{Q}_2}(W_Q^{(i)}(s)) \leq P_i \ltimes \langle B, I_{2^i} \otimes (L_{s-i} \ltimes C_{\mathbb{Q}_2}(C_{s,i}))\rangle.$$

Now the claim follows from $C_{\mathbb{Q}_2}(C_{s,i}) = \mathbb{Q}_2[C_{s,i}] \setminus \{0\}$, see [44, Satz 19 and 35], and the structure of $N_Q^{(i)}(s)$ and $C_{\mathbb{Q}_2}(W_Q^{(i)}(s))$ as given in the lemma. □

The proof of the next theorem follows ideas of [30, Theorem 19] and [44].

Theorem 7.33. *Write $Z_i = Z(W_Q^{(i)}(s))$ for $i \in \{0, \ldots s-1\}$. If $U \leq W_Q(s)$ is uniserial, then the following hold.*

a) *The centre $Z(U)$ is cyclic of order 2^k with $k \leq s+1$.*

b) *We have $Z_i \leq Z(U)$ if and only if $U \leq W_Q^{(i)}(s)$ for all $i \leq s-1$.*

c) *If U is not conjugate to a subgroup of $W_Q^{(s-2)}(s)$, then $|Z(U)| = 2$.*

d) *If $U \leq W_Q(s)$ is uniserial such that $|Z(U)| = |Z_i|$ for some $i \leq s-1$, then up to conjugacy $U \leq W_Q^{(i)}(s)$ and $Z(U)$ is conjugate in $W_Q(s)$ to Z_i.*

Proof. In this proof, let $\beta_1 = -I_2$, so that $Z_i = I_{2^i} \otimes \langle \beta_{s-i} \rangle$ for all $i \leq s-1$, see Remark 7.24; each Z_{i+1} has index 2 in Z_i with the exception $[Z_{s-2} : Z_{s-1}] = 4$.

a) The uniseriality of U implies that the action on $\mathbb{Q}_2^{2^s}$ is faithful and irreducible, see [60, p. 201]. Over the algebraic closure $\bar{\mathbb{Q}}_2$ of $\mathbb{Q}_2$, this irreducible $\mathbb{Q}_2$-module splits into a direct sum of irreducible modules (*Galois conjugates*), see [62, Definition 1.5.8, Lemma 1.5.9, Theorem 1.8.4], and U acts faithfully and irreducibly on each of those. Let $\mathbb{C}_2$ be the completion of the algebraic closure of $\mathbb{Q}_2$; since $\mathbb{C}_2 \cong \mathbb{C}$ as fields, see [43, Theorem 6.4.8], this implies that U has a faithful and irreducible complex representation; now [50, 2.32] proves that $Z(U)$ is cyclic. Since $\exp(Q_{16}) = 8$, an induction on s proves that $\exp(W_Q(s)) = 2^{s+1}$, hence $Z(U)$ is cyclic of order at most 2^{s+1}.

b) Suppose $U \leq W_Q^{(i)}(s)$. Then Z_i is centralised by U and UZ_i is a uniserial group by Theorem 7.26. It follows from a) that $Z(UZ_i)$ is a cyclic 2-group; since it contains both $Z(U)$ and Z_i, either $Z(U) < Z_i$ or $Z_i \leq Z(U)$. We show that $Z(U) \not< Z_i$. This holds trivially if $i = s-1$ since in this case $|Z_i| = 2$; in the following let $i < s-1$ and suppose, for a contradiction, that $Z(U) < Z_i$. Let us consider the decomposition $\mathbb{Q}^{2^s} = V_1 \oplus \ldots \oplus V_{2^i}$ according to the wreath product structure of $Z_i = I_{2^i} \otimes \langle \beta_{s-i} \rangle$, where each V_j is a Z_i-module. Since $U \leq W_Q^{(i)}(s)$, the group U permutes the direct summands V_j and the kernel of this action contains $Z(U)$. Up to equivalence, there is a unique faithful irreducible rational representation of the cyclic group of order $2^{s-i+1} = |Z_i|$, and this representation has degree 2^{s-i}, see [29, pp. 104-105]. This implies that each V_j is an irreducible Z_i-module; note that, because of characteristic 0, every module is a direct sum of irreducible modules. Since $Z(U) < Z_i$ by assumption, it follows from the above comment that $Z(U)$ acts reducibly on each V_j. Since U permutes the spaces V_j, it follows that U acts reducibly on $\mathbb{Q}^{2^s}$. This is a contradiction to the fact that U acts uniserially. Thus, $Z_i \leq Z(U)$. Conversely if $Z_i \leq Z(U)$ then $U \leq C_{W_Q(s)}(Z_i) = W_Q^{(i)}(s)$ by Remark 7.24.

