J. Group Theory **20** (2017), 227–256
DOI 10.1515/jgth-2016-0036

Finite p-groups of maximal class with 'large' automorphism groups

Heiko Dietrich and Bettina Eick

Communicated by Evgenii I. Khukhro

Abstract. The classification of p-groups of maximal class still is a wide open problem. Coclass Conjecture W proposes a way to approach such a classification: It suggests that the coclass graph $\mathcal{G}$ associated with the p-groups of maximal class can be determined from a finite subgraph using certain periodic patterns. Here we consider the subgraph $\mathcal{G}^*$ of $\mathcal{G}$ associated with those p-groups of maximal class whose automorphism group orders are divisible by $p-1$. We describe the broad structure of $\mathcal{G}^*$ by determining its so-called skeleton. We investigate the smallest interesting case $p = 7$ in more detail using computational tools, and propose an explicit version of Conjecture W for $\mathcal{G}^*$ for arbitrary $p \geq 7$. Our results are the first explicit evidence in support of Conjecture W for a coclass graph of infinite width.

1 Introduction

The investigation of the p-groups of maximal class was initiated by Blackburn [1], and has had a long history since then; we refer to the book of Leedham-Green and McKay [11] for details and references. A central tool is the *coclass graph* $\mathcal{G}$ associated with the p-groups of maximal class: the vertices of $\mathcal{G}$ are identified with isomorphism type representatives of the considered groups, and there is an edge $G \to H$ if and only if $H/\gamma(H) \cong G$, where $\gamma(H)$ is the last non-trivial term of the lower central series of H. Investigating the structure of $\mathcal{G}$ is an approach towards a detailed understanding (and thus towards a possible classification) of the associated groups.

It is well known that $\mathcal{G}$ consists of an isolated vertex corresponding to the cyclic group of order p^2, and an infinite *coclass tree* whose root is an elementary abelian group of order p^2. This tree has a single infinite path starting at its root; the groups on this infinite path $S_2 \to S_3 \to \cdots$ satisfy $|S_n| = p^n$ and are the lower central

This research was supported by a Go8-DAAD Joint Research Co-operation Scheme, project "Groups of Prime-Power Order and Coclass Theory". The second author was also supported by an ARC DECRA (Australia), project DE140100088.

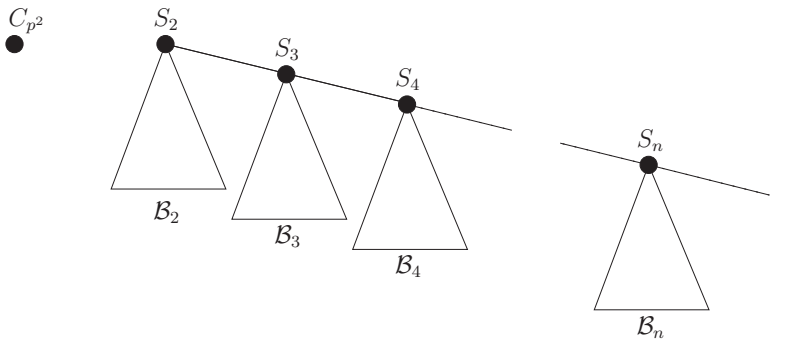

Figure 1. The coclass graph $\mathcal{G}$ with its coclass tree and branches $\mathcal{B}_n$.

series quotients of the (unique) infinite pro-p-group of maximal class. Proofs of these facts and further background information can also be found in [11].

We need some graph-theoretic notation to describe $\mathcal{G}$ in more detail. If there is a path of length k from a group G to a group H in $\mathcal{G}$, then H is a (k-step) *descendant* of G, and G is the (k-step) parent of H; a 1-step descendant is an *immediate descendant* of G. For $n \in \mathbb{N}$ the *branch* $\mathcal{B}_n$ of $\mathcal{G}$ is the subtree generated by all descendants of S_n which are not descendants of S_{n+1}. Note that every branch $\mathcal{B}_n$ is a finite tree with root S_n, and the whole coclass tree of $\mathcal{G}$ is partitioned into its branches, which are connected via the infinite path, see Figure 1. In conclusion, the structure of $\mathcal{G}$ is determined by the structure of its branches.

The *depth* of a vertex in a rooted tree is its distance from the root; the *depth* of a rooted tree is the maximal depth of a vertex. For $k \in \mathbb{N}$ the pruned branch $\mathcal{B}_n(k)$ is the subtree of $\mathcal{B}_n$ generated by all groups of depth at most k in $\mathcal{B}_n$. It was proved independently by du Sautoy [18] and Eick and Leedham-Green [8] that for each $k \in \mathbb{N}$ there exists $l(k) > 0$ such that $\mathcal{B}_{n+p-1}(k) \cong \mathcal{B}_n(k)$ for all $n \geq l(k)$. Thus the pruned branches eventually repeat periodically; we call this the *first periodicity*.

If $p \in \{2, 3\}$, then all branches in $\mathcal{G}$ have depth 1 and therefore can be described by the first periodicity. For larger p, however, the depth of the branches lies between $n - m$ and $n + m - 3$ for $m = 2p - 8$, see for example [4, Theorem 1.2]. Hence, the first periodicity is *not* capable of describing $\mathcal{G}$ completely. It remains to understand how the branches grow beyond their pruned versions. The work of Leedham-Green and McKay (see [10, 11] and the references there) sheds some light on this. We call a group in $\mathcal{G}$ *capable* if it is not a leaf, and we define the *skeleton* $\mathcal{S}_n$ as the subtree of $\mathcal{B}_n$ generated by all capable groups at depth at most $n - m$ in $\mathcal{B}_n$. Leedham-Green and McKay [10] introduced a construction for certain skeleton groups and they showed how the isomorphism problem for these

groups is related to number theory over the p-adic rational numbers; we briefly recall and then extend this in Section 4.

We say that $\mathcal{G}$ has *finite width* if the number of groups of fixed depth in $\mathcal{B}_n$ is bounded by a constant independent of n. It is known that $\mathcal{G}$ has finite width if and only if $p \leq 5$. This indicates that $p = 5$ is a special case. Indeed, in this case the branches are small enough to be accessible to computer investigations. Moreover, the associated groups are significantly easier to study theoretically than the groups for larger primes. Further references and a more detailed description of explicit results are given in Appendix A.

The situation changes considerably for $p \geq 7$. Here the graph $\mathcal{G}$ has infinite width and its branches are too complex for a detailed (computational) investigation. In particular, it is also an open question whether or not the groups of maximal class can be classified by an investigation of $\mathcal{G}$. If such a classification is at all possible, then Coclass Conjecture W (see [9]) proposes an approach: it suggests that there exists an integer k such that for each $n \geq k$ the branch $\mathcal{B}_{n+p-1}$ can be constructed from $\mathcal{B}_n$ using *two* types of periodic patterns. One of these patterns is the first periodicity, the other could be called a *second periodicity*. We note that the description of the second periodicity in Conjecture W is rather vague and not as explicit as the first periodicity; this may be part of the reason why it is so difficult to investigate. We emphasise that there is only very little evidence for Conjecture W so far and that *all* the available evidence is in coclass trees of finite width. We exhibit further details on Conjecture W in Appendix A.

1.1 Main results

We consider an arbitrary prime $p \geq 7$, which is fixed throughout this paper, and define constants

$$d = p - 1, \quad \ell = \frac{p-3}{2}, \quad m = 2p - 8.$$

We use the notation $\mathcal{G}$, $\mathcal{B}_n$, $\mathcal{S}_n$ defined above. The aim of this paper is to study the subgraph $\mathcal{G}^*$ of $\mathcal{G}$ generated by all groups whose automorphism group order is divisible by d. More precisely, we investigate $\mathcal{G}^*$ with a view towards understanding the periodicities proposed by Conjecture W; if there is any chance to prove Conjecture W at all, then it seems useful to understand first the possible periodicities in more detail. We denote by $\mathcal{B}_n^*$ and $\mathcal{S}_n^*$ the subgraphs of $\mathcal{B}_n$ and $\mathcal{S}_n$ contained in $\mathcal{G}^*$; these are both subtrees of $\mathcal{B}_n$. Our first result is a complete determination of the skeletons $\mathcal{S}_n^*$; see Section 6 for its proof.

Theorem 1.1. *Let* $n \geq \max\{m, 8\}$.

(a) *The skeleton* $\mathcal{S}_n^*$ *has* ℓ *groups at depth* 1*; we denote these by* $G_{n,1}, \ldots, G_{n,\ell}$.

(b) *Let H be a descendant of $G_{n,i}$ at depth $e < n - m$ in $\mathcal{S}_n^*$. Then H has p immediate descendants in $\mathcal{S}_n^*$ if and only if $(e \bmod d) \in \{2, 4, \ldots, d-2\} \setminus \{d - 2i\}$; otherwise, H has one immediate descendant in $\mathcal{S}_n^*$.*

Theorem 1.1 exhibits that each skeleton $\mathcal{S}_n^*$ consists of ℓ subtrees starting at depth 1 and each subtree has a well-described branching pattern depending on the parameter i of the root of the subtree. The next corollary is an immediate consequence.

Corollary 1.2. *Let $n \geq \max\{m, 8\}$ and $e < n-m$. The number of groups at depth e in $\mathcal{S}_n^*$ is at least $\ell p^{\lfloor e/d \rfloor (\ell-1)}$; in particular, $\mathcal{G}^*$ has infinite width.*

We have determined $\mathcal{B}_n^*$ for $p = 7$ and $10 \leq n \leq 18$ by computer, cf. Section 1.2. Based on this, we formulate a conjectural description for $\mathcal{B}_n^*$ for arbitrary $p \geq 7$. To describe this conjecture, we define the *twig* $\mathcal{W}_G^*$ of a group G in $\mathcal{S}_n^*$: this is the subtree of $\mathcal{B}_n^*$ with root G containing all descendants of G which are not descendants of any proper descendant of G in $\mathcal{S}_n^*$. Thus each group of $\mathcal{B}_n^*$ is contained in exactly one twig and the twigs of $\mathcal{B}_n^*$ are connected by the skeleton of $\mathcal{B}_n^*$. We continue to denote the groups of depth 1 in a skeleton $\mathcal{S}_n^*$ by $G_{n,1}, \ldots, G_{n,\ell}$ and we assume that these are sorted via Theorem 1.1 (b). Note that every group G of depth at least 1 in $\mathcal{S}_n^*$ has exactly one of the groups $G_{n,i}$ as parent.

Conjecture 1.3. There exists $l \geq m$ such that for all $n \geq l$ and for each G of depth e at least 1 in $\mathcal{S}_n^*$ with parent $G_{n,i}$ the following holds.

(a) If G is not a leaf in $\mathcal{S}_n^*$, then the isomorphism type of the graph $\mathcal{W}_G^*$ depends on the index i, on e mod d, and on n mod d only.

(b) If G is a leaf in $\mathcal{S}_n^*$, then there exists a group $\overline{G}$ with parent $G_{n-d,i}$ at depth $e - d$ in $\mathcal{S}_{n-d}^*$ with $\mathcal{W}_G^* \cong \mathcal{W}_{\overline{G}}^*$.

Conjecture 1.3 suggests that there are three types of twigs: the twigs of the leaves in $\mathcal{S}_n^*$, the twigs of the roots of $\mathcal{S}_n^*$, and the twigs of the other skeleton groups. Note that, by definition, $\mathcal{W}_G^*$ has depth at most 1 for every group G in $\mathcal{S}_n^*$ which is not a leaf. We choose l large enough such that the first periodicity holds for all groups of depth 1 in $\mathcal{B}_n^*$; then the twigs of the roots in $\mathcal{S}_n^*$ behave periodically for all $n \geq l$ and thus there are at most $l + d$ different twigs of roots in $\mathcal{G}^*$. Conjecture 1.3 suggests that for $n \geq l$ there are only ℓd^2 different twigs in $\mathcal{S}_n^*$ for groups that are neither roots nor leaves. The twigs of the leaves of $\mathcal{S}_n^*$ are trees of depth at most $2m + 3$. Conjecture 1.3 suggests that there are finitely many different twigs of skeleton-leaves; more precisely, if the skeleton $\mathcal{S}_n^*$ has w_n

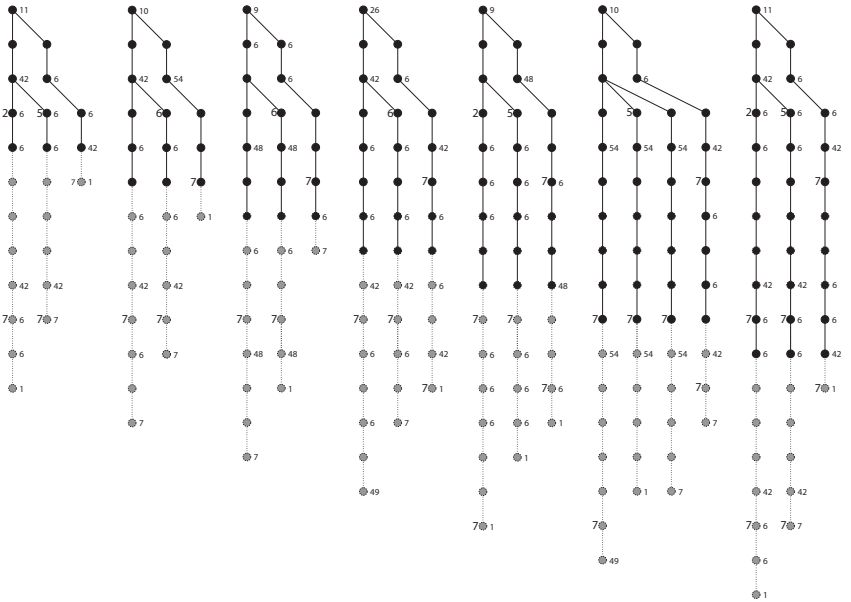

Figure 2. The branches $\mathcal{B}_n^*$ (and skeleton $\mathcal{S}_n^*$) for $p = 7$ and $n = 10, \ldots, 16$.

leaves, then Conjecture 1.3 proposes that there are at most $w_{l+1} + \cdots + w_{l+d}$ different twigs arising for the leaves in all $\mathcal{S}_n^*$ with $n \geq l$.