c) Suppose for a contradiction that $|Z(U)| > 2$. Recall that $U \leq W_Q(s)$ and by construction, every $u \in U$ is a $2^{s-2} \times 2^{s-2}$ matrix of 4×4 block matrices in $Q_{16} = \langle x, y \rangle$. Let $Q(U)$ be the subgroup of Q_{16} generated by all those blocks. A direct computation shows that if $Q(U) \neq Q_{16}$, then either $Q(U) \leq Q_{16}' \langle x \rangle$, or $Q(U) \leq Q_{16}' \langle y \rangle$, or $Q(U) \leq Q_{16}' \langle \alpha \rangle$ with $\alpha = yx$. Note that $\alpha \in \mathrm{GL}(4, \mathbb{Z})$ and hence the last case is not possible since U is not conjugate to a subgroup of $W_Q^{(s-2)}(s)$. In the first two cases, $U \leq V_{Q,s}(s)$ or $U \leq V_{Q,s-1}(s)$, which is not possible since U is uniserial, see Theorem 7.26. This shows that $Q(U) = Q_{16}$. Next note that, by a) and b), $Z(U)$ is cyclic and contains $\langle -I_{2^s} \rangle$. Since $|Z(U)| > 2$, there is $g \in Z(U)$ with $g^2 = -I_{2^s}$. As recalled above, every element

in $W_Q(s)$ comes from a $2^{s-2} \times 2^{s-2}$ permutation matrix where 1's are replaced by some 4×4 blocks in Q_{16} and 0's are replaced by 4×4 zero blocks. Let $\mathbb{Q}_2^{2^s} = \bigoplus_{j=1}^{2^{s-2}} V_j$ be the corresponding decomposition into 4-dimensional subspaces such that $W_Q(s)$ preserves this decomposition. These subspaces are permuted according to the permutation matrix action. Since U is uniserial, hence irreducible, it follows that the permutation action is transitive. Now we have two cases for the structure of g. We prove below that none of these cases is possible; this proves $|Z(U)| = 2$.

First we consider that g is block-diagonal with $g = \mathrm{diag}(g_1, \ldots, g_{2^{s-2}})$ with each g_j is a 4×4 matrix in Q_{16} acting on V_j; note that each $g_j^2 = -I_4$. Since U is transitive, for every j there is $u_j \in U$ such that u_j maps V_1 to V_j, that is, j-th entry of the diagonal in g^{u_j} is $k^{-1}g_1k$ for some $k \in Q_{16}$. But $g \in Z(U)$, so $g^u = g$ which proves that g_j is conjugate in Q_{16} to g_1. Since $g_1^2 = -I_4$, each g_j has order 4. There are three classes of order 4 elements in Q_{16}, those of x, y, and α^2. So we can assume that $g = \mathrm{diag}(h^{i_1}, \ldots, h^{i_{2^{s-2}}})$ for some $h \in \{x, y, \alpha^2\}$ and $i_j \in \{1, 3\}$. Note that $g \in Z(U)$ and neither of the subgroups $\langle x \rangle$ and $\langle y \rangle$ is normal in Q_{16}. This forces $h = \alpha^2$, hence $g = \mathrm{diag}(\pm h, \ldots, \pm h)$ where the signs can be arbitrary; note that $h^3 = h^{-1} = -h$. Since $\langle h \rangle$ is normal in Q_{16}, for every $w \in Q_{16}$ we have $hw = wh$ or $hw = -wh$; in particular, h is not central, so there exists $w \in Q_{16}$ with $hw = -wh$. Since $w \in Q_{16} = Q(U)$, there is $u \in U$ containing w as a 4×4 block. But then $gu \neq ug$, which contradicts $g \in Z(U)$.

In the second case, g is not block-diagonal, so g can be regarded as a permutation matrix of order 4 or of order 2 (in its action on the subspaces of the decomposition mentioned above). If the permutation action has order 4, then g permutes the V_j as a product of transpositions and 4-cycles. However, since $g^2 = -I_{2^s}$ fixes each V_j, we know that 4-cycles can not occur; so we only consider the latter case. In the following we need to suppose that $s > 3$; for $s \in \{2, 3\}$, part c) can be verified directly by a computation. Suppose g swaps blocks V_i and V_j with $i \neq j$. Recall the structure of an element of $W_Q(s)$ as mentioned above and note that the permutation matrix comes from the iterated wreath product of $(1, 2)$. Since $U \leq W_Q(s)$ and U acts transitively, there is $u \in U$ that swaps V_j with V_k, where $i \neq k \neq j$. But then g^u swaps V_i and V_k, contradicting $g^u = g$ (which holds because of $g \in Z(U)$). This final contradiction shows that there is no $g \in Z(U)$ of order 4, hence $Z(U) = Z_{s-1} \cong C_2$.

d) If $|Z(U)| = |Z_{s-1}|$ then the statement holds trivially. Now let $i \neq s - 1$. If U is not conjugate to a subgroup of $W_Q^{(s-2)}(s)$ then part c) shows that $Z(U) = Z_{s-1}$. Hence in the following we assume, up to conjugacy, that $U \leq W_Q^{(s-2)}(s)$. Part b) and Remark 7.24 show that $8 = |Z_{s-2}| \leq |Z(U)|$. We prove the assertion of the theorem by induction on the index of U in $W_Q^{(s-2)}(s)$. If $U = W_Q^{(s-2)}(s)$, then the claim follows from b). Now suppose $U < W_Q^{(s-2)}(s)$. Since $W_Q^{(s-2)}(s)$ is a finite 2-group, there exists a group H such that $U < H \leq W_Q^{(s-2)}(s)$ and $[H : U] = 2$. By the induction hypothesis, we can assume

(up to conjugacy) that

$$Z(H) = Z_i$$

for $i < s-1$; in particular, $|Z_i| \neq 2$. We now consider two cases.

First, suppose that $Z_i \not\leq U$. Then $H = UZ_i$, and $UZ_i/U \cong Z_i/(U \cap Z_i)$ shows that $Z(U) = U \cap Z_i$ has index 2 in Z_i; recall that $i \neq s-1$. Since Z_i is cyclic, there is a unique subgroup of index 2, and it follows that $Z(U) = U \cap Z_i = Z_{i+1}$. This proves c) for $Z_i \not\leq U$.