1.2 Computations for $p = 7$

We have computed some branches for $p = 7$ (and partial branches for $p = 11$) using the computer algebra system GAP [20] and the GAP package AnuPQ which is based on [16]. Figure 2 illustrates Conjecture 1.3 with the branches $\mathcal{B}_{10}^*, \ldots, \mathcal{B}_{16}^*$ for $p = 7$. The black parts of the graphs and the bold numbers on the left of vertices describe the skeletons: a number k on the left of a vertex indicates that this vertex and all of its descendants appear k times with the same parent. A number w on the right of a vertex says that this vertex has w immediate descendants in addition to the displayed descendants. The grey parts of the graphs are twigs of the leaves in $\mathcal{S}_n^*$.

1.3 Structure of the paper

In Section 2 we recall some p-adic number theory; these results are important for defining the groups in the skeleton and for solving their isomorphism problem. In Section 4 we recall the construction of the skeleton groups in $\mathcal{S}_n$, and we consider

their isomorphism problem and automorphism groups. In Section 5 we then investigate the skeleton groups in $\mathcal{S}_n^*$ in more detail. In particular, we show how they can be constructed up to isomorphism. In Section 6, we prove Theorem 1.1. Appendix A contains a short survey on known periodicity results for coclass graphs.

2 Some number theory

Throughout the paper, $\mathbb{Q}_p$ and $\mathbb{Z}_p$ denote the field of p-adic rational numbers and ring of p-adic integers, respectively. The p-th cyclotomic polynomial

$$1 + x + \cdots + x^{p-1} \in \mathbb{Q}_p[x]$$

is irreducible; we consider a fixed root θ and define $K = \mathbb{Q}_p(\theta)$, so that K is a field extension of degree $d = p - 1$ over $\mathbb{Q}_p$, with $\mathbb{Q}_p$-basis $\{1, \theta, \ldots, \theta^{d-1}\}$. For $a \in \mathbb{Z}$ with $p \nmid a$ the field automorphism $\sigma_a \colon K \to K$ is defined by $\sigma_a(\theta) = \theta^a$. The Galois group of K is $\mathrm{Gal}(K) = \{\sigma_a \mid 1 \leq a \leq d\}$; it is cyclic and we fix a generator $\sigma = \sigma_k$. The equation order $\mathcal{O} = \mathbb{Z}_p[\theta]$ is the maximal order of K; it has $\{1, \theta, \ldots, \theta^{d-1}\}$ as $\mathbb{Z}_p$-basis, and a unique maximal ideal $\mathfrak{p} = (\theta - 1)$. We abbreviate $\kappa = \theta - 1$, so that $(\kappa^m) = \mathfrak{p}^m$ for $m \in \mathbb{Z}$; this defines a series of ideals through $\mathcal{O}$. For $z \in \mathbb{Z}$ and $n \in \mathbb{N}$ we denote by $(\mathfrak{p}^z)^n$ the direct sum of n copies of $\mathfrak{p}^z$ (and not the ideal $\mathfrak{p}^{nz}$). For each non-zero $w \in K$ there exist unique $z \in \mathbb{Z}$ and a unit $u \in \mathbb{Z}_p[\theta]^*$ such that $w = \kappa^z u$; we call $\mathrm{val}(w) = z$ the valuation of w. Note that if $v, w \in K$ are non-zero, then $\mathrm{val}(vw) = \mathrm{val}(v) + \mathrm{val}(w)$. We extend this definition to non-zero n-tuples $\boldsymbol{v} \in K^n$, so that $\mathrm{val}(\boldsymbol{v}) = z$ if and only if $\boldsymbol{v} \in (\mathfrak{p}^z)^n \setminus (\mathfrak{p}^{z+1})^n$.

2.1 Eigenvalues

The generator σ of the Galois group of K can be considered as a $\mathbb{Q}_p$-linear map of K. The next lemma determines its eigenvalues; it is proved in [10, Lemma 2.3] for $z \geq 0$, but the same proof holds for all $z \in \mathbb{Z}$.

Lemma 2.1. *The eigenvalues of the $\mathbb{Q}_p$-linear map $\sigma : K \to K$ are $\omega^0, \ldots, \omega^{d-1}$ and each eigenspace has dimension 1. If $w \in K$ with $\mathrm{val}(w) = z$ is an eigenvector of σ, then the corresponding eigenvalue is ω^z. For every $z \in \mathbb{Z}$ there exists an eigenvector w of σ with $\mathrm{val}(w) = z$.*

2.2 The group of units

Let $\mathcal{U}$ be the unit group of $\mathcal{O}$. For $i \geq 2$ define $\mathcal{U}_i = 1 + \mathfrak{p}^i$, and let ω be a primitive d-th root of unity in $\mathbb{Z}_p$; we assume throughout that ω is chosen such that

$\omega \equiv k \bmod p$ where k is defined by the fixed generator $\sigma = \sigma_k$ of $\mathrm{Gal}(K)$. It is shown in [13, Satz II.5.3] that

$$\mathcal{U} = \langle\omega\rangle \times \langle\theta\rangle \times \mathcal{U}_2.$$

The unit group of $\mathbb{Z}_p$ is $\mathbb{Q}_p \cap \mathcal{U}$, that is, $\mathbb{Z}_p^* = \langle\omega\rangle \times (1 + p\mathbb{Z}_p)$. In the course of the paper we will need various maps based on these unit groups. The following lemma investigates one of them.

Lemma 2.2. *The map* $\chi\colon \mathcal{U} \to \mathcal{U}$, $u \mapsto u\sigma(u)^{-1}$, *is a group homomorphism with* $\ker\chi = \mathbb{Z}_p^*$ *and* $\mathcal{U} = \ker\chi \times \operatorname{im}\chi$.

Proof. Since σ generates $\mathrm{Gal}(K)$, the fixed points of σ in K are exactly the elements of the subfield $\mathbb{Q}_p$ of K, hence $\ker\chi = \mathcal{U} \cap \mathbb{Q}_p = \mathbb{Z}_p^*$. Next, we consider the restriction of χ to $\mathcal{U}_2 = 1 + \mathfrak{p}^2$. As shown in [13, Satz II.5.5 and p. 146], the additive group of $\mathfrak{p}^2$ is isomorphic to the multiplicative group $\mathcal{U}_2$ via

$$\exp\colon (\mathfrak{p}^2, +) \to (\mathcal{U}_2, \cdot), \quad x \mapsto \sum_{k=0}^{\infty} \frac{x^k}{k}!.$$

As this exponential map is compatible with the action of σ, we can translate χ to a map $\psi\colon \mathfrak{p}^2 \to \mathfrak{p}^2$, $x \mapsto x - \sigma(x)$. Since σ is a diagonalisable $\mathbb{Z}_p$-linear map on $\mathfrak{p}^2$ with eigenvalues $\omega^0, \omega^1, \ldots, \omega^{d-1}$, the map ψ is diagonalisable with eigenvalues $0, 1-\omega^1, \ldots, 1-\omega^{d-1}$. Now note that if $i \in \{1, \ldots, d-1\}$, then $1 - \omega^i \not\equiv 0 \bmod p$, so $1 - \omega^i \in \mathbb{Z}_p^*$; moreover, Lemma 2.1 implies that there exists an eigenvector of ψ in $\mathfrak{p}^2 \setminus \mathfrak{p}^3$. In conclusion, we have shown that

$$\mathfrak{p}^2 = \ker\psi \oplus \operatorname{im}\psi,$$

and hence $\mathcal{U}_2$ is the direct product of $\ker\chi$ and $\operatorname{im}\chi$ restricted to $\mathcal{U}_2$. Finally, note that $\chi(\omega) = 1$ and $\chi(\theta) = \theta^{1-k}$. Thus the result follows from the decomposition of $\mathcal{U}$ as $\mathcal{U} = \langle\omega\rangle \times \langle\theta\rangle \times \mathcal{U}_2$. □

3 The infinite pro p-group of maximal class

The following lemma shows how the structure of K relates to the infinite pro-p-group of maximal class, see [11, Proposition 8.3.2]. From now on, we denote by $T = (\mathcal{O}, +)$ the additive group of the ring $\mathcal{O}$, and let P be the cyclic group of order p generated by θ. We let P act on T by multiplication.

Lemma 3.1. *The semidirect product* $S = T \rtimes P$ *is an infinite pro-*p*-group of coclass* 1.

The unique maximal S-invariant series through T is $T = T_1 > T_2 > \cdots$, where each $T_i = (\mathfrak{p}^{i-1}, +)$. Moreover, if $i \geq 2$, then $T_i = \gamma_i(S)$ is the i-th term in the lower central series of S. For $i \in \mathbb{N}$ define $S_i = S/\gamma_i(S)$, so that $S_2 \to S_3 \to \cdots$ is the unique maximal infinite path in $\mathcal{G}$. The automorphism groups of S and its quotients S_i are described in the following lemma from [4, Section 4.2]; it implies that the maximal path $S_2 \to S_3 \to \cdots$ is contained in $\mathcal{G}^*$.

Lemma 3.2. *Writing elements of S as tuples (t, θ^i) with $t \in T$ and $i \in \mathbb{Z}$, the following hold:*

(a) *The natural restriction $\pi\colon \mathrm{Aut}(S) \to \mathrm{Aut}(T)$, $\alpha \mapsto \alpha|_T$, satisfies*

$$\mathrm{im}\,\pi \cong \mathcal{U} \rtimes \mathrm{Gal}(K) \quad \textit{and} \quad \ker \pi \cong Z^1(P, T).$$

A preimage of $(u, \sigma_b) \in \mathcal{U} \rtimes \mathrm{Gal}(K)$ under π is given by

$$\alpha(u, b)\colon S \to S, \quad (t, \theta^i) \mapsto (u\sigma_b(t), \theta^{ib}).$$

The kernel of π is generated by $\{\alpha(1), \alpha(\theta), \ldots, \alpha(\theta^{d-1})\}$, where for $s \in T$ we define

$$\alpha(s)\colon S \to S, \quad (t, \theta^i) \mapsto (t + (1 + \theta + \cdots + \theta^{i-1})s, \theta^i).$$

(b) *If $i \geq 4$, then the natural projection $\mathrm{Aut}(S) \to \mathrm{Aut}(S_i)$ is surjective and $|\mathrm{Out}(S_i)| = p^{i-2}d^2$.*

4 The skeleton groups in $\mathcal{S}_n$

In this section we describe the construction of skeleton groups and their isomorphism problem, based on results of Leedham-Green and McKay [10], see also [11, Section 8.2]. A key ingredient in that construction is homomorphisms from the exterior square $T \wedge T$: this is the $\mathbb{Z}_p P$-module generated by $s \wedge t$ with $s, t \in T$ such that for all $s, s', t \in T$ and $z \in \mathbb{Z}_p$ the following holds: $s \wedge s = 0$, hence $s \wedge t = -(t \wedge s)$, and $z(s \wedge t) = (zs) \wedge t = s \wedge (zt)$, and $(s \wedge t) + (s' \wedge t) = (s + s') \wedge t$. The group P acts diagonally on $T \wedge T$, which defines the $\mathbb{Z}_p P$ action on $T \wedge T$.

In the following let $n \geq \max\{m, 8\}$ and $e \in \{0, \ldots, n - m\}$. Every surjective homomorphism $f \in \mathrm{Hom}_P(T \wedge T, T_n)$ defines an associative multiplication on T/T_{n+e} via

$$(t + T_{n+e}) \circ (s + T_{n+e}) = t + s + \frac{1}{2} f(t \wedge s) + T_{n+e}.$$

We denote the resulting group by $M_{n,e}(f)$. It is not difficult to show that $M_{n,e}(f)$ has class 2 and derived subgroup $M_{n,e}(f)' = T_n/T_{n+e}$. Since f is a P-module homomorphism, the multiplication in $M_{n,e}(f)$ is compatible with the action of P, and we can define the group

$$C_{n,e}(f) = M_{n,e}(f) \rtimes P;$$

these groups are called *constructible* in [11]. Each group $C_{n,e}(f)$ is an extension of the natural S_n-module T_n/T_{n+e} by the group S_n on the infinite path of $\mathcal{G}$; in particular, it is a group of depth e in the skeleton $\mathcal{S}_n$. By [4, Theorem 1.3], the groups $C_{n,e}(f)$ are exactly the groups in the skeleton $\mathcal{S}_n$.

4.1 The structure of $\mathrm{Hom}_P(T \wedge T, T)$

The structure of $\mathrm{Hom}_P(T \wedge T, T)$ has been investigated by Leedham-Green and McKay. We recall some of the results here for completeness, as we need them in later applications. We refer to [11, Sections 8.2 and 8.3] for further details.

First, $T \wedge T = F \oplus Z$, where F is a $\mathbb{Z}_p P$-module of rank $\ell = (p-3)/2$ generated by $\kappa^i \wedge \kappa^{i-1}$ with $i = 1, \ldots, \ell$, and Z is a free $\mathbb{Z}_p$-module of rank 1. Let δ_{ij} denote the Kronecker-delta and recall that σ_a is an element of $\mathrm{Gal}(K)$ for $p \nmid a$. For $i \in \{1, \ldots, \ell\}$ we define $\mathbb{T}_i \in \mathrm{Hom}_P(T \wedge T, T)$ via

$$\mathbb{T}_i(\kappa^j \wedge \kappa^{j-1}) = \delta_{ij} \quad \text{and} \quad \mathbb{T}_i(z) = 0 \text{ for } z \in Z.$$

For $2 \le a \le \ell + 1$ we define $\mathbb{S}_a \in \mathrm{Hom}_P(T \wedge T, T)$ via

$$\mathbb{S}_a(x \wedge y) = \sigma_a(x)\sigma_{1-a}(y) - \sigma_{1-a}(x)\sigma_a(y).$$

For an ℓ-tuple $\boldsymbol{c} = (c_1, \ldots, c_\ell) \in K^\ell$ let

$$\mathbb{S}(\boldsymbol{c}) = c_1\mathbb{S}_2 + \cdots + c_\ell \mathbb{S}_{\ell+1} \quad \text{and} \quad \mathbb{T}(\boldsymbol{c}) = c_1\mathbb{T}_1 + \cdots + c_\ell \mathbb{T}_\ell.$$

For $a \in \{2, \ldots, \ell + 2\}$ and $i \in \{1, \ldots, \ell\}$ let

$$b_{a,i} = (\theta^a - \theta^{1-a})((\theta^a - 1)(\theta^{1-a} - 1))^{i-1},$$

and define the $\ell \times \ell$-matrix B over K as

$$B = \begin{pmatrix} b_{2,1} & b_{2,2} & \ldots & b_{2,\ell} \\ b_{3,1} & b_{3,2} & \ldots & b_{3,\ell} \\ \vdots & \vdots & \ddots & \vdots \\ b_{\ell+1,1} & b_{\ell+1,2} & \ldots & b_{\ell+1,\ell} \end{pmatrix} \in K^{\ell \times \ell}.$$

The next lemma is proved in [11, Theorems 8.3.1 and 8.3.7] and the proof of [11, Proposition 8.3.8].