Second, suppose that $Z_i \leq U$. If $Z_i = Z(U)$, then the claim follows, so now suppose that $Z_i < Z(U)$. Since $U \leq H$, we have $Z_i = Z(H) \cap U \leq Z(U)$. First consider the case $i = 0$. In this case, $W_Q^{(0)}(s) = Z_0 \leq U$; on the other hand, $U \leq H$ and $Z(H) \leq U$ imply $Z(H) = Z(H) \cap U \leq Z(U)$. Since $Z(H) = Z(W_Q^{(0)}(s)) = W_Q^{(0)}(s)$, part b) shows that $U \leq W_Q^{(0)}(s)$. Hence $U = W_Q^{(0)}(s)$, and so the claim is proved for $i = 0$. Now consider $i > 0$. Since $[H : U] = 2$, both U and $Z(U)$ are normal in H. The group H acts as $H/U \cong C_2$ on $Z(U)$, and the set of fixed points under this action is Z_i. Since $Z(U)$ is a cyclic 2-group of order 2^k, a direct computation shows that every automorphism of $Z(U)$ of order 2 either has 2^{k-1} fixed points or 2 fixed points. The case $|Z_i| = 2$ is not possible, as mentioned before, thus we conclude that $|Z_i| = 2^{k-1}$, and $[Z(U) : Z_i] = 2$. Note that b) implies

$$U \leq H \leq W_Q^{(i)}(s) = C_{s,i} \wr P_i.$$

If $i = 1$, then by assumption $Z_1 < Z(U)$ and hence $|Z(U)| \geq 2^{s+1}$ since $|Z_1| = 2^s$. But $Z(U)$ is cyclic, hence it contains a unique subgroup of order 2^{s+1}. Now by [55, Proposition 2.4] we find that, up to conjugacy, $W_Q^{(0)}(s) = Z_0 \leq Z(U)$. Therefore, using b), this gives $U \leq W_Q^{(0)}(s)$. We now take $i > 1$ and use a similar argument as in c) to show that $U \leq W_Q^{(i-1)}(s)$. Recall that $[Z(U) : Z_i] = 2$ and Z_i is generated by $l_i = I_{2^i} \otimes \beta_{s-i}$. Since $Z(U)$ is cyclic and $U \leq W_Q^{(i)}(s)$, there is a generator $g \in Z(U)$ with $g^2 = l_i$. Note that the generator $l_{i-1} = I_{2^{i-1}} \otimes \beta_{s-i+1}$ of Z_{i-1} satisfies $l_{i-1}^2 = l_i$. The structure of l_i also shows that it has 2^i blocks each of the form β_{s-i}. Similarly, l_{i-1} has 2^{i-1} blocks of the form $\left(\begin{smallmatrix} 0 & I_{2^{s-i}} \\ \beta_{s-i} & 0 \end{smallmatrix}\right)$ and the square of each such block yields $I_2 \otimes \beta_{s-i}$. Similar to c), we note that every matrix in $W_Q^{(i)}(s)$ comes from a $2^i \times 2^i$ permutation matrix, where each 1 is replaced by some block of dimension 2^{s-i} from $C_{s,i}$ and every 0 is replaced by such a 0-block. Let $\mathbb{Q}_2^{2^s} = \bigoplus_{j=1}^{2^i} V_j$ be the corresponding decomposition into 2^{s-i} dimensional subspaces such that $W_Q^{(i)}(s)$ preserves this decomposition. These subspaces are permuted according to the permutation matrix action. The permutation action of l_i on these spaces is trivial and $g^2 = l_i$. If g is block-diagonal with $g = \mathrm{diag}(g_1, g_2, \ldots)$ then $g_1^2 = \beta_{s-i}$, so g_1 has order 2^{s-i+2}; recall from Remark 7.24 that β_{s-i} has order 2^{s-i+1}. However as said before, the blocks of $W_Q^{(i)}(s)$ come from $C_{s,i}$ and therefore, have order at most 2^{s-i+1}. Hence, g cannot have a block-diagonal structure. This means that

g must be swapping pairs of the underlying subspaces of the decomposition mentioned above. In other words, g permutes these spaces as a product of transpositions. Note that U is uniserial, hence irreducible, it follows that the permutation action is transitive. Suppose for a contradiction that $U \not\leq W_Q^{(i-1)}(s)$, then it acts transitively on the blocks of g and these blocks act as transposition on the subspaces mentioned above. Suppose g swaps blocks V_l and V_j with $l \neq j$. Recall the structure of an element of $W_Q^{(i)}(s)$ as mentioned above and note that the permutation matrix comes from the iterated wreath product of $(1,2)$. Since $U(\leq W_Q^{(i)}(s))$ acts transitively, there is $u \in U$ that swaps V_j with V_k, where $l \neq k \neq j$. Then g^u swaps V_l and V_k, contradicting $g^u = g$ (which holds because of $g \in Z(U)$). This shows that

$$U \leq W_Q^{(i-1)}(s).$$

Then b) shows that $Z_{i-1} = Z(U)$ as Z_i has index 2 both in Z_{i-1} and in $Z(U)$. □

Recall the definition of $N_Q^{(i)}(s)$ from the proof of Lemma 7.32. Recall that every uniserial subgroup of $W_Q^{(s-2)}(s)$ is integral and has a cyclic center. Now the structure of $N_{\mathbb{Z}_p}(U)$ can be determined using the same arguments as given in the proof of [44, Theorem 56] for certain uniserial points with cyclic centers; this yields the following theorem.

Theorem 7.34. *If $U \leq W_Q^{(s-2)}(s)$ is uniserial with $Z(U) = Z(W_Q^{(i)}(s))$, then*

$$N_{\mathbb{Z}_p}(U) = C_{\mathbb{Z}_p}(W_Q^{(i)}(s)) N_{N_Q^{(i)}(s)}(U).$$

7.5 Extensions of quaternion point groups

Let $U \leq \mathrm{GL}(2^s, \mathbb{Z}_2)$ be a uniserial point group and let $T = \mathbb{Z}_2^{2^s}$ and $V = \mathbb{Q}_2^{2^s}$. It is well-known that the equivalence classes of extensions of T by U correspond to the elements of the second cohomology group $H^2(U,T)$. As U is a finite group and T has finite rank, $H^2(U,T)$ is a finite group, see [80, Setion 11.4]. Recall the action of $N_{\mathbb{Z}_2}(U)$ on $Z^2(U,T)$ from (7.2). Theorem 7.6 tells us that the isomorphism types of extensions of T by U correspond to the $N_{\mathbb{Z}_2}(U)$-orbits of elements in $H^2(U,T)$. As before, we denote by $\mathrm{Fix}_{Z(U)}(V/T)$ the set of fixed points in V/T under the action of $Z(U)$. As for odd primes, we use dimension shifting to reduce $H^2(U,T)$ to $H^1(U/Z(U), F)$.

Theorem 7.35. *Let $U \leq W_Q(s)$ be uniserial with $Z(U) = Z(W_Q^{(i)}(s))$ for some i; let $F = \mathrm{Fix}_{Z(U)}(V/T)$. Then the following hold.*

a) *The group F is elementary abelian of rank at most 2^s.*

b) $H^2(U,T) \cong H^1(U/Z(U), F)$.

Proof. a) If $i = s-1$, then $Z(U) = \langle -I_{2^s} \rangle$; otherwise we have $Z(U) = \langle I_{2^i} \otimes \beta_{s-i} \rangle$, see Remark 7.24. In any case, $-I_{2^s} \in Z(U)$, which proves that if $f + T \in F$, then $2f \in T$. This shows that $F \leq \frac{1}{2}T/T$, and the latter is elementary abelian of rank 2^s.

b) This is [30, Theorem 28]. □

The isomorphism between $H^2(U,T)$ and $H^1(U,V/T)$ in Theorem 7.35 originates from the short exact sequence $0 \to T \to V \to V/T \to 0$, see [61, Theorem 3.3]. The explicit definition of the map $H^1(U,V/T) \to H^2(U,T)$ can be found in [68, Remark II.1.21] and it follows that the isomorphism between $H^2(U,T)$ and $H^1(U/Z(U),F)$ in Theorem 7.35 is compatible with the action of $N_{\mathbb{Z}_2}(U)$. Hence the orbits of $N_{\mathbb{Z}_2}(U)$ on $H^1(U/Z(U),F)$ correspond to the isomorphism types of extensions of T by U, where $g \in N_{\mathbb{Z}_2}(U)$ acts on $\delta \in Z^1(U,T)$ via $\delta \mapsto \delta^g$, where the latter is defined by

$$\delta^g(u) = \delta(u^{g^{-1}})^g. \tag{7.3}$$

As discussed in Section 7.2, this action leaves $B^1(U/Z(U),F)$ invariant. Thus in order to get the isomorphism types of the space groups, we need to determine the action of $N_{\mathbb{Z}_2}(U)$ on $H^1(U/Z(U),F)$. In Theorem 7.34 the structure of $N_{\mathbb{Z}_2}(U)$ has been determined for $U \leq W_Q^{(s-2)}(s)$. This theorem explains why we are firstly interested in the action of the centraliser of $W_Q^{(i)}(s)$ for $i \in \{0,\dots,s-2\}$. We recall from Theorem 7.35 that F is elementary abelian of rank 2^i and can thus be considered as a $\mathbb{F}_2$-space of dimension 2^i. As before, if $u_1,\dots,u_t$ is a generating set for U, then we can identify the group $H^1(U/Z(U),F)$ with a subspace H of the vector space F^t via $\delta \mapsto (\delta(u_1Z(U)),\dots,\delta(u_tZ(U)))$. Hence from (7.3) we find that an element $c \in C_{\mathbb{Z}_2}(U)$ acts on $\delta \in Z^1(U/Z(U),F)$ via $\delta \mapsto \delta^c$, where the latter is defined by $\delta^c(u) = \delta(u^{c^{-1}})^c$; this induces an action on $H^1(U/Z(U),F)$. Recall that in Section 7.4.3, we determined the structure of $C_{\mathbb{Z}_2}(W_Q^{(i)}(s))$ for $i \in \{0,\dots,s-1\}$.