Lemma 4.1. *Let* $f \in \mathrm{Hom}_P(T \wedge T, T)$.

(a) *There exists a unique* $\boldsymbol{c} \in \mathcal{O}^\ell$ *with* $f = \mathbb{T}(\boldsymbol{c})$.

(b) *There exists a unique* $\boldsymbol{d} \in K^\ell$ *with* $f = \mathbb{S}(\boldsymbol{d})$.

(c) *The matrix* B *describes a base change from* $\{\mathbb{S}_2, \ldots, \mathbb{S}_{\ell+1}\}$ *to* $\{\mathbb{T}_1, \ldots, \mathbb{T}_\ell\}$, *that is,* $\boldsymbol{c} = \boldsymbol{d}B$.

If $\boldsymbol{c} \in \mathcal{O}^\ell$, then both $\mathbb{T}(\boldsymbol{c})$ and $\mathbb{S}(\boldsymbol{c})$ lie in $\mathrm{Hom}_P(T \wedge T, T)$. By Lemma 4.1, $\{\mathbb{T}_1, \ldots, \mathbb{T}_\ell\}$ forms an $\mathcal{O}$-basis for $\mathrm{Hom}_P(T \wedge T, T)$. There exists $\boldsymbol{c} \in K^\ell \setminus \mathcal{O}^\ell$ with $\mathbb{S}(\boldsymbol{c}) \in \mathrm{Hom}_P(T \wedge T, T)$, which shows that the set $\{\mathbb{S}_2, \ldots, \mathbb{S}_{\ell+1}\}$ generates $\mathrm{Hom}_P(T \wedge T, T)$, but not as an $\mathcal{O}$-module. Nonetheless, the latter generating set plays an important role in the solution of the isomorphism problem, see Section 4.2.

The groups at depth e in $\mathcal{S}_n$ can be obtained as $C_{n,e}(\mathbb{S}(\boldsymbol{c}))$, where $\mathbb{S}(\boldsymbol{c})$ has image T_n; thus we define

$$\begin{aligned}
\Gamma_n &= (\mathfrak{p}^{n-1})^\ell B^{-1},\\
\Delta_n &= \{\boldsymbol{c} \in K^\ell \mid C_{n,e}(\mathbb{S}(\boldsymbol{c})) \in \mathcal{S}_n\}\\
&= \Gamma_n \setminus \Gamma_{n+1},\\
\Delta_{n,e}^* &= \{\boldsymbol{c} \in K^\ell \mid C_{n,e}(\mathbb{S}(\boldsymbol{c})) \in \mathcal{S}_n^*\} \subseteq \Delta_n.
\end{aligned}$$

Note that $\Delta_n = \kappa\Delta_{n-1}$.

For the next lemma, recall the definition of the valuation given in Section 2.

Lemma 4.2. *For* $i = 1, \ldots, \ell$ *let* $\boldsymbol{t_i}$ *be the* i*-th row of* B^{-1}.

(a) *We have* $\mathbb{T}_i = \mathbb{S}(\boldsymbol{t_i})$ *and* $\mathrm{val}(\boldsymbol{t_i}) = -2i + 1$.

(b) *If* $\boldsymbol{v} = a_1\boldsymbol{t_1} + \cdots + a_\ell\boldsymbol{t_\ell} \in \Delta_1$ *with each* $a_i \in K$, *then*

$$\mathrm{val}(\boldsymbol{v}) = \min\{\mathrm{val}(a_i\boldsymbol{t_i}) \mid i = 1, \ldots, \ell\}.$$

Proof. (a) The proof of [11, Proposition 8.3.8] shows that $\det(B) \in \mathfrak{p}^{\ell^2} \setminus \mathfrak{p}^{\ell^2+1}$, hence B is invertible over K. By Lemma 4.1, the i-th row $\boldsymbol{t_i}$ of B^{-1} satisfies $\mathbb{T}_i = \mathbb{S}(\boldsymbol{t_i})$; it remains to analyse the valuation of $\boldsymbol{t_i}$. It is straightforward to see that each entry $b_{a,i}$ of B has valuation $\mathrm{val}(b_{a,i}) = \mathfrak{p}^{2i-1}$, hence

$$B = U\,\mathrm{diag}(\kappa, \kappa^3, \ldots, \kappa^{2\ell-1}),$$

where U is an $\ell \times \ell$ matrix with entries in $\mathcal{U}$ only. Since $\det(B) \in \mathfrak{p}^{\ell^2} \setminus \mathfrak{p}^{\ell^2+1}$, this implies that $\det(U) \in \mathcal{U}$. Moreover,

$$B^{-1} = \mathrm{diag}(\kappa^{-1}, \kappa^{-3}, \ldots, \kappa^{-2\ell+1})U^{-1}.$$

Since $\det(U) \in \mathcal{U}$, Cramer's rule for matrix inverses shows that each entry of U^{-1} lies in $\mathcal{O}$. Since $\det(U^{-1}) \in \mathcal{U}$, each row and column of U^{-1} contains at least one element in $\mathcal{O} \setminus \mathfrak{p}$. In conclusion, the valuation of the i-th row of U^{-1} is 0, hence the valuation of the i-th row of B^{-1} is $-2i + 1$.

(b) Let $\mu = \min\{\mathrm{val}(a_i \boldsymbol{t_i}) \mid i = 1, \ldots, \ell\}$, $J = \{i \in 1, \ldots, \ell \mid \mathrm{val}(a_i \boldsymbol{t_i}) = \mu\}$. Clearly, $\mathrm{val}(\boldsymbol{v}) \geq \mu$, and we have to show equality. If $|J| = 1$, then $\mathrm{val}(\boldsymbol{v}) = \mu$ follows readily; thus we suppose $J = \{i_1, \ldots, i_n\}$ with $i_1 < \cdots < i_n$ and $1 < n$. Note that $\mathrm{val}(\boldsymbol{v}) = \mu$ if and only if

$$\mathrm{val}(a_{i_1} \boldsymbol{t_{i_1}} + \cdots + a_{i_n} \boldsymbol{t_{i_n}}) = \mu. \tag{4.1}$$

Since $\mathrm{val}(a_{i_j} \boldsymbol{t_{i_j}}) = \mu$ for all j, we can assume that $\mu = 0$: simply replace $\boldsymbol{v}$ by a multiple $\kappa^{-\mathrm{val}(\boldsymbol{v})} \boldsymbol{v}$. By part (a), each $\mathrm{val}(\boldsymbol{t_{i_j}}) = -2i_j + 1$, so $\mathrm{val}(a_{i_j} \boldsymbol{t_{i_j}}) = 0$ implies $\mathrm{val}(a_{i_j}) = 2i_j - 1$, that is, there is a uniquely defined $c_{i_j} \in \{1, \ldots, p-1\}$ such that

$$a_{i_j} \boldsymbol{t_i} \equiv c_{i_j} \kappa^{2i_j - 1} \boldsymbol{t_i} \bmod (\mathfrak{p})^\ell.$$

Suppose, for a contradiction, that (4.1) is false, that is,

$$\mathrm{val}(a_{i_1} \boldsymbol{t_{i_1}} + \cdots + a_{i_n} \boldsymbol{t_{i_n}}) > 0.$$

This means that $a_{i_1} \boldsymbol{t_{i_1}} + \cdots + a_{i_n} \boldsymbol{t_{i_n}} \in (\mathfrak{p})^\ell$, and so

$$c_{i_1} \kappa^{2i_1 - 1} \boldsymbol{t_{i_1}} + \cdots + c_{i_n} \kappa^{2i_n - 1} \boldsymbol{t_{i_n}} \in (\mathfrak{p})^\ell.$$

In other words, if (4.1) is false, then there are $c_1, \ldots, c_\ell \in \{0, \ldots, p-1\}$, not all 0, such that

$$c_1 \kappa^1 \boldsymbol{t_1} + c_2 \kappa^3 \boldsymbol{t_2} + \cdots + c_\ell \kappa^{2\ell - 1} \boldsymbol{t_\ell} \in (\mathfrak{p})^\ell. \tag{4.2}$$

We show that this is not possible; then (4.1) must be true, and then so is the claim of the lemma.

Since the rows of B^{-1} are $\boldsymbol{t_1}, \ldots, \boldsymbol{t_\ell}$, equation (4.2) is false if and only if the rows of the matrix

$$M = \mathrm{diag}(\kappa, \kappa^3, \ldots, \kappa^{2\ell-1}) B^{-1} \in \mathcal{O}^{\ell \times \ell}$$

are linearly independent over $\mathcal{O}/\mathfrak{p}$, which is isomorphic to the field with p-elements. This is the case if and only if M is invertible over $\mathcal{O}/\mathfrak{p}$, if and only if

$$M^{-1} = B \,\mathrm{diag}(\kappa^{-1}, \kappa^{-3}, \ldots, \kappa^{-2\ell+1}) \in \mathcal{O}^{\ell \times \ell}$$

is invertible over $\mathcal{O}/\mathfrak{p}$. It follows from the definition of the entries $b_{a,i}$ of B that

$$B = \mathrm{diag}(x_2, \ldots, x_{\ell+1}) V(z_2, \ldots, z_{\ell+1}) \,\mathrm{diag}(\kappa^1, \kappa^3, \ldots, \kappa^{2\ell-1}),$$

where

$$x_a = \theta^{1-a}(1 + \theta + \cdots + \theta^{2a-2}),$$
$$z_a = (1 + \theta + \cdots + \theta^{a-1})(1 + \theta + \cdots + \theta^{-a}) \quad \text{for all } a,$$

and $V(z_2, \ldots, z_{\ell+1})$ is a Vandermonde matrix with parameters $z_2, \ldots, z_{\ell+1}$. This yields

$$M^{-1} = \operatorname{diag}(x_2, \ldots, x_{\ell+1})V(z_2, \ldots, z_{\ell+1}).$$

Note that each $x_a \equiv (2a - 1 \bmod p) \bmod \mathfrak{p} \neq 0$, and all $z_a \equiv (-a^2 + a \bmod p) \bmod \mathfrak{p} \neq 0$ are pairwise distinct. This proves that the determinant of M^{-1} is a unit in $\mathcal{O}/\mathfrak{p}$; therefore M is invertible over $\mathcal{O}/\mathfrak{p}$, which proves that (4.2) cannot be true. Thus (4.1) must hold, and the lemma is proved. □

4.2 The isomorphism problem and automorphism groups

Recall that the groups in $\mathcal{S}_n$ can be constructed as $C = C_{n,e}(\mathbb{S}(\boldsymbol{c}))$ with $\boldsymbol{c} \in \Delta_n$. By definition, C is an extension of T_n/T_{n+e} by S_n, and T_n/T_{n+e} is a fully invariant subgroup of C. Hence the isomorphism problem and the determination of $\mathrm{Aut}(C)$ can be approached using the general ideas for group extensions, see for example [17].

We investigate under which conditions two elements of Δ_n define isomorphic groups. For this undertaking, the group homomorphisms

$$\rho_a \colon \mathcal{U} \to \mathcal{U}, \quad u \mapsto u^{-1}\sigma_a(u)\sigma_{1-a}(u),$$

with $a \in \{2, \ldots, \ell + 1\}$ play an important role. We first recall an action on Δ_n, motivated by [10].

Lemma 4.3. *The element* $(u, \sigma_b) \in \mathcal{U} \rtimes \mathrm{Gal}(K)$ *acts on* $\boldsymbol{c} = (c_1, \ldots, c_\ell) \in \Delta_n$ *via*

$$(u, \sigma_b)(\boldsymbol{c}) = (\rho_2(u)^{-1}\sigma_b(c_1), \ldots, \rho_{\ell+1}(u)^{-1}\sigma_b(c_\ell)) \in \Delta_n.$$

This induces an action of $\mathcal{U} \rtimes \mathrm{Gal}(K)$ *on* Γ_n *and on the set of cosets* Γ_n/Γ_{n+e} *for each* $e \in \mathbb{N}$.

Proof. We explain the origin of this action. Every automorphism $\beta \in \mathrm{Aut}(S)$ acts on $f \in \mathrm{Hom}_P(T \wedge T, T_n)$ via $f \mapsto \beta[f] = \beta \circ f \circ (\beta^{-1} \wedge \beta^{-1})|_{T \wedge T}$; if f is surjective, then so is $\beta[f]$. For the following, recall the notation of Lemma 3.2. If β is in the kernel of the map $\pi \colon \mathrm{Aut}(S) \to \mathrm{Aut}(T)$, then $\beta[f] = f$ for every $f \in \mathrm{Hom}_P(T \wedge T, T_n)$. Now let $\beta = \alpha(u, b)$ with $(u, \sigma_b) \in \mathcal{U} \rtimes \mathrm{Gal}(K)$. If $a \in \{2, \ldots, \ell + 1\}$, $c \in K$, and $x \wedge y \in T \wedge T$, then a short computation shows that $\beta[c\mathbb{S}_a](x \wedge y) = \rho_a(u^{-1})\sigma_b(c)\mathbb{S}_a(x \wedge y)$. This implies that $f = \mathbb{S}(\boldsymbol{c})$ is mapped to $\beta[f] = \mathbb{S}((u, \sigma_b)(\boldsymbol{c}))$, and $(u, \sigma_b)(\boldsymbol{c}) \in \Delta_n$ as required. □

Lemma 4.3 allows us to formulate a solution to the isomorphism problem for skeleton groups and a description for their automorphism groups. For this purpose, let $C = C_{n,e}(\mathbb{S}(\boldsymbol{c}))$ be defined as above and let

$$\lambda\colon \mathrm{Aut}(S) \to \mathrm{Aut}(S_n) \times \mathrm{Aut}(T_n/T_{n+e}),$$
$$\lambda_C\colon \mathrm{Aut}(C) \to \mathrm{Aut}(S_n) \times \mathrm{Aut}(T_n/T_{n+e})$$

be induced by the natural restrictions. It is easy to show that the kernel of λ_C is isomorphic to $Z^1(S_n, T_n/T_{n+e})$; its image is described in [17] using cohomology. Here we describe the image of λ_C in a different way that will be more useful in our setting. Recall from Lemma 3.2 that $\mathrm{Aut}(S)$ is an extension of $Z^1(P,T)$ by $\mathcal{U} \rtimes \mathrm{Gal}(K)$.

Theorem 4.4. *Let $n \geq \max\{m, 8\}$ and $e \in \{0, \ldots, n-m\}$; let $\boldsymbol{c}, \boldsymbol{d} \in \Delta_n$.*

(a) *The groups $C_{n,e}(\mathbb{S}(\boldsymbol{c}))$ and $C_{n,e}(\mathbb{S}(\boldsymbol{d}))$ are isomorphic if and only if $\boldsymbol{c} + \Gamma_{n+e}$ and $\boldsymbol{d} + \Gamma_{n+e}$ lie in the same orbit under the action of $\mathcal{U} \rtimes \mathrm{Gal}(K)$ as defined in Lemma* 4.3.

(b) *The group $\mathrm{Aut}(C_{n,e}(\boldsymbol{c}))$ is an extension of the p-group $Z^1(S_n, T_n/T_{n+e})$ by $\lambda(Z^1(P,T).\Sigma)$, where Σ is the stabiliser of $\boldsymbol{c} + \Gamma_{n+e}$ in $\mathcal{U} \rtimes \mathrm{Gal}(K)$.*

Proof. This follows from results in [3, 4], based on the general cohomological approach outlined in [17]. We briefly summarise the approach since this explains the reduction to the action of $\mathcal{U} \rtimes \mathrm{Gal}(K)$.

(a) Every group of depth e in $\mathcal{B}_n$ is an extension of T_n/T_{n+e} by the root S_n of $\mathcal{B}_n$, where T_n/T_{n+e} carries the obvious S_n-module structure, see [4, Theorem 3.1]. Such extensions can be described by elements of the second cohomology group $H^2(S_n, T_n/T_{n+e})$, and the isomorphism problem of such extensions can be solved by considering the action of the group of compatible pairs $\mathrm{Comp}(S_n, T_n/T_{n+e})$, which consists of pairs of *compatible automorphisms* of S_n and T_n/T_{n+e}, respectively, see [4, Section 7.1]. By [4, Theorem 7.1], the isomorphism problem for skeleton groups can be solved by considering compatible pairs $\lambda(\alpha) = (\alpha|_{S_n}, \alpha|_{T_n/T_{n+e}})$ defined by $\alpha \in \mathrm{Aut}(S)$, acting on certain cohomology classes defined by surjective homomorphisms $T \wedge T \to T_n$. This action is discussed in detail in [3, Section 4.2], and it turns out that one has to consider exactly the automorphisms $\alpha(u,b)$ of S which are defined by elements $(u, \sigma_b) \in \mathcal{U} \rtimes \mathrm{Gal}(K)$; the automorphisms $\alpha(s)$ with $s \in T$ act trivially. Putting all this together, the statement of the theorem follows. We note that in [3, 4] groups of depth e in $\mathcal{B}_n$ are described as extensions of T/T_{e+1} by S_n; however, $T_n/T_{n+e} \cong T/T_{e+1}$ as S_n-modules, and applying a suitable S_n-module isomorphism translates the results to our set-up, cf. [3, Remark 1].

(b) The claim follows from known results about automorphism groups of extensions, together with [4, Lemma 5.4]. We use the notation introduced in part (a) and let $\gamma \in H^2(S_n, T_n/T_{n+e})$ be a cohomology class defining $C_{n,e}(\mathbb{S}(\boldsymbol{c}))$. It is shown in [17] that the image of λ_C is isomorphic to the stabiliser of γ in $\mathrm{Comp}(S_n, T_n/T_{n+e})$, and that the kernel of λ_C is isomorphic to the p-group $Z^1(S_n, T_n/T_{n+e})$. The proof of [3, Lemma 5.4] now shows that the stabiliser of γ in the group of compatible pairs is isomorphic to the stabiliser of $\boldsymbol{c} + \Gamma_{n+e}$ in $\mathrm{Aut}(S_{n+e})$, where $\alpha \in \mathrm{Aut}(S_{n+e})$ acts as the compatible pair $\lambda(\alpha)$. Note that $Z^1(P,T).\Sigma$ is the stabiliser of $\boldsymbol{c} + \Gamma_{n+e}$ in $\mathrm{Aut}(S)$; since $\mathrm{Aut}(S) \to \mathrm{Aut}(S_{n+e})$ is surjective (and its kernel acts trivially on $\boldsymbol{c} + \Gamma_{n+e}$), the claim follows. □

Leedham-Green and McKay [10] also considered the isomorphism problem using a different approach: they considered the homomorphism defined by commutation in a skeleton group, and investigated how this homomorphism changes when one modifies certain generators of the group. Their results [10, Propositions 1.1 and 1.2] are in line with ours and might be used to prove one direction of the isomorphism problem.

5 The skeleton groups in $\mathcal{S}_n^*$

The automorphism group of a skeleton group $C = C_{n,e}(\boldsymbol{c})$ with $\boldsymbol{c} \in \Delta_n$ is described in Theorem 4.4, and we have

$$\mathrm{Aut}(C) \cong Z^1(S_n, T_n/T_{n+e}).\lambda(Z^1(P,T).\Sigma),$$

where Σ is the stabiliser of $\boldsymbol{c} + \Gamma_{n+e}$ in $\mathcal{U} \rtimes \mathrm{Gal}(K)$. Note that $Z^1(S_n, T_n/T_{n+e})$ and $\lambda(Z^1(P,T))$ are both p-groups, and also the subquotient $\lambda_C(\mathcal{U}_2 \cap \Sigma)$ induces a p-group in $\mathrm{Aut}(C)$. Recall that $\mathcal{U} = \langle\omega\rangle \times \langle\theta\rangle \times \mathcal{U}_2$; by Lemma 4.3, the element $\theta \in \mathcal{U}$ acts trivially in $\mathrm{Aut}(C)$, and $\omega \in \mathcal{U}$ acts by multiplication with ω^{-1}. In particular, ω cannot stabilise any non-trivial element in Γ_n/Γ_{n+e}. In summary, if $e > 0$, then $\boldsymbol{c} + \Gamma_{n+e}$ is non-trivial and $\mathrm{Aut}(C)$ is an extension of a p-group by a subgroup of $\mathrm{Gal}(K)$. Using the notation of Theorem 4.4, we have proved the following result; recall that $\mathrm{Gal}(K)$ is cyclic of order $d = p - 1$ and generated by σ.

Lemma 5.1. *If $n \geq \max\{m, 8\}$ and $e \in \{1, \ldots, n-m\}$, then*

$$\Delta_{n,e}^* = \{\boldsymbol{c} \in \Delta_n \mid \textit{there exists } u \in \mathcal{U} \textit{ with } (u,\sigma)(\boldsymbol{c}) \equiv \boldsymbol{c} \bmod \Gamma_{n+e}\}.$$

It remains to determine which units $u \in \mathcal{U}$ arise in this setting, and also how to solve the isomorphism problem for the groups defined by elements in $\Delta_{n,e}^*$.

For this purpose, the following two sets are important; they are defined for $y \in \mathbb{Z}$; recall that $\Delta_n = \Gamma_n \setminus \Gamma_{n+1}$:

$$\Phi_{n,y} = \{\boldsymbol{c} \in \Gamma_n \mid (\omega^y, \sigma)(\boldsymbol{c}) = \boldsymbol{c}\},$$
$$\Lambda_{n,y} = \{\boldsymbol{c} \in \Delta_n \mid (\omega^y, \sigma)(\boldsymbol{c}) = \boldsymbol{c}\}.$$

It follows that $\Lambda_{n,y} = \Phi_{n,y} \setminus \Phi_{n+1,y}$ for every $y \in \mathbb{Z}$. Note that the elements of $\Lambda_{n,y}$ are "global" fixed points, while the elements of $\Delta^*_{n,e}$ are fixed points modulo Γ_{n+e}. Every global fixed point induces fixed points modulo Γ_{n+e}, hence for every $e \in \mathbb{N}$ and $y \in \mathbb{Z}$ we have

$$\Lambda_{n,y} \subseteq \Delta^*_{n,e}.$$

We can now state the main result of this section.

Theorem 5.2. *Let $\boldsymbol{c} \in \Delta^*_{n,e}$ where $n \geq \max\{m, 8\}$ and $e \in \{1, \ldots, n-m\}$.*

(a) *There exist $y \in \{(n-2i) \bmod d \mid i = 1, \ldots, \ell\}$ and $\boldsymbol{a} \in \Lambda_{n,y}$ such that $C_{n,e}(\mathbb{S}(\boldsymbol{c})) \cong C_{n,e}(\mathbb{S}(\boldsymbol{a}))$.*

(b) *If $\boldsymbol{c} \in \Lambda_{n,y_1}$ and $\boldsymbol{d} \in \Lambda_{n,y_2}$ with $y_1, y_2 \in \mathbb{Z}$, then $C_{n,e}(\mathbb{S}(\boldsymbol{c})) \cong C_{n,e}(\mathbb{S}(\boldsymbol{d}))$ if and only if $y_1 \equiv y_2 \bmod d$ and $\boldsymbol{c} = (u, 1)(\boldsymbol{d}) \bmod \Gamma_{n+e}$ for some $u \in \mathbb{Z}_p^*$.*

Our proof of Theorem 5.2 proceeds in several steps and is split up into various lemmas; these are exhibited in the following two subsections.

5.1 Proof of Theorem 5.2 (a)

Throughout this section let $n \geq \max\{m, 8\}$ and $e \in \{1, \ldots, n-m\}$.

Lemma 5.3. *If $\boldsymbol{c}, \boldsymbol{d} \in \Delta^*_{n,e}$, then*

$$C_{n,e}(\mathbb{S}(\boldsymbol{c})) \cong C_{n,e}(\mathbb{S}(\boldsymbol{d}))$$

if and only if $(u, 1)(\boldsymbol{c}) \equiv \boldsymbol{d} \bmod \Gamma_{n+e}$ for some $u \in \mathcal{U}$.

Proof. By Theorem 4.4, if $C_{n,e}(\mathbb{S}(\boldsymbol{c})) \cong C_{n,e}(\mathbb{S}(\boldsymbol{d}))$, then

$$\boldsymbol{d} \equiv (w, \sigma_b)(\boldsymbol{c}) \bmod \Gamma_{n+e}$$

for some $\sigma_b \in \mathrm{Gal}(K)$ and $w \in \mathcal{U}$. By Lemma 5.1, there exists an element $v \in \mathcal{U}$ with $(v, 1)(\boldsymbol{c}) \equiv (1, \sigma)(\boldsymbol{c}) \bmod \Gamma_{n+e}$. Write $\sigma_b = \sigma^h$ for some $h \in \{1, \ldots, d\}$, and let $u = wv^h \in \mathcal{U}$. Then

$$\boldsymbol{d} \equiv (w, \sigma^h)(\boldsymbol{c}) \equiv (w, 1)(1, \sigma^h)(\boldsymbol{c}) \equiv (w, 1)(v^h, 1)(\boldsymbol{c}) \equiv (u, 1)(\boldsymbol{c}) \bmod \Gamma_{n+e},$$

as desired. The converse follows directly from Theorem 4.4. □

Lemma 5.4. *If $\boldsymbol{c} \in \Delta^*_{n,e}$, then $C_{n,e}(\mathbb{S}(\boldsymbol{c})) \cong C_{n,e}(\mathbb{S}(\boldsymbol{d}))$ for some $\boldsymbol{d} \in \Delta^*_{n,e}$ such that $(v,\sigma)(\boldsymbol{d}) \equiv \boldsymbol{d} \bmod \Gamma_{n+e}$ for some $v \in \mathbb{Z}_p^*$.*

Proof. By Lemma 5.1, there exists $u \in \mathcal{U}$ with $(u,\sigma)(\boldsymbol{c}) \equiv \boldsymbol{c} \bmod \Gamma_{n+e}$. We use Lemma 2.2 to decompose $u = vx$ with $v \in \ker \chi = \mathbb{Z}_p^*$ and $x \in \operatorname{im} \chi$. Choose $y \in \mathcal{U}$ with $x^{-1} = \chi(y) = y\sigma(y)^{-1}$, and define $\boldsymbol{d} = (y,1)(\boldsymbol{c})$. By Theorem 4.4, we have $C_{n,e}(\boldsymbol{d}) \cong C_{n,e}(\boldsymbol{c})$, and the claim follows from

$$\begin{aligned}\boldsymbol{d} &\equiv (y,1)(\boldsymbol{c})\\ &\equiv (y,1)(u,\sigma)(\boldsymbol{c})\\ &\equiv (y,1)(u,\sigma)(y^{-1},1)(\boldsymbol{d})\\ &\equiv (x^{-1}u,\sigma)(\boldsymbol{d})\\ &\equiv (v,\sigma)(\boldsymbol{d}) \bmod \Gamma_{n+e}.\end{aligned}$$

□

In the next lemma we investigate the set $\Lambda_{n,y} = \Phi_{n,y} \cap \Delta_n$ in more detail. Recall that ω acts by multiplication by ω^{-1} on Γ_n, and therefore

$$\Phi_{n,y} = \{\boldsymbol{c} \in \Gamma_n \mid (1,\sigma)(\boldsymbol{c}) = \omega^y \boldsymbol{c}\}. \tag{5.1}$$

Lemma 5.5. *For each y, the set $\Phi_{n,y}$ is a $\mathbb{Z}_p$-sublattice of Γ_n; moreover*

$$\Gamma_n = \Phi_{n,0} \oplus \cdots \oplus \Phi_{n,d-1}.$$

Proof. The action of $\mathcal{U} \rtimes \mathrm{Gal}(K)$ on Γ_n defined in Lemma 4.3 extends to an action on the ℓ-fold direct product K^ℓ; in particular, $(1,\sigma)$ acts via

$$(x_1,\ldots,x_\ell) \mapsto (\sigma(x_1),\ldots,\sigma(x_\ell)).$$

By Lemma 2.1, $\sigma\colon K \to K$ is diagonalisable with eigenvalues $\omega^0,\ldots,\omega^{d-1}$, and each eigenspace has dimension 1. Thus, the action of $(1,\sigma)$ on K^ℓ is diagonalisable with eigenvalues $\omega^0,\ldots,\omega^{d-1}$ and each eigenspace has dimension ℓ. We denote by V_i the eigenspace with eigenvalue ω^i in K^ℓ.