Theorem 7.36. *Let U be uniserial such that U is conjugate to some subgroup of $W_Q^{(s-2)}(s)$ and $Z(U) = Z(W_Q^{(i)}(s))$ for some $i < s-1$, and write $F = \mathrm{Fix}_{Z(U)}(V/T)$. Then $C_{\mathbb{Z}_2}(W_Q^{(i)}(s))$ acts trivially on $H^1(U/Z(U),F)$.*

Proof. Up to conjugacy we assume $U \leq W_Q^{(s-2)}(s)$. Note that $C_{\mathbb{Q}_2}(W_Q^{(i)}(s)) \cap \mathrm{GL}(d_s,\mathbb{Z}) = C_{\mathbb{Z}_2}(W_Q^{(i)}(s))$ and Lemma 7.32 shows that $C_{\mathbb{Q}_2}(W_Q^{(i)}(s)) = I_{2^i} \otimes (\mathbb{Q}_2[C_{s,i}] \setminus \{0\})$. Since $Z(U) = \langle I_{2^i} \otimes \beta_{s-i} \rangle$, see Remark 7.24, it follows that $C_{\mathbb{Z}_2}(W_Q^{(i)}(s))$ centralises U. Hence $c \in C_{\mathbb{Z}_2}(W_Q^{(i)}(s))$ acts on $\delta \in H^1(U/Z(U),F)$ by $\delta^c : u \mapsto \delta(u)^c$. This action coincides with its natural diagonal linear action on F^t. Next we investigate the action of $C_{\mathbb{Z}_2}(W_Q^{(i)}(s))$ on F. Since $E_{\mathbb{Q}_2}(W_Q^{(i)}(s)) = \mathbb{Q}_2[Z(W_Q^{(i)}(s))] = \mathbb{Q}_2[I_{2^i} \otimes \langle \beta_{s-i} \rangle]$, we have $C_{\mathbb{Z}_2}(W_Q^{(i)}(s)) = \mathbb{Z}_2[c]^*$, where $c = I_{2^i} \otimes \beta_{s-i}$, and so the elements of $C_{\mathbb{Z}_2}(W_Q^{(i)}(s))$ are

$\mathbb{Z}_2$-linear combinations of powers of c. By definition, c acts trivially on F and hence $C_{\mathbb{Z}_2}(W_Q^{(i)}(s))$ acts as $\mathbb{Z}_2^*$ on F; since every unit in $\mathbb{Z}_2$ is congruent to 1 modulo 2, the result follows. □

Recall the definition of $\mathfrak{C}_s = C_{\mathbb{Z}_2}(W_Q(s))$ from Section 7.4.3. We now investigate the action of $\mathfrak{C}_s$ on $H^1(U/Z(U), F)$ for the uniserial subgroups $U \leq W_Q(s)$ with $Z(U) = Z(W_Q(s))$. For any $Y \in M_{2^n}(\mathbb{Z}_2)$ where $n \leq s$, we denote $Y_s = I_{2^{s-n}} \otimes Y \in M_{2^s}(\mathbb{Z}_2)$. Recall the definition of L from Section 7.4.3 and denote $\hat{L} = I_4 + L$; note that $\hat{L} \bmod 2$ has order 2.

Theorem 7.37. *Let $U \leq W_Q(s)$ be uniserial such that U is not conjugate to any subgroup of $W_Q^{(s-2)}(s)$, so $Z(U) = Z(W_Q(s))$; write $F = \mathrm{Fix}_{Z(U)}(V/T)$. Then $C_{\mathbb{Z}_2}(U)$ acts as powers of $\hat{L}_s$ on $H^1(U/Z(U), F)$, in particular, the orbit of $v + T \in F$ under the action of $C_{\mathbb{Z}_2}(U)$ is $\{v + T, v\hat{L}_s + T\}$.*

Proof. We first note from Theorem 7.35 that $F = \frac{1}{2}T/T$. Also from Lemma 7.28 we see that any $c \in C_{\mathbb{Z}_2}(U)$ has the form $c = I_{2^{s-2}} \otimes (c_1 I_4 + c_2 L)$ for some $c_1 \in \mathbb{Z}_2^*$ and $c_2 \in \mathbb{Z}_2$. Now c_1 is a unit, hence $c_1 \equiv 1 \bmod 2$. Also $c_2 \equiv k \bmod 2$ where $k \in \{0, 1\}$. Thus for any $v \in \frac{1}{2}T$ we have $(vc + T) = (v + kvL_s) + T$, that is, $(vc + T)$ is either $v + T$ or $v\hat{L}_s + T$. Hence we have $\{(v + T)c \mid c \in C_{\mathbb{Z}_2}(U)\} = \{v\hat{L}_s^i + T \mid i \geq 0\}$. Note that $v \in \frac{1}{2}T$ and $\hat{L} \bmod 2$ has order 2. Hence the orbit of $v + T$ under the action of $C_{\mathbb{Z}_2}(U)$ is $\{v + T, v\hat{L}_s + T\}$. □

We now discuss how the above results yield a constructive classification of the 2-adic space groups, up to isomorphism. Our construction of 2-adic space groups involves two steps: determining the uniserial point groups (up to conjugacy) and then constructing the extensions by their natural $\mathbb{Z}_2$-modules. First we determine the uniserial point groups. We find the largest point group $W_Q(s)$ in Theorem 7.19. We then determine the 2-step centralisers of $W_Q(s)$ and identify the uniserial point groups (see Theorem 7.26): only those subgroups of $W_Q(s)$ that do not lie in any 2-step centraliser are uniserial. To construct all uniserial 2-adic space groups of dimension 2^s, up to isomorphism, we first show (Theorem 7.33) that it is sufficient to consider uniserial point groups $U \leq W_Q(s)$ with $Z(U) = Z(W_Q^{(i)}(s))$ for some $i \in \{0, \ldots, s-1\}$. In order to construct such uniserial groups one first constructs all $W_Q^{(i)}(s)$ and their centres; then for each i one constructs up to conjugacy subgroups of $W_Q^{(i)}(s)$ that are not conjugate to a subgroup of $W_Q^{(s-1)}(s)$ and that have centre Z_i. For each such point group U, one needs to compute the $N_{\mathbb{Z}_2}(U)$-orbits in $H^2(U, T)$, see Theorem 7.6. This computation is simplified by Theorem 7.35 which shows that it is sufficient to determine the $N_{\mathbb{Z}_2}(U)$-orbits in $H^1(U/Z(U), F)$ where F is elementary abelian as defined in the said theorem. Theorems 7.36 and 7.37 explain