It follows from (5.1) that $\Phi_{n,y} = V_y \cap \Gamma_n$, hence $\Phi_{n,0} \oplus \cdots \oplus \Phi_{n,d-1} \le \Gamma_n$ and each $\Phi_{n,y}$ is a sublattice of Γ_n. It remains to show the following inclusion: $\Gamma_n \subseteq \Phi_{n,0} \oplus \cdots \oplus \Phi_{n,d-1}$. For this purpose, consider $w \in \Gamma_n$ and write $w = w_0 + \cdots + w_{d-1}$ with $w_i \in V_i$ for $i = 1,\ldots,\ell$. Let k be the number of non-zero summands w_i in w. We prove by induction on k that each $w_i \in \Phi_{n,i}$; then the assertion of the lemma follows.

If $k = 0$ or $k = 1$, then our claim is obviously true. Now suppose that $k > 1$ and choose j with $w_j \neq 0$. It follows from Lemma 4.3 that both $(1,\sigma)(w)$ and $(\omega^{-j},1)(w) = \omega^j w$ lie in Γ_n, hence also their difference $u = (1,\sigma)(w) - \omega^j w$ lies in Γ_n. Note that $u = u_0 + \cdots + u_{d-1}$, where each $u_i = (\omega^i - \omega^j)w_i \in V_i$.

By construction, u has at most $k-1$ non-zero summands u_i and, by the induction hypothesis, we have $u_i \in \Phi_{n,i}$ for each i. Recall that $\mathbb{Z}_p^* = \langle\omega\rangle(1+p\mathbb{Z}_p)$; this implies that $\omega^i - \omega^j \not\equiv 0 \bmod p$ and hence $\omega^i - \omega^j \in \mathbb{Z}_p^*$ for all $i \neq j$. Since $u_i = (\omega^i - \omega^j)w_i \in \Phi_{n,i}$, it follows that $w_i \in \Phi_{n,i}$ for all $i \neq j$. In particular, we have $w - w_j = w_0 + \cdots + w_{j-1} + w_{j+1} + \cdots + w_{d-1} \in \Gamma_n$, and so $w_j = w - (w - w_j) \in \Gamma_n$ as well. Now clearly $w_j \in \Phi_{n,j}$, which completes the proof. □

The next lemma considers $\boldsymbol{d} \in \Delta_{n,e}^*$ and $v \in \mathbb{Z}_p^*$ with $(v,\sigma)(\boldsymbol{d}) \equiv \boldsymbol{d} \bmod \Gamma_{n,e}$, as in Lemma 5.4. Recall that every $v \in \mathbb{Z}_p^*$ can be written as

$$v = \omega^u(1+px) = \omega^{-y}(1+px)$$

for some $u, y \in \{0,\ldots,d-1\}$ and $x \in \mathbb{Z}_p$.

Lemma 5.6. *Let $\boldsymbol{d} \in \Delta_{n,e}^*$ and $v \in \mathbb{Z}_p^*$ with $(v,\sigma)(\boldsymbol{d}) \equiv \boldsymbol{d} \bmod \Gamma_{n,e}$, and write $v = \omega^{-y}(1+px)$ for some $y \in \{0,\ldots,d-1\}$ and $x \in \mathbb{Z}_p$. There exists $\boldsymbol{a} \in \Lambda_{n,y}$ with $C_{n,e}(\mathbb{S}(\boldsymbol{d})) = C_{n,e}(\mathbb{S}(\boldsymbol{a}))$.*

Proof. By definition, $\boldsymbol{d} \in \Delta_n = \Gamma_n \setminus \Gamma_{n+1}$; by Lemma 5.5, we can decompose $\boldsymbol{d} = \boldsymbol{d}_0 + \cdots + \boldsymbol{d}_{d-1}$ with each $\boldsymbol{d}_i \in \Phi_{n,i}$. As $(v,\sigma)(\boldsymbol{d}) \equiv \boldsymbol{d} \bmod \Gamma_{n+e}$ and $v \in \mathbb{Z}_p^*$, it follows that

$$(v,\sigma)(\boldsymbol{d}) - \boldsymbol{d} = (v^{-1}\omega^0 - 1)\boldsymbol{d}_0 + \cdots + (v^{-1}\omega^{d-1} - 1)\boldsymbol{d}_{d-1} \in \Gamma_{n+e}.$$

As $v^{-1}\omega^i - 1 \in \mathbb{Z}_p$, Lemma 5.5 yields that $(v^{-1}\omega^i - 1)\boldsymbol{d}_i \in \Gamma_{n+e}$ for each i. Using $v = \omega^{-y}(1+px)$, it follows that $v^{-1}\omega^i - 1 \equiv \omega^{i-y} - 1 \bmod p$; in particular, $v^{-1}\omega^i - 1 \in \mathbb{Z}_p^*$ and $\boldsymbol{d}_i \in \Gamma_{n+e}$ for all $i \neq y$. We can now choose $\boldsymbol{a} = \boldsymbol{d}_y \in \Phi_{n,y}$; we have shown that $\boldsymbol{d} \equiv \boldsymbol{a} \bmod \Gamma_{n+e}$, thus

$$C_{n,e}(\mathbb{S}(\boldsymbol{d})) = C_{n,e}(\mathbb{S}(\boldsymbol{a})).$$

As $\boldsymbol{d} \in \Delta_n$, it follows that $\boldsymbol{a} \in \Delta_n$. Hence $\boldsymbol{a} \in \Lambda_{n,y}$ as claimed. □

Lemma 5.7. *We have $\Lambda_{n,y} \neq \emptyset$ if and only if $(1,\sigma)$ has an eigenvector in Δ_1 with eigenvalue ω^{y-n+1}.*

Proof. Let $\boldsymbol{r} \in \Delta_1$ be an eigenvector of $(1,\sigma)$ with eigenvalue ω^{y-n+1}. By Lemma 2.1, there exists an eigenvector $x \in \mathfrak{p}^{n-1} \setminus \mathfrak{p}^n$ of σ with eigenvalue ω^{n-1}. Then $x\boldsymbol{r} \in \Delta_n$ and

$$\begin{aligned}(\omega^y,\sigma)(x\boldsymbol{r}) &= \omega^{-y}\sigma(x)(1,\sigma)(\boldsymbol{r})\\ &= \omega^{-y}\omega^{n-1}x\omega^{y-n+1}\boldsymbol{r}\\ &= x\boldsymbol{r},\end{aligned}$$

so $x\boldsymbol{r} \in \Lambda_{n,y}$. Conversely, let $\boldsymbol{c} \in \Lambda_{n,y}$. Then $\boldsymbol{c}$ is an eigenvector of $(1,\sigma)$ with eigenvalue ω^y. If $x \in \mathfrak{p}^{-n+1} \setminus \mathfrak{p}^{-n+2}$ is an eigenvector of σ with eigenvalue ω^{-n+1}, then $x\boldsymbol{c} \in \Delta_1$ and

$$\begin{aligned}(1,\sigma)(x\boldsymbol{c}) &= \omega^{-n+1}x(1,\sigma)(\boldsymbol{c})\\ &= \omega^{-n+1}x\omega^y\boldsymbol{c}\\ &= \omega^{y-n+1}x\boldsymbol{c}.\end{aligned}$$

□

The next lemma is the last result we need for our proof of Theorem 5.2 (a).

Lemma 5.8. *The eigenvalues of* $(1,\sigma)$ *on* Δ_1 *are* $\{\omega^{-2i+1} \mid i = 1,\dots,\ell\}$.

Proof. The main tool in the following proof is Lemma 4.2: with Lemma 2.1 it implies that the eigenvalue of an eigenvector $\boldsymbol{f} \in \Delta_1$ of $(1,\sigma)$ is $\omega^{\mathrm{val}(\boldsymbol{t})}$, where $\mathrm{val}(\boldsymbol{t})$ is the valuation defined in Section 2. The eigenvalues on $\Delta_1 = \Gamma_1 \setminus \Gamma_2$ coincide with the eigenvalues of $(1,\sigma)$ on the elementary abelian quotient Γ_1/Γ_2 of rank ℓ; in particular, this number of different eigenvalues is at most ℓ. We show that it is exactly ℓ. To prove this, we use the notation of Lemma 4.2 and define an isomorphism

$$\psi\colon C_p^\ell \cong \Gamma_1/\Gamma_2, \quad (a_1,\dots,a_\ell) \mapsto a_1\boldsymbol{t_1} + \cdots + a_\ell\boldsymbol{t_\ell} + \Gamma_2,$$

recall that each $\boldsymbol{t_j}$ has valuation $\mathrm{val}(\boldsymbol{t_j}) = -2j+1$. In the following we let $(1,\sigma)$ act on C_p^ℓ via ψ; in particular, the action of $(1,\sigma)$ on C_p^ℓ is diagonalisable. Our claim is that for each $i \in \{1,\dots,\ell\}$ there is, up to scalar multiples, a unique eigenvector $(a_1,\dots,a_i,0,\dots,0) \in C_p^\ell$ of $(1,\sigma)$ with $a_i \neq 0$, and that this eigenvector has eigenvalue ω^{-2i+1}. We use induction to prove this claim. We note that the assertion of the lemma follows from this claim.

Base case. For the base case consider $i = \ell$. Since the action of $(1,\sigma)$ on C_p^ℓ is diagonalisable, there must be an eigenvector $a = (a_1,\dots,a_\ell) \in C_p^\ell$ with $a_\ell \neq 0$. This eigenvector comes from an eigenvector $\boldsymbol{f} = a_1\boldsymbol{t_1} + \cdots + a_\ell\boldsymbol{t_\ell} + \boldsymbol{g} \in \Delta_1$ for some $\boldsymbol{g} \in \Delta_2$. Recall that $\Delta_2 = \kappa\Delta_1 \subseteq (\mathfrak{p}^{-2\ell+2})^\ell$. Now

$$\mathrm{val}(a_\ell\boldsymbol{t_\ell}) = \mathrm{val}(a_\ell) + \mathrm{val}(\boldsymbol{t_\ell}) = \mathrm{val}(\boldsymbol{t_\ell}) = -2\ell+1$$

and $\mathrm{val}(\boldsymbol{g}) \geq -2\ell+2$ imply that $\mathrm{val}(\boldsymbol{f}) = -2\ell+1$, see Lemma 4.2, whence the eigenvalue of $\boldsymbol{f}$ (and a) is $\omega^{-2\ell+1}$. For the uniqueness, consider an eigenvector $a' = (a'_1,\dots,a'_\ell) \in C_p^\ell$ with $a'_\ell \neq 0$; as just shown, the eigenvalue is $\omega^{-2\ell+1}$. Without loss of generality, we can assume that $a_\ell = a'_\ell$. Suppose, for a contradiction, that a and a' are linearly independent, so that

$$b = a - a' = (b_1,\dots,b_{\ell-1},0) \in C_p^\ell$$

is an eigenvector of $(1,\sigma)$ with eigenvalue $\omega^{-2\ell+1}$. This eigenvector comes from an eigenvector $\boldsymbol{u} = b_1\boldsymbol{t_1} + \cdots + b_{\ell-1}\boldsymbol{t_{\ell-1}} + \boldsymbol{h} \in \Delta_1$ for some $\boldsymbol{h} \in \Delta_2$. But now $\mathrm{val}(\boldsymbol{u}) \geq -2\ell + 2$, so the eigenvalue of b cannot be $\omega^{-2\ell+1}$, a contradiction. (Indeed, if $\omega^{\mathrm{val}(\boldsymbol{u})} = \omega^{-2\ell+1}$, then $\mathrm{val}(\boldsymbol{u}) \geq -2\ell+2$ forces $\mathrm{val}(\boldsymbol{u}) \geq -2\ell+p > 0$, so $\boldsymbol{u} \in \Delta_2$ and $(b_1, \ldots, b_{\ell-1}, 0) = (0, \ldots, 0)$, which is not possible.) This proves that there is, up to scalar multiples, a unique eigenvector of $(1,\sigma)$ in C_p^ℓ of the form $(a_1, \ldots, a_\ell)$ with $a_\ell \neq 0$, and that the corresponding eigenvalue is $\omega^{-2\ell+1}$.

Induction hypothesis. Our induction hypothesis now is that for each index $j \in \{i+1, \ldots, \ell\}$ there is, up to scalar multiples, a unique eigenvector of $(1,\sigma)$ in C_p^ℓ of the form

$$v_j = (b_{j,1}, \ldots, b_{j,j}, 0, \ldots, 0) \in C_p^\ell$$

with $b_{j,j} \neq 0$, and that the corresponding eigenvalue is ω^{-2j+1}. Note that v_j comes from an eigenvector

$$\boldsymbol{w_j} = b_{j,1}\boldsymbol{t_1} + \cdots + b_{j,j}\boldsymbol{t_j} + \boldsymbol{h_j} \in \Delta_1$$

for some $\boldsymbol{h_j} \in \Delta_2$, with

$$\mathrm{val}(\boldsymbol{h_j}) \geq \mathrm{val}(b_{j,1}\boldsymbol{t_1} + \cdots + b_{j,j}\boldsymbol{t_j}) = \mathrm{val}(b_{j,j}\boldsymbol{t_j}) = -2j + 1.$$

Existence of eigenvector. It follows from the induction hypothesis that there is an eigenvector

$$a = (a_1, \ldots, a_i, 0, \ldots, 0) \in C_p^\ell$$

of $(1,\sigma)$ with $a_i \neq 0$: if not, then there would be a basis of C_p^ℓ consisting of $\{v_{i+1}, \ldots, v_\ell\}$ and i additional eigenvectors each having 0 as k-th entry for all $k = i, \ldots, \ell$; this is not possible as such a set of i vectors cannot be linearly independent. Thus, an eigenvector a as above exists.

Eigenvalue. Our first claim is that the corresponding eigenvalue is ω^{-2i+1}. Note that a comes from an eigenvector

$$\boldsymbol{f} = a_1\boldsymbol{t_1} + \cdots + a_i\boldsymbol{t_i} + \boldsymbol{g} \in \Delta_1$$

for some $\boldsymbol{g} \in \Delta_2$; in the following, write $r = \mathrm{val}(\boldsymbol{g})$. If

$$\begin{aligned} r &\geq \mathrm{val}(a_1\boldsymbol{t_1} + \cdots + a_i\boldsymbol{t_i}) \\ &= \mathrm{val}(a_i\boldsymbol{t_i}) = \mathrm{val}(a_i) + \mathrm{val}(a_i\boldsymbol{t_i}) = \mathrm{val}(a_i\boldsymbol{t_i}) = -2i + 1, \end{aligned}$$

then $\mathrm{val}(\boldsymbol{f}) = -2i+1$ by Lemma 4.2, and it follows that the eigenvalue is ω^{-2i+1}. It remains to consider the case $r < -2i + 1$, so that the eigenvalue of a is ω^r.

We show that this is not possible; we achieve this by modifying $\boldsymbol{g}$ by our known eigenvectors $\boldsymbol{w_{i+1}}, \ldots, \boldsymbol{w_\ell}$ until we obtain a contradiction. For this purpose, write

$$\boldsymbol{g} = u_1\boldsymbol{t_1} + \cdots + u_\ell\boldsymbol{t_\ell} \in \Delta_2$$

and let $s \in \{1, \ldots, \ell\}$ be minimal with $\mathrm{val}(u_s\boldsymbol{t_s}) = \mathrm{val}(\boldsymbol{g}) = r$; such an s exists by Lemma 4.2. Note that $r = \mathrm{val}(u_s\boldsymbol{t_s}) > -2s+1$ since $u_s \in \mathfrak{p}$, hence $r+2s-1 > 0$. Since $r < -2i+1$ by assumption, this implies $s \in \{i+1, \ldots, \ell\}$. By the induction hypothesis, we know the existence of the eigenvector

$$\boldsymbol{w_s} = b_{s,1}\boldsymbol{t_1} + \cdots + b_{s,s}\boldsymbol{t_s} + \boldsymbol{h_s} \in \Delta_1$$

of $(1, \sigma)$ with eigenvalue ω^{-2s+1}. Let $k \in \mathfrak{p}^{r+2s-1} \setminus \mathfrak{p}^{r+2s}$ be an eigenvector of σ with eigenvalue ω^{r+2s-1}. Now $\boldsymbol{f'} = \boldsymbol{f} - k\boldsymbol{w_s}$ is an eigenvector of $(1, \sigma)$ with eigenvalue ω^r, and that both $\boldsymbol{f}$ and $\boldsymbol{f'}$ correspond to

$$a = (a_1, \ldots, a_i, 0, \ldots, 0) \in C_p^\ell$$

since $k \in \mathfrak{p}$. In particular,

$$\begin{aligned}\boldsymbol{f'} &= a_1\boldsymbol{t_1} + \cdots + a_i\boldsymbol{t_i} + (\boldsymbol{g} - k\boldsymbol{w_s}) \\ &= a_1\boldsymbol{t_1} + \cdots + a_i\boldsymbol{t_i} \\ &\quad + \underbrace{((u_1 - kb_{s,1})\boldsymbol{t_1} + \cdots + (u_s - kb_{s,s})\boldsymbol{t_s} + u_{s+1}\boldsymbol{t_{s+1}} + \cdots + u_\ell\boldsymbol{t_\ell}) - k\boldsymbol{h_s}}_{=:\,\boldsymbol{g'}}.\end{aligned}$$

Since both $u_s, kb_{s,s} \in \mathfrak{p}^{r-2s+1} \setminus \mathfrak{p}^{r-2s+2}$, we can replace k by a suitable scalar multiple of k such that $u_s - kb_{s,s} \in \mathfrak{p}^{r-2s+2}$, and so $\mathrm{val}((u_s - kb_{s,s})\boldsymbol{t_s}) > r$; note that $\mathrm{val}((u_j - kb_{s,j})\boldsymbol{t_j}) \geq \mathrm{val}(u_j\boldsymbol{t_j})$ for all j. In conclusion, we have found $\boldsymbol{f'} = a_1\boldsymbol{t_1} + \cdots + a_i\boldsymbol{t_i} + \boldsymbol{g'}$ with $\boldsymbol{g'} \in \Delta_2$ such that if $\boldsymbol{g'} = u'_1\boldsymbol{t_1} + \cdots + u'_\ell\boldsymbol{t_\ell}$ and $s' \in \{1, \ldots, \ell\}$ is minimal with $\mathrm{val}(u_{s'}\boldsymbol{t_{s'}}) = \mathrm{val}(\boldsymbol{g'}) = \mathrm{val}(\boldsymbol{g}) = r$, then $s' > s$. (Note that $\boldsymbol{f'}$ has eigenvalue ω^r and $r < -2i+1$, so we must indeed have $\mathrm{val}(\boldsymbol{g'}) = r = \mathrm{val}(\boldsymbol{g})$.) Now we iterate this argument until we find an eigenvector

$$\hat{\boldsymbol{f}} = a_1\boldsymbol{t_1} + \cdots + a_i\boldsymbol{t_i} + \hat{\boldsymbol{g}}$$

of $(1, \sigma)$ with eigenvalue ω^r and $\hat{\boldsymbol{g}} \in \Delta_2$ such that if $\hat{\boldsymbol{g}} = \hat{u_1}\boldsymbol{t_1} + \cdots + \hat{u_\ell}\boldsymbol{t_\ell}$, then $\mathrm{val}(\hat{u_j}\boldsymbol{t_j}) > r$ for all j. But then Lemma 4.2 implies that $\mathrm{val}(\hat{\boldsymbol{g}}) > r$, a contradiction to $\omega^{\mathrm{val}(f)} = \omega^r$ and $\mathrm{val}(\hat{\boldsymbol{g}}) = r$. In summary, this proves $r \geq -2i+1$, hence the eigenvalue of an eigenvector $a = (a_1, \ldots, a_i, 0, \ldots, 0)$ with $a_i \neq 0$ must be ω^{-2i+1}.

Uniqueness. Consider a second eigenvector $a' = (a'_1, \ldots, a'_i, 0, \ldots, 0) \in C_p^\ell$ of $(1, \sigma)$ with $a'_i \neq 0$; as proved in the previous paragraph, the eigenvalue of a'

is ω^{-2i+1}. We claim that a' and a are linearly dependent. Note that a comes from an eigenvector $\boldsymbol{f} = a_1\boldsymbol{t_1} + \cdots + a_i\boldsymbol{t_i} + \boldsymbol{g} \in \Delta_1$ for some $\boldsymbol{g} \in \Delta_2$ with $\mathrm{val}(\boldsymbol{g}) \geq -2i+1$. Similarly, a' comes from an eigenvector $\boldsymbol{f'} = a'_1\boldsymbol{t_1} + \cdots + a'_i\boldsymbol{t_i} + \boldsymbol{g'} \in \Delta_1$ for some $\boldsymbol{g'} \in \Delta_2$ with $\mathrm{val}(\boldsymbol{g'}) \geq -2i+1$. Suppose, for a contradiction, that a and a' are linearly independent. Replacing a' by a suitable scalar multiple, we can assume that $a_i = a'_i$, so that $b = a - a' = (b_1, \ldots, b_j, 0, \ldots, 0)$, with $b_j \neq 0$ and $j < i$, is also an eigenvector of $(1, \sigma)$ with eigenvalue ω^{-2i+1}. This eigenvector comes from $\hat{\boldsymbol{f}} = \boldsymbol{f} - \boldsymbol{f'} = b_1\boldsymbol{t_1} + \cdots + b_j\boldsymbol{t_j} + \hat{\boldsymbol{g}}$, where $\hat{\boldsymbol{g}} = \boldsymbol{g} - \boldsymbol{g'} \in \Delta_2$ satisfies $\mathrm{val}(\hat{\boldsymbol{g}}) \geq -2i+1$; in fact, we must have $\mathrm{val}(\hat{\boldsymbol{g}}) = -2i+1$ since otherwise the eigenvalue of b cannot be ω^{-2i+1}. Note that for all $u = i+1, \ldots, \ell$ we already found eigenvectors $\boldsymbol{w_u}$ with eigenvalue ω^{-2u+1}, thus we can use the same construction as in the previous paragraph to obtain from $\hat{\boldsymbol{f}}$ and $\boldsymbol{w_{i+1}}, \ldots, \boldsymbol{w_\ell}$ an eigenvector $\tilde{\boldsymbol{f}} = b_1\boldsymbol{t_1} + \cdots + b_j\boldsymbol{t_j} + \tilde{\boldsymbol{g}}$ with eigenvalue ω^{-2i+1}, where $\tilde{\boldsymbol{g}} \in \Delta_2$ satisfies $\mathrm{val}(\tilde{\boldsymbol{g}}) > -2i+1$: this is not possible since $\tilde{\boldsymbol{f}}$ has eigenvalue ω^{-2i+1}, that is, $-2i+1 = \mathrm{val}(\tilde{\boldsymbol{f}}) = \min\{-2j+1, \mathrm{val}(\tilde{\boldsymbol{g}})\}$, but we have deduced that $\min\{-2j+1, \mathrm{val}(\tilde{\boldsymbol{g}})\} > -2i+1$. This contradiction proves that a and a' must be linearly dependent. In conclusion, we have proved that, up to scalar multiples, there is a unique eigenvector of $(1, \sigma)$ of the form $(a_1, \ldots, a_i, 0, \ldots, 0)$ with $a_i \neq 0$, and that the corresponding eigenvalue is ω^{-2i+1}. This completes the induction step. □

Lemmas 5.7 and 5.8 yield the following corollary.

Corollary 5.9. *We have $\Lambda_{n,y} \neq \emptyset$ if and only if $y \equiv n - 2i \bmod d$ for some $i = 1, \ldots, \ell$.*

We can now prove Theorem 5.2 (a).

Proof of Theorem 5.2 (a). Let $\boldsymbol{c} \in \Delta^*_{n,e}$. By Lemmas 5.4 and 5.6, there exist $y \in \{0, \ldots, d-1\}$ and $\boldsymbol{a} \in \Lambda_{n,y}$ such that

$$C_{n,e}(\mathbb{S}(\boldsymbol{c})) \cong C_{n,e}(\mathbb{S}(\boldsymbol{a})).$$

Since $\Lambda_{n,y} \neq \emptyset$, it follows from Corollary 5.9 that $y \equiv n - 2i \bmod d$ for some $i \in \{1, \ldots, \ell\}$, as claimed. □

5.2 Proof of Theorem 5.2 (b)

Again, we assume that $n \geq \max\{m, 8\}$ and $e \in \{1, \ldots, n-m\}$. Recall the map $\chi\colon \mathcal{U} \to \mathcal{U}, u \mapsto u\sigma(u)^{-1}$, which is discussed in Lemma 2.2.

Lemma 5.10. *Let* $\boldsymbol{c} \in \Lambda_{n,y_1}$ *and* $\boldsymbol{d} \in \Lambda_{n,y_2}$ *with* $y_1, y_2 \in \mathbb{Z}$. *If* $C_{n,e}(\mathbb{S}(\boldsymbol{c})) \cong C_{n,e}(\mathbb{S}(\boldsymbol{d}))$, *then* $y_1 = y_2$; *if* $u \in \mathcal{U}$ *with* $\boldsymbol{d} \equiv (u,1)(\boldsymbol{c}) \bmod \Gamma_{n+e}$ *as in Lemma* 5.3, *then* $\boldsymbol{c}$ *and* $\boldsymbol{d}$ *are fixed points of* $(\chi(u),1)$ *modulo* Γ_{n+e}.

Proof. It is shown in Lemma 5.3 that $\boldsymbol{d} \equiv (u,1)(\boldsymbol{c}) \bmod \Gamma_{n+e}$ for some $u \in \mathcal{U}$. This implies that

$$\begin{aligned}
\boldsymbol{d} &\equiv (\omega^{y_2},\sigma)(\boldsymbol{d}) \\
&\equiv (\omega^{y_2},\sigma)(u,1)(\boldsymbol{c}) \\
&\equiv (\omega^{y_2},\sigma)(u,1)(\omega^{y_1},\sigma)^{-1}(\boldsymbol{c}) \\
&\equiv (\omega^{y_2},\sigma)(u,1)(\omega^{y_1},\sigma)^{-1}(u,1)^{-1}(\boldsymbol{d}) \\
&\equiv (\omega^{y_2-y_1}\sigma(u)u^{-1},1)(\boldsymbol{d}) \\
&\equiv (\omega^{y_2-y_1}\chi(u)^{-1},1)(\boldsymbol{d}) \bmod \Gamma_{n+e}.
\end{aligned}$$

By Theorem 4.4, the element $(\omega^{y_2-y_1}\chi(u)^{-1},1)$ yields an element of the group $\mathrm{Aut}(C_{n,e}(\boldsymbol{d}))$, and the discussion of the automorphism groups of skeleton groups (in the beginning of Section 5) forces that $y_2 \equiv y_1 \bmod d$. Since we have $y_1, y_2 \in \{0,\dots,d-1\}$, this yields $y_1 = y_2$. In turn, this implies that $\boldsymbol{d}$ (and, by duality also $\boldsymbol{c}$) are fixed points of $(\chi(u)^{-1},1)$ modulo Γ_{n+e}. □

Lemma 5.11. *Let* $\boldsymbol{c},\boldsymbol{d} \in \Lambda_{n,y}$ *with* $y \in \mathbb{Z}$. *If* $C_{n,e}(\mathbb{S}(\boldsymbol{c})) \cong C_{n,e}(\mathbb{S}(\boldsymbol{d}))$, *then* $\boldsymbol{c} \equiv (s,1)(\boldsymbol{d}) \bmod \Gamma_{n+e}$ *for some* $s \in \mathbb{Z}_p^*$.