how $C_{\mathbb{Z}_2}(W_Q^{(i)}(s))$ (and $C_{\mathbb{Z}_2}(U)$ for $i = s-1$) acts on $H^1(U/Z(U), F)$. The final step is to fuse (using Theorems 7.31 and 7.34) those centraliser-orbits under the action of $N_{\mathbb{Z}_2}(U)$; for $i < s-1$ the latter group is constructed using a lattice subgroup algorithm (as in the odd prime case), and fusion of orbits can be achieved with an Orbit-Stabiliser algorithm. For $i = s - i$, one needs to determine $N_{\mathbb{Z}_2}(U)$ directly. Theorem 7.33 shows that in such cases $Z(U) = Z_{s-1}$, hence the orbit calculation can be simplified using Theorem 7.37.

References

[1] Hans Ulrich Besche, Bettina Eick, and E. A. O'Brien. A millennium project: constructing small groups. *Internat. J. Algebra Comput.*, 12(5):623–644, 2002.

[2] J. N. S. Bidwell and M. J. Curran. Corrigendum to "The automorphism group of a split metacyclic p-group". [Arch. Math. 87 (2006) 488–497]. *Arch. Math. (Basel)*, 92(1):14–18, 2009.

[3] N. Blackburn. On a special class of p-groups. *Acta Math.*, 100:45–92, 1958.

[4] H. Brown, J. Neubüser, and H. Zassenhaus. On integral groups. I. The reducible case. *Numer. Math.*, 19:386–399, 1972.

[5] H. Brown, J. Neubüser, and H. Zassenhaus. On integral groups. II. The irreducible case. *Numer. Math.*, 20:22–31, 1972/73.

[6] H. Brown, J. Neubüser, and H. Zassenhaus. On integral groups. III. Normalizers. *Math. Comp.*, 27:167–182, 1973.

[7] Harold Brown, Rolf Bülow, Joachim Neubüser, Hans Wondratschek, and Hans Zassenhaus. *Crystallographic groups of four-dimensional space*. Wiley-Interscience [John Wiley & Sons], New York-Chichester-Brisbane, 1978. Wiley Monographs in Crystallography.

[8] Professor Cayley. Desiderata and Suggestions: No. 1. The Theory of Groups. *Amer. J. Math.*, 1(1):50–52, 1878.

[9] Professor Cayley. Desiderata and Suggestions: No. 2. The Theory of Groups: Graphical Representation. *Amer. J. Math.*, 1(2):174–176, 1878.

[10] Professor Cayley. Desiderata and Suggestions: No. 3.The Newton-Fourier Imaginary Problem. *Amer. J. Math.*, 2(1):97, 1879.

[11] Professor Cayley. Desiderata and Suggestions: No. 4. Mechanical Construction of Conformable Figures. *Amer. J. Math.*, 2(2):186, 1879.

[12] Martin Couson. Character degrees of finite p-groups by coclass. *J. Algebra*, 418:91–109, 2014.

[13] Septimiu Crivei and cStefan cSuteu SzöllHosi. Subgroup lattice algorithms related to extending and lifting abelian groups. *Int. Electron. J. Algebra*, 2:54–70, 2007.

[14] Charles W. Curtis and Irving Reiner. *Representation theory of finite groups and associative algebras*. Pure and Applied Mathematics, Vol. XI. Interscience Publishers, a division of John Wiley & Sons, New York-London, 1962.

[15] J.L. de Lagrange. Réflexions sur la résolution algébrique des équations. *Nouveaux mémoires de l'Académie royale des sciences et belles-lettres de Berlin*, 1770.

[16] Max Dehn. *Papers on group theory and topology*. Springer-Verlag, New York, 1987. Translated from the German and with introductions and an appendix by John Stillwell.

[17] Heiko Dietrich. *Periodic structures in the graph associated with p-groups of maximal class*. PhD thesis, Technische Universität Carolo-Wilhelmina zu Braunschweig, 2009.

[18] Heiko Dietrich. A new pattern in the graph of p-groups of maximal class. *Bull. Lond. Math. Soc.*, 42(6):1073–1088, 2010.

[19] Heiko Dietrich. Periodic patterns in the graph of p-groups of maximal class. *J. Group Theory*, 13(6):851–871, 2010.

[20] Heiko Dietrich and Bettina Eick. Finite p-groups of maximal class with 'large' automorphism groups. *J. Group Theory*, 20(2):227–256, 2017.

[21] Heiko Dietrich, Bettina Eick, and Dörte Feichtenschlager. Investigating p-groups by coclass with GAP. In *Computational group theory and the theory of groups*, volume 470 of *Contemp. Math.*, pages 45–61. Amer. Math. Soc., Providence, RI, 2008.

[22] Heiko Dietrich and Subhrajyoti Saha. A note on skeleton groups in coclass graphs. *Internat. J. Algebra Comput.*, 29(1):127–146, 2019.

[23] J. D. Dixon, M. P. F. du Sautoy, A. Mann, and D. Segal. *Analytic pro-p groups*, volume 61 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, second edition, 1999.

[24] Stephen Donkin. Space groups and groups of prime-power order. VIII. Pro-p-groups of finite coclass and p-adic Lie algebras. *J. Algebra*, 111(2):316–342, 1987.