Proof. Recall that $\boldsymbol{c},\boldsymbol{d} \in \Lambda_{n,y} \subseteq \Delta_{n,e}^*$. Thus, by Lemma 5.3, there exists $u \in \mathcal{U}$ with $(u,1)(\boldsymbol{c}) \equiv \boldsymbol{d} \bmod \Gamma_{n+e}$. By Lemma 5.10, both $\boldsymbol{c}$ and $\boldsymbol{d}$ are fixed points under $(\chi(u),1)$. It follows from Lemma 2.2 that the restriction $\chi|_{\mathrm{im}\,\chi}$ induces an automorphism of $\mathrm{im}\,\chi$; write $u = sw$ with $s \in \ker\chi = \mathbb{Z}_p^*$ and $w \in \mathrm{im}\,\chi$. We want to show that $(w,1)(\boldsymbol{d}) \equiv \boldsymbol{d} \bmod \Gamma_{n+e}$ since this implies that

$$\boldsymbol{c} \equiv (u,1)(\boldsymbol{d}) \equiv (s,1)(w,1)(\boldsymbol{d}) \equiv (s,1)(\boldsymbol{d}) \bmod \Gamma_{n+e},$$

which proves the lemma.

We start with a more general observation: Let $v \in \mathcal{U}$ and suppose $(v,1)$ maps the fixed point $\boldsymbol{d}$ of (ω^y,σ) to another fixed point $(v,1)(\boldsymbol{d})$ of (ω^y,σ) modulo Γ_{n+e}. Then it follows from

$$(v,1)(\boldsymbol{d}) \equiv (\omega^y,\sigma)(v,1)(\boldsymbol{d}) \equiv (\sigma(v),1)(\omega^y,\sigma)(\boldsymbol{d}) \equiv (\sigma(v),1)(\boldsymbol{d}) \bmod \Gamma_{n+e}$$

that such a $(v,1)$ has an image $(\chi(v),1)$ which acts trivially on $\boldsymbol{d}$ modulo $\Gamma_{n,e}$, and by duality also on $\boldsymbol{c}$ modulo $\Gamma_{n,e}$.

Since $(u, 1)$ maps the fixed point $\boldsymbol{d}$ to the fixed point $\boldsymbol{c}$, it follows that $(\chi(u), 1)$ stabilises $\boldsymbol{d}$ modulo Γ_{n+e}. Note that $\chi(u) = \chi(w)$, hence also $(\chi(w), 1)$ stabilises $\boldsymbol{d}$ modulo Γ_{n+e}. Now we iterate this argument: since $(\chi(w), 1)$ maps the fixed point $\boldsymbol{d}$ of $(\omega^y, 1)$ to the fixed point $\boldsymbol{d}$ of $(\omega^y, 1)$, modulo Γ_{n+e}, it follows from the general observation that $(\chi^2(w), 1)$ stabilises $\boldsymbol{d}$ modulo Γ_{n+e}. By induction, $(\chi^i(w), 1)$ stabilises $\boldsymbol{d}$ modulo Γ_{n+e} for every $i \geq 1$.

There is $j \geq 2$ such that $\mathcal{U}_j = 1 + \mathfrak{p}^j$ acts trivially on Γ_n/Γ_{n+e}: for example, choose j large enough such that $\mathfrak{p}^j \leq p^x\mathcal{O}$ for some x with $p^x\Gamma_n \leq \Gamma_{n+e}$. It follows from the definition that χ stabilises $\mathcal{U}_j$. Since $\mathcal{U}_j \leq \mathcal{U}_2$, the proof of Lemma 2.2 shows that $\mathcal{U}_j = \ker(\chi|_{\mathcal{U}_j}) \times \operatorname{im}(\chi|_{\mathcal{U}_j})$; this implies that χ induces an automorphism of $J = (\operatorname{im}\chi)/(\operatorname{im}\chi|_{\mathcal{U}_j})$, which we denote by ψ. Since J is a finite group, it follows that ψ has finite order, say t.

Recall that w as above lies in $\operatorname{im}\chi$. If w lies in $\mathcal{U}_j$, then $(w, 1)$ acts trivially on $\boldsymbol{d}$ modulo Γ_{n+e}, and there is nothing to show. If $w \notin \mathcal{U}_j$, then its coset $c = w\operatorname{im}(\chi|_{\mathcal{U}_j})$ in J is non-trivial, and $\psi^t(c) = c$ follows. But this means that $\chi^t(w) = wr$ for some $r \in \mathcal{U}_j$. As shown above, $\chi^t(w) = wr$ stabilises $\boldsymbol{d}$ modulo Γ_{n+e}. Since $r \in \mathcal{U}_j$ acts trivially on Γ_n/Γ_{n+e}, it follows that w stabilises $\boldsymbol{d}$ modulo Γ_{n+e}. □

We can now prove Theorem 5.2 (b).

Proof of Theorem 5.2(b). Let $\boldsymbol{c} \in \Lambda_{n,y_1}$ and $\boldsymbol{d} \in \Lambda_{n,y_2}$. If there exists an element $u \in \mathbb{Z}_p^*$ with $\boldsymbol{c} \equiv (u, 1)(\boldsymbol{d}) \bmod \Gamma_{n+e}$, then we have $C_{n,e}(\mathbb{S}(\boldsymbol{c})) \cong C_{n,e}(\mathbb{S}(\boldsymbol{d}))$ by Lemma 5.3. For the converse, suppose that $C_{n,e}(\mathbb{S}(\boldsymbol{c})) \cong C_{n,e}(\mathbb{S}(\boldsymbol{d}))$. Then $y_1 \equiv y_2 \bmod d$ follows from Lemma 5.10, and $\boldsymbol{c} = (u, 1)(\boldsymbol{d}) \bmod \Gamma_{n+e}$ for some $u \in \mathbb{Z}_p^*$ follows from Lemma 5.11. □

6 The ramification levels in the skeleton $\mathcal{S}_n^*$

We apply Theorem 5.2 to prove the explicit description of the skeleton $\mathcal{S}_n^*$ as suggested in Theorem 1.1. First we consider the groups of depth 1.

Theorem 6.1. *Let $n \geq \max\{8, m\}$. There are ℓ groups $G_{n,1}, \ldots, G_{n,\ell}$ at depth 1 in $\mathcal{S}_n^*$; these are obtained as $G_{n,i} = C_{n,1}(\mathbb{S}(\boldsymbol{c}_i))$, where $\boldsymbol{c}_i$ is a fixed point of (ω^{j_i}, σ) with $j_i = n - 2i \bmod d$.*

Proof. It follows from Theorem 5.2 (a) that the groups at depth 1 in $\mathcal{S}_n^*$ can be constructed as $C_{n,1}(\boldsymbol{c})$ with $\boldsymbol{c} \in \Lambda_{n,y}$ for $y = 0, \ldots, d-1$. It is shown in Corollary 5.9 that $\Lambda_{n,y} \neq \emptyset$ if and only if $y = y_i = n - 2i \bmod d$ for some index $i \in \{1, \ldots, \ell\}$; this allows us to construct ℓ groups $G_{n,i} = C_{n,1}(\boldsymbol{c_i})$, where $\boldsymbol{c_i} \in \Lambda_{n,y_i}$ for $i = 1, \ldots, \ell$. Theorem 5.2 (b) shows that $G_{n,i} \cong G_{n,j}$ if and only if

$i = j$. It follows from Lemmas 5.7 and 5.8 that the eigenspace of each (ω^{y_i}, σ) in Γ_n/Γ_{n+1} has dimension 1. Thus the elements in $\Lambda_{n,y_i} \neq \emptyset$ admit exactly one isomorphism type of skeleton group for each $i = 1, \ldots, \ell$. This completes the proof. □

Now we consider the remaining part of the skeleton.

Theorem 6.2. *Let $i \in \{1, \ldots, \ell\}$ and let H be a descendant of $G_{n,i}$ at depth $e \in \{1, \ldots, n-m-1\}$ in $\mathcal{S}_n^*$, where $G_{n,i}$ is as in Theorem* 6.1. *The group H has p immediate descendants in $\mathcal{S}_n^*$ if and only if $e \bmod d \in \{2, 4, \ldots, d-2\} \setminus \{d-2i\}$; otherwise, H has one immediate descendant in $\mathcal{S}_n^*$.*

Proof. We investigate the descendants of $G_{n,i}$ for a fixed $i \in \{1, \ldots, \ell\}$. By Theorems 5.2 and 6.1, our aim is to determine the orbits and stabilisers of $\mathbb{Z}_p^*$ acting on

$$\Pi_{n,j,e} = \{\boldsymbol{c} + \Gamma_{n+e} \mid \boldsymbol{c} \in \Lambda_{n,j}\},$$

where $j = n - 2i \bmod d$. In the following, let $\mathcal{C} = \{0, 2, \ldots, d-2\} \setminus \{d-2i\}$.

We first consider stabilisers; recall that $\mathbb{Z}_p^* = \langle\omega\rangle(1 + p\mathbb{Z}_p)$, and note that $u \in \mathbb{Z}_p^*$ acts on $\boldsymbol{d} \in \Lambda_{n,j}$ via

$$(u, 1)(\boldsymbol{d}) = u^{-1}\boldsymbol{d} \bmod \Gamma_{n+e}.$$

Thus $(u, 1)(\boldsymbol{d}) \equiv \boldsymbol{d} \bmod \Gamma_{n+e}$ if and only if $u \in 1 + p^{\overline{e}}$ with $\overline{e} = \lceil e/d \rceil$; this implies that $\mathrm{Stab}_{\mathbb{Z}_p^*}(\boldsymbol{d} + \Gamma_{n+e}) = 1 + p^{\lceil e/d \rceil}\mathbb{Z}_p$. Note that the stabiliser depends on e, but not on $\boldsymbol{d}$. In particular, it follows that each $\mathbb{Z}_p^*$-orbit has the same size, namely $dp^{\overline{e}-1}$.

Next we show that

$$|\Pi_{n,j,e}| = \begin{cases} |\Pi_{n,j,e+1}| & \text{if } e \bmod d \notin \mathcal{C}, \\ p|\Pi_{n,j,e+1}| & \text{otherwise.} \end{cases}$$

To prove this, note that $|\Pi_{n,j,e}| < |\Pi_{n,j,e+1}|$ if and only if there exist $\boldsymbol{d}, \boldsymbol{e} \in \Lambda_{n,j}$ with $\boldsymbol{d} \equiv \boldsymbol{e} \bmod \Gamma_{n+e}$ and $\boldsymbol{d} \not\equiv \boldsymbol{e} \bmod \Gamma_{n+e+1}$. This holds if and only if there exists a fixed point $\boldsymbol{r} \in \Gamma_{n+e} \setminus \Gamma_{n+e+1}$ of (ω^j, σ) with $\boldsymbol{d} = \boldsymbol{c} + \boldsymbol{r}$. By Corollary 5.9, such a fixed point exists if and only if $j \equiv n + e - 2i' \bmod d$ for some $i' \in \{1, \ldots, \ell\}$. Since $j \equiv n - 2i \bmod d$, such an i' exists if and only if $e \equiv 2(i' - i) \bmod d$. A straightforward computation shows that

$$\mathcal{C} = \{2(i' - i) \bmod d \mid i' = 1, \ldots, \ell\}.$$

Thus, in summary, $|\Pi_{n,j,e}| > |\Pi_{n,j,e+1}|$ if and only if $e \bmod d \in \mathcal{C}$; in this case, $|\Pi_{n,j,e}| = p|\Pi_{n,j,e+1}|$ follows since the eigenspace of (ω^j, σ) on $\Gamma_{n+e}/\Gamma_{n+e+1}$ has dimension 1.

It remains to consider $e \equiv 0 \bmod d$. In this case, the size of the action domain grows by p, but also the size of the orbits grows by p, that is, the number of orbits remains stable; in other words, H has a single immediate descendant in $\mathcal{S}_n^*$. If $e \bmod d \in \mathcal{C} \setminus \{0\}$, then the size of the action domain grows by p, but the size of the orbit stays the same; in other words, H has p immediate descendants in $\mathcal{S}_n^*$. □

A Historical notes

A serious problem for classifying finite p-groups is that the number of isomorphism types of p-groups of order p^n grows exponentially with n; for large n, this makes a classification by order an impossible task. A more promising approach to bring structure into the realm of p-groups is to consider finite p-groups by *coclass*, where the coclass of a finite group of order p^n and nilpotency class c is defined as $n - c$. Note that the p-groups of maximal class are exactly the p-groups of coclass 1. Initiated by Leedham-Green and Newman [12] in 1980, this program is still an active area of research (cf. the recent work [2–5, 7, 9, 18]), which has led to deep and interesting results; we refer to the book of Leedham-Green and McKay [11] for more details and references.

A main tool in coclass theory is the coclass graph $\mathcal{G}(p, r)$ associated with the p-groups of coclass r. As for maximal class, the vertices of $\mathcal{G}(p, r)$ are identified with isomorphism type representatives of the considered groups, and there is an edge $G \to H$ if and only if G is isomorphic to $H/\gamma(H)$, where $\gamma(H)$ is the last non-trivial term of the lower central series of H. It is known that $\mathcal{G}(p, r)$ can be partitioned into a finite set of *isolated groups*, and a finite collection of *coclass trees*: a coclass tree is an infinite tree $\mathcal{T}$ which has a unique infinite path $G_1 \to G_2 \to \cdots$ starting at its root. The *branch* $\mathcal{B}_n$ of $\mathcal{T}$ is the subtree of $\mathcal{T}$ generated by all descendants of G_n which are not descendants of G_{n+1}; thus, every coclass tree can be partitioned into its branches, which are connected via the infinite path.