[25] Marcus du Sautoy. Counting p-groups and nilpotent groups. *Inst. Hautes Études Sci. Publ. Math.*, (92):63–112 (2001), 2000.

[26] David S. Dummit and Richard M. Foote. *Abstract algebra*. John Wiley & Sons, Inc., Hoboken, NJ, third edition, 2004.

[27] Walther Dyck. Gruppentheoretische Studien. *Math. Ann.*, 20(1):1–44, 1882.

[28] Walther Dyck. Gruppentheoretische Studien. II. Ueber die Zusammensetzung einer Gruppe diskreter Operationen, über ihre Primitivität und Transitivität. *Math. Ann.*, 22(1):70–108, 1883.

[29] Beno Eckmann. *Mathematical survey lectures 1943–2004*. Springer-Verlag, Berlin, 2006.

[30] Bettina Eick. Determination of the uniserial space groups with a given coclass. *J. London Math. Soc. (2)*, 71(3):622–642, 2005.

[31] Bettina Eick. Automorphism groups of 2-groups. *J. Algebra*, 300(1):91–101, 2006.

[32] Bettina Eick. Schur multiplicators of finite p-groups with fixed coclass. *Israel J. Math.*, 166:157–166, 2008.

[33] Bettina Eick and David J. Green. Cochain sequences and the Quillen category of a coclass family. *J. Aust. Math. Soc.*, 102(2):185–204, 2017.

[34] Bettina Eick, C. R. Leedham-Green, M. F. Newman, and E. A. O'Brien. On the classification of groups of prime-power order by coclass: the 3-groups of coclass 2. *Internat. J. Algebra Comput.*, 23(5):1243–1288, 2013.

[35] Bettina Eick and Charles Leedham-Green. On the classification of prime-power groups by coclass. *Bull. Lond. Math. Soc.*, 40(2):274–288, 2008.

[36] Dörte Feichtenschlager. *Symbolic computation with infinite sequences of p-groups with fixed coclass*. PhD thesis, Technische Universität Carolo-Wilhelmina zu Braunschweig, 2010.

[37] H. Finken, J. Neubüser, and W. Plesken. Space groups and groups of prime-power order. II. Classification of space groups by finite factor groups. *Arch. Math. (Basel)*, 35(3):203–209, 1980.

[38] É. Galois. Mémoire sur les conditions de résolubilité des équations par radicaux. *J. Math. Pure. Appl.*, 11:417–433, 1846.

[39] The GAP Group. *GAP – Groups, Algorithms, and Programming, Version 4.8.4*, 2016. `http://www.gap-system.org`.

[40] Oihana Garaialde Ocaña. Cohomology of uniserial p-adic space groups with cyclic point group. *J. Algebra*, 493:79–88, 2018.

[41] Marek Golasiński and Daciberg Lima Gonçalves. Spherical space forms—homotopy types and self-equivalences. In *Categorical decomposition techniques in algebraic topology (Isle of Skye, 2001)*, volume 215 of *Progr. Math.*, pages 153–165. Birkhäuser, Basel, 2004.

[42] Fernando Q. Gouvêa. *p-adic numbers*. Universitext. Springer-Verlag, Berlin, second edition, 1997. An introduction.

[43] Fernando Q. Gouvêa. *A guide to groups, rings, and fields*, volume 48 of *The Dolciani Mathematical Expositions*. Mathematical Association of America, Washington, DC, 2012. MAA Guides, 8.

[44] Christian Greve. Rationale Uniserielle 2-adische Raumgruppen. Diploma thesis, Institut Computational Mathematics, TU Braunschweig, Germany, 2006.

[45] Helmut Hasse. *Number theory*. Classics in Mathematics. Springer-Verlag, Berlin, german edition, 2002. Reprint of the 1980 English edition [Springer, Berlin], Edited and with a preface by Horst Günter Zimmer.

[46] Graham Higman. Enumerating p-groups. I. Inequalities. *Proc. London Math. Soc. (3)*, 10:24–30, 1960.

[47] Graham Higman. Enumerating p-groups. II. Problems whose solution is PORC. *Proc. London Math. Soc. (3)*, 10:566–582, 1960.

[48] 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.

[49] B. Huppert. *Endliche Gruppen. I.* Die Grundlehren der Mathematischen Wissenschaften, Band 134. Springer-Verlag, Berlin-New York, 1967.

[50] I. Martin Isaacs. *Character theory of finite groups*. Academic Press [Harcourt Brace Jovanovich, Publishers], New York-London, 1976.

[51] C. R. Leedham-Green. Pro-p-groups of finite coclass. *J. London Math. Soc. (2)*, 50(1):43–48, 1994.

[52] C. R. Leedham-Green. The structure of finite p-groups. *J. London Math. Soc. (2)*, 50(1):49–67, 1994.

[53] C. R. Leedham-Green and S. McKay. *The structure of groups of prime power order*, volume 27 of *London Mathematical Society Monographs. New Series*. Oxford University Press, Oxford, 2002. Oxford Science Publications.

[54] C. R. Leedham-Green, S. McKay, and W. Plesken. Space groups and groups of prime-power order. V. A bound to the dimension of space groups with fixed coclass. *Proc. London Math. Soc. (3)*, 52(1):73–94, 1986.

[55] C. R. Leedham-Green, S. McKay, and W. Plesken. Space groups and groups of prime power order. VI. A bound to the dimension of a 2-adic space group with fixed coclass. *J. London Math. Soc. (2)*, 34(3):417–425, 1986.