The main focus in coclass theory currently is to understand the structure of $\mathcal{G}(p, r)$. The aim of this appendix is to provide more details on known periodicity results for $\mathcal{G}(p, r)$, thereby putting our main results into context. We do not claim to present a complete historical account on existing results.

A.1 Coclass theory

The origins of coclass theory lie in the study of p-groups of maximal class. This study was initiated by Wiman [19] in 1952, and the first major results are due to Blackburn [1] in 1958. In particular, Blackburn obtained a complete classification

of the 2- and 3-groups of maximal class. Motivated by Blackburn's success, the p-groups of maximal class became a well-studied type of p-groups and, as a generalisation, Leedham-Green and Newman defined the coclass of a p-group in their 1980 paper [12]. Now coclass theory started out in two directions.

First, Leedham-Green and Newman related p-groups of a fixed coclass to certain extensions of uniserial space groups, so called pro-p-groups of fixed coclass. Their investigations culminated in the formulation of five Coclass Conjectures, called Conjecture A–E, where Conjecture A is the strongest since it implies Conjectures B–E. Many authors contributed to a proof of these conjectures, and the final proof of Conjecture A was found independently by Leedham-Green and Shalev, both in 1994. For details and references we refer to [11] and also the book of Dixon, du Sautoy, Mann and Segal [6, p. 265]. We remark that it is Conjecture D which implies that each coclass graph $\mathcal{G}(p, r)$ has finitely many coclass trees.

Second, between 1976 and 1984, Leedham-Green and McKay published a series of papers on p-groups of maximal class, see [10] and the references given there. The concept of *skeleton groups* (groups in the coclass graph which are defined by certain homomorphisms, cf. Section 4 for coclass 1) has its roots in these papers. It was proved later that these skeleton groups essentially determine the general structure of a coclass graph, cf. [11, Section 11], which underpins the importance of the skeletons.

Motivated by further promising computer experiments, the focus of coclass theory then turned to the investigation of the detailed structure of coclass graphs. The next section describes the main highlights of the last two decades.

A.2 Periodicities in coclass graphs

In general, $\mathcal{T}$ denotes a coclass tree with branches $\mathcal{B}_n$ in some specified coclass graph $\mathcal{G}(p, r)$. For an integer $k > 0$ let $\mathcal{B}_n(k)$ be the pruned subtree of $\mathcal{B}_n$ generated by all groups at depth at most k in $\mathcal{B}_n$.

For $p \in \{2, 3\}$, Blackburn proved that the branches of the coclass tree in $\mathcal{G}(p, 1)$ satisfy $\mathcal{B}_n \cong \mathcal{B}_{n+p-1}$ for all large enough n, that is, $\mathcal{G}(p, 1)$ is virtually periodic.

Newman [14], and later Dietrich, Eick and Feichtenschlager [5], did extensive computer experiments for $\mathcal{G}(5, 1)$, which suggest that $\mathcal{B}_n(n-1) \cong \mathcal{B}_{n+4}(n-1)$ 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. Eventually Dietrich [3] proved that indeed

$$\mathcal{B}_n(n-4) \cong \mathcal{B}_{n+4}(n-4) \quad \text{and} \quad \mathcal{B}_{n+4}(n) \setminus \mathcal{B}_{n+4}(n-4) \cong \mathcal{B}_n(n-4) \setminus \mathcal{B}_n(n-8)$$

for all large enough n; the proof that $\mathcal{B}_{n+4} \setminus B_{n+4}(n) \cong \mathcal{B}_n \setminus \mathcal{B}_n(n-4)$ for all large enough n is currently still missing. Nevertheless, these periodicity results describe $\mathcal{G}(5, 1)$ almost completely.

The investigations by Newman and by Leedham-Green and McKay already showed that the p-groups of maximal class are significantly more difficult to classify for $p \geq 7$. Their analysis revealed that the structure of $\mathcal{G}(p,1)$ is very complicated, and that a complete classification seems a highly non-trivial task. As a special case, Leedham-Green and McKay studied a subtree of the coclass tree in $\mathcal{G}(p,1)$ consisting of certain capable "1-parameter groups". Using the language of Section 4, these are the skeleton groups of the type $C_{n,e}(\mathbb{S}(\boldsymbol{c}))$, where $\boldsymbol{c} = (c_1, \ldots, c_\ell)$ with exactly one non-zero c_i. These subtrees of 1-parameter groups have finite widths if $p \equiv 5 \bmod 6$, cf. the comment on [10, p. 299].

Newman and O'Brien [15] investigated the graph $\mathcal{G}(2,r)$ for arbitrary r; their extensive computations led to the conjecture that each coclass tree in $\mathcal{G}(2,r)$ is virtually periodic, that is, there is an integer $d \geq 1$ such that $\mathcal{B}_n \cong \mathcal{B}_{n+d}$ for all large enough n.

The first periodicity theorem for general coclass graphs $\mathcal{G}(p,r)$ was established independently by du Sautoy [18] and Eick and Leedham-Green [8]: they proved that for every coclass tree with branches $\mathcal{B}_1, \mathcal{B}_2, \ldots$ and every integer $k > 0$, there exists $d \geq 1$ such that $\mathcal{B}_n(k) \cong \mathcal{B}_{n+d}(k)$ for all large enough n. The results by Eick and Leedham-Green [8] yield further that the virtual periodicity of a coclass tree translates to a classification of the groups in this tree in terms of finitely many parametrised group presentations. It is known that this periodicity pattern is capable of describing the complete graph $\mathcal{G}(p,r)$ if and only if $p = 2$ or $(p,r) \in \{(2,1),(3,1)\}$. In all other cases, there exist coclass trees which have branches of arbitrarily large depth and a second periodic pattern is required to describe the growth of these branches.

Dietrich [3, 4] considered $\mathcal{G}(p,1)$ in detail for $p \equiv 5 \bmod 6$; this work is the first analysis of coclass trees of infinite width. In particular, the results in [3] led to the aforementioned (almost complete) classification of $\mathcal{G}(5,1)$, which has finite width. For $p > 5$ the coclass tree in $\mathcal{G}(p,1)$ has infinite width, and the main result can be described as follows: First, there is an isomorphism of pruned branches $\mathcal{B}_n(n-2p+8) \cong \mathcal{B}_{n+p-1}(n-2p+8)$ for all large enough n. Second, if G is a capable group at depth $n-2p+8$ in $\mathcal{B}_{n+p-1}$ and if the automorphism group of its $(p-1)$-step parent H is a p-group, then $\mathcal{D}_{p-1}(G) \cong \mathcal{D}_{p-1}(H)$, where $\mathcal{D}_{p-1}(K)$ is the subtree generated by all descendants of K of distance at most $p-1$ to K. This second periodicity result describes the growth of the branches in some cases; it is a local result since it requires knowledge of the structure of the group and its $(p-1)$-step parent. It is known, however, that "almost all" p-groups have a p-group as automorphism group, hence the results in [3] can be used to describe large parts of $\mathcal{G}(p,1)$. We conclude this paragraph with two comments: First, the results in [3] are slightly more general than described here: a second periodicity result can also be formulated for groups whose $(p-1)$-step

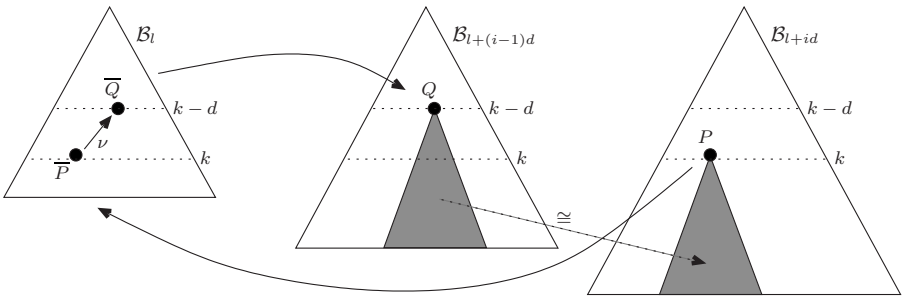

Figure 3. An illustration of Conjecture W.

parent does *not* have a p-group as automorphism group; instead, the requirement is that the group in question has bounded distance to a maximal path in $\mathcal{B}_n$ whose groups have automorphism group orders with constant p'-part; we refer to [3, Theorem 1.3] for more details. Note that the groups we consider in Theorem 1.1 satisfy this condition, which relates our work to the approach in [3]. Second, the maybe surprising restriction to $p \equiv 5 \bmod 6$ comes from underlying problems in p-adic number theory, already discussed in [10].

Eick, Leedham-Green, Newman and O'Brien [9] have investigated $\mathcal{G}(3,2)$ in detail. More precisely, they have studied the skeletons of each of the sixteen coclass trees of $\mathcal{G}(3,2)$. Each of these skeleton groups is a 1-parameter group (of coclass 2), and the trees have finite width. Based on their computations and the aforementioned existing results, Conjecture W in [9] suggests a construction of $\mathcal{G}(p,r)$ from a finite subgroup. We briefly sketch this conjecture here; for full details see [9, Section 9]. Let $\mathcal{T}$ be a coclass tree in $\mathcal{G}(p,r)$ with branches $\mathcal{B}_1, \mathcal{B}_2, \ldots$ of arbitrarily large depths. Choose $k \geq 1$; the results in [8] imply that there exist $d \geq 1$ and $l \in \mathbb{N}$ such that $B_l(k) \cong B_{l+id}(k)$ for all $i \in \mathbb{N}$. For a group $P \in B_{l+id}(k)$ denote by $\overline{P}$ the group in $\mathcal{B}_l(k)$ under a suitable graph isomorphism. Conjecture W now states that if one chooses k and l large enough, then there is a map ν from the groups of depth k in $\mathcal{B}_l$ to the groups of depth $k-d$ in $\mathcal{B}_l$ such that the following holds: If P has depth k in $\mathcal{B}_{l+id}$, then $\mathcal{D}(P) \cong \mathcal{D}(Q)$, where Q is the group at depth $k-d$ in $\mathcal{B}_{l+(i-1)d}$ corresponding to $\overline{Q} = \nu(\overline{P})$, and $\mathcal{D}(K)$ is the subtree generated by all descendants of K. This conjecture is illustrated in Figure 3.

In conclusion, with the exception of the local periodicity results in [3], all known periodicity results are for pruned subgraphs consisting of skeleton groups in coclass trees of finite width. Our Theorem 1.1 is the first result for such trees of infinite widths, and the first significant evidence supporting Conjecture W in this case.

Bibliography

[1] N. Blackburn, On a special class of p-groups, *Acta Math.* **100** (1958), 45–92.

[2] M. Couson, Character degrees of finite p-groups by coclass, *J. Algebra* **418** (2014), 91–109.

[3] H. Dietrich, A new periodic pattern in the graph of p-groups of maximal class, *Bull. Lond. Math. Soc.* **42** (2010), 1073–1088.

[4] H. Dietrich, Periodic patterns in the graph of p-groups of maximal class, *J. Group Theory* **13** (2010), 851–871.

[5] H. Dietrich, B. Eick and D. Feichtenschlager, Investigating p-groups by coclass with GAP, in: *Computational Group Theory and the Theory of Groups* (Davidson 2007), Contemp. Math. 470, American Mathematical Society, Providence (2008), 45–61.

[6] J. D. Dixon, M. P. F. du Sautoy, A. Mann and D. Segal, *Analytic Pro-p-groups*, 2nd ed., Cambridge University Press, Cambridge, 2003.

[7] B. Eick, Metabelian p-groups and coclass theory, *J. Algebra* **421** (2015), 102–118.

[8] B. Eick and C. R. Leedham-Green, On the classification of prime-power groups by coclass, *Bull. Lond. Math. Soc.* **40** (2008), 274–288.

[9] B. 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** (2013), 1243–1288.

[10] C. R. Leedham-Green and S. McKay, On the classification of p-groups of maximal class, *Quart. J. Math. Oxford* **35** (1984), 293–304.

[11] C. R. Leedham-Green and S. McKay, *The Structure of Groups of Prime Power Order*, London Math. Soc. Monogr. Ser. (N.S.) 27, Oxford University Press, Oxford, 2002.

[12] C. R. Leedham-Green and M. F. Newman, Space groups and groups of prime-power order I, *Arch. Math.* **35** (1980), 193–203.

[13] J. Neukirch, *Algebraische Zahlentheorie*, Springer, Berlin, 1992.

[14] M. F. Newman, Groups of prime-power order, in: *Groups* (Canberra 1989), Lecture Notes in Math. 1456, Springer, Berlin (1990), 49–62.

[15] M. F. Newman and E. A. O'Brien, Classifying 2-groups using coclass, *Trans. Amer. Math. Soc.* **351** (1990), 131–169.

[16] E. A. O'Brien, The p-group generation algorithm, *J. Symbolic Comput.* **9** (1990), 677–698.

[17] D. J. S. Robinson, Applications of cohomology groups to the theory of groups, in: *Groups* (St. Andrews 1981), London Math. Soc. Lecture Note Ser. 71, Cambridge University Press, Cambridge (1981), 46–80.

[18] M. du Sautoy, Counting p-groups and nilpotent groups, *Publ. Math. Inst. Hautes Etudes Sci.* **92** (2001), 63–112.

[19] A. Wiman, Über p-Gruppen mit maximaler Klasse, *Acta Math.* **88** (1952), 317–346.

[20] GAP – Groups, Algorithms and Programming, `http://www.gap-system.org`.

Received March 15, 2016.

Author information

Heiko Dietrich, School of Mathematical Sciences, Monash University,
Clayton VIC 3800, Australia.
E-mail: `heiko.dietrich@monash.edu`

Bettina Eick, Institut Computational Mathematics, Technische Universität Braunschweig,
Braunschweig, Germany.
E-mail: `beick@tu-bs.de`