[56] C. R. Leedham-Green and Susan McKay. On p-groups of maximal class. I. *Quart. J. Math. Oxford (2)*, 27(107):297–311, 1976.

[57] C. R. Leedham-Green and Susan McKay. On p-groups of maximal class. II. *Quart. J. Math. Oxford Ser. (2)*, 29(114):175–186, 1978.

[58] C. R. Leedham-Green and Susan McKay. On p-groups of maximal class. III. *Quart. J. Math. Oxford Ser. (2)*, 29(115):281–299, 1978.

[59] C. R. Leedham-Green and Susan McKay. On the classification of p-groups of maximal class. *Quart. J. Math. Oxford Ser. (2)*, 35(139):293–304, 1984.

[60] C. R. Leedham-Green and M. F. Newman. Space groups and groups of prime-power order. I. *Arch. Math. (Basel)*, 35(3):193–202, 1980.

[61] C. R. Leedham-Green and W. Plesken. Some remarks on Sylow subgroups of general linear groups. *Math. Z.*, 191(4):529–535, 1986.

[62] Klaus Lux and Herbert Pahlings. *Representations of groups*, volume 124 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 2010. A computational approach.

[63] A. Mann. A featured online review for the papers [52] and [83]. `www.ams.org/mathscinet/search/publdoc.html?pg1=MR&r=1&s1=1258908&vfpref=html`, 1994.

[64] Ursula Martin. Almost all p-groups have automorphism group a p-group. *Bull. Amer. Math. Soc. (N.S.)*, 15(1):78–82, 1986.

[65] S. McKay. The precise bound to the coclass of space groups. *J. London Math. Soc. (2)*, 50(3):488–500, 1994.

[66] G. A. Miller. On Several Points in the Theory of the Groups of a Finite Order. *Amer. Math. Monthly*, 5(8-9):196–199, 1898.

[67] G. A. Miller. Book Review: Theory of Groups of a Finite Order. *Bull. Amer. Math. Soc.*, 6(9):390–398, 1900.

[68] J.S. Milne. Class field theory (v4.02), 2013. Available at www.jmilne.org/math/.

[69] Jürgen Neukirch. *Algebraic number theory*, volume 322 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1999. Translated from the 1992 German original and with a note by Norbert Schappacher, with a foreword by G. Harder.

[70] Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg. *Cohomology of number fields*, volume 323 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, second edition, 2008.

[71] Peter M. Neumann. On the structure of standard wreath products of groups. *Math. Z.*, 84:343–373, 1964.

[72] M. F. Newman. Determination of groups of prime-power order. In *Group theory (Proc. Miniconf., Australian Nat. Univ., Canberra, 1975)*, pages 73–84. Lecture Notes in Math., Vol. 573, 1977.

[73] M. F. Newman and E. A. O'Brien. Classifying 2-groups by coclass. *Trans. Amer. Math. Soc.*, 351(1):131–169, 1999.

[74] M. F. Newman, E. A. O'Brien, and M. R. Vaughan-Lee. Groups and nilpotent Lie rings whose order is the sixth power of a prime. *J. Algebra*, 278(1):383–401, 2004.

[75] E. A. O'Brien and M. R. Vaughan-Lee. The groups with order p^7 for odd prime p. *J. Algebra*, 292(1):243–258, 2005.

[76] J. Opgenorth, W. Plesken, and T. Schulz. Crystallographic algorithms and tables. *Acta Cryst. Sect. A*, 54(5):517–531, 1998.

[77] I. B. S. Passi, Mahender Singh, and Manoj K. Yadav. Automorphisms of abelian group extensions. *J. Algebra*, 324(4):820–830, 2010.

[78] Wilhelm Plesken. The Bravais group and the normalizer of a reducible finite subgroup of $GL(n, \mathbb{Z})$. *Comm. Algebra*, 5(4):375–396, 1977.

[79] Alain M. Robert. *A course in p-adic analysis*, volume 198 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2000.

[80] Derek J. S. Robinson. *A course in the theory of groups*, volume 80 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1996.

[81] P. Ruffini. Teoria generale delle equazioni, in cui si dimostra impossibile la soluzione algebraica delle equazioni generali di grado superiore al quarto. *Bologna, stamperia di s. Tommaso d́aquino*, 1799.

[82] A. Shalev and E. I. Zel' manov. Pro-p groups of finite coclass. *Math. Proc. Cambridge Philos. Soc.*, 111(3):417–421, 1992.

[83] Aner Shalev. The structure of finite p-groups: effective proof of the coclass conjectures. *Invent. Math.*, 115(2):315–345, 1994.

[84] Charles C. Sims. Enumerating p-groups. *Proc. London Math. Soc. (3)*, 15:151–166, 1965.

[85] M. L. Sylow. Théorèmes sur les groupes de substitutions. *Math. Ann.*, 5(4):584–594, 1872.

[86] Michael Vaughan-Lee. Non-PORC behaviour in groups of order p^7. *J. Algebra*, 500:30–45, 2018.

[87] Michael Vaughan-Lee. Graham Higman's PORC theorem. *Int. J. Group Theory*, 8(4):11–28, 2019.

[88] L. R. Vermani. *An elementary approach to homological algebra*, volume 130 of *Chapman & Hall/CRC Monographs and Surveys in Pure and Applied Mathematics*. Chapman & Hall/CRC, Boca Raton, FL, 2003.

[89] A. Wiman. Über p-Gruppen von maximaler Klasse. *Acta Math.*, 88:317–346, 1952.