

Spring 2012

# On a Problem of Burnside

Matthew Mizuhara  
*Bucknell University*

Follow this and additional works at: [https://digitalcommons.bucknell.edu/honors\\_theses](https://digitalcommons.bucknell.edu/honors_theses)

 Part of the [Mathematics Commons](#)

---

## Recommended Citation

Mizuhara, Matthew, "On a Problem of Burnside" (2012). *Honors Theses*. 120.  
[https://digitalcommons.bucknell.edu/honors\\_theses/120](https://digitalcommons.bucknell.edu/honors_theses/120)

This Honors Thesis is brought to you for free and open access by the Student Theses at Bucknell Digital Commons. It has been accepted for inclusion in Honors Theses by an authorized administrator of Bucknell Digital Commons. For more information, please contact [dcadmin@bucknell.edu](mailto:dcadmin@bucknell.edu).

# ON A PROBLEM OF BURNSIDE

by

Matthew Mizuhara

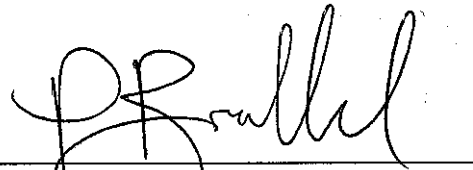
A Thesis

Presented to the Faculty of  
Bucknell University

in Partial Fulfillment of the Requirements for the Degree of  
Bachelor of Science with Honors in Mathematics

May 10, 2012

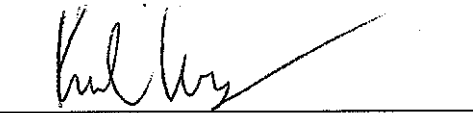
Approved:



---

Peter Brooksbank

Thesis Advisor



---

Karl Voss

Chair, Department of Mathematics

## Acknowledgments

I would like to thank my family and friends for their constant support and encouragement throughout the research and writing process. I also would like to thank my defense committee for their dedication and helpful feedback. Finally, I extend my deepest gratitude to my adviser, Professor Peter Brooksbank. His guidance, patience, and invaluable insight made this project possible.

# Contents

<b>1</b>	<b>Introduction</b>	<b>1</b>
<b>2</b>	<b>Preliminaries</b>	<b>3</b>
2.1	Groups . . . . .	3
2.2	Structure of Groups . . . . .	6
2.3	Nilpotent Groups and $p$ -Groups . . . . .	7
2.4	Automorphisms . . . . .	8
<b>3</b>	<b>Burnside's Problem</b>	<b>10</b>
<b>4</b>	<b>Computational Methods</b>	<b>12</b>
4.1	The Small Group Library . . . . .	12
4.2	Algorithms . . . . .	13
4.3	Computational Results . . . . .	15
<b>5</b>	<b><math>p</math>-Group Generation</b>	<b>18</b>

<i>CONTENTS</i>	iv
5.1 Generating $p$ -Groups . . . . .	18
5.2 Polycyclic Groups . . . . .	19
5.3 Power-conjugate Presentations . . . . .	19
5.4 The $p$ -Covering Group . . . . .	21
<b>6 A New Family of NI-Groups</b>	<b>23</b>
6.1 A Family of Groups . . . . .	24
6.2 Constructing the 2-Covering Group . . . . .	25
6.3 A Distinguished Descendant . . . . .	26
6.4 Consistency of the Immediate Descendant . . . . .	27
6.5 Constructing a Nearly-Inner Automorphism . . . . .	29
6.6 Proof Of Main Theorem . . . . .	33
<b>7 Conclusion</b>	<b>34</b>

# List of Tables

4.1	The NI-groups of order $\leq 1000^{(*)}$ . . . . .	17
-----	--	----

## List of Figures

2.1	Reflectional symmetries of the square . . . . .	4
4.1	Commutative diagram of permutation representation . . . . .	14

# Chapter 1

## Introduction

Groups are fundamental objects in mathematics and the natural sciences; they capture the essential properties of symmetry. In some instances, general properties intrinsic to a physical object or system can be understood in terms of the group structure underlying it. Groups themselves also possess symmetries in the form of *automorphisms*, which are bijective maps from a group to itself which preserve the group structure. Automorphisms arise “internally” in the sense that to each element of the group we can associate an *inner automorphism*. Most groups also possess “external” symmetries, namely automorphisms that are not inner.

In 1911, Burnside posed the question as to whether or not there exist groups having an external automorphism that behaves in a certain, specific way like an inner automorphism: we shall define such automorphisms to be *nearly-inner*. Two years later he answered his own question by exhibiting a family of such groups, which in general we shall call *NI-groups*. Burnside’s problem has been revisited by several researchers since that time. New families of NI-groups have been found [8, 11, 17], negative results have been proved about important families of groups [5, 13, 14, 15, 16], and connections have been made between NI-groups and other fields of study [13, 14, 15, 16, 7].

The general feeling that one develops from reading the literature is that NI-groups are fairly rare. With the aid of the computer algebra system MAGMA - in particular with the aid of its small group database - we set out to test this hypothesis.

As a consequence of the study, all NI-groups of size  $n$  for almost all  $n \leq 1000$



are now known (see Table 4.1). The obvious immediate conclusion we draw from our findings is that the NI-property is much more common than one might have thought. For instance, over 60% of the 56,092 pairwise non-isomorphic groups of order 256 are NI-groups.

Beyond mere curiosity, one key motivation of our exploration was to discover new infinite families of NI-groups. To this end we have also been successful (see Main Theorem in Chapter 6). The family that we build consists of certain finite groups, called *p*-groups, whose cardinality is a prime power. Our approach is based on a fairly modern technique for constructing *p*-groups. Related to that technique is an ambitious project to classify *p*-groups in terms of an invariant called *coclass*. The project was initiated in the 1980s by Leedham-Green and Newman [10] and has led to significant advances in our understanding of *p*-groups. One key result in this area asserts that the set of all *p*-groups of a fixed *coclass* contains a finite number of certain (infinite) families of groups, called “mainline families”. Our main result shows that there is at least one such mainline family of 2-groups of *coclass* 4 all of whose members are NI-groups.

The thesis is organized into the following chapters.

In Chapter 2 we summarize the group theoretic preliminaries we need to state our main results.

In Chapter 3 we introduce Burnside’s problem and briefly discuss its history.

Chapter 4 describes the algorithms that we used to process the small group database, searching for NI-groups. The results of our exhaustive search are also tabulated in this chapter.

In Chapter 5 we give a description of the technique mentioned above for constructing *p*-groups. We tailor this “*p*-group generation algorithm” to our specific needs.

In Chapter 6 we present our new family of groups and prove that each member is indeed an NI-group.

Finally, in Chapter 7 we provide some concluding remarks and observations, and we indicate some avenues for further investigation.

# Chapter 2

## Preliminaries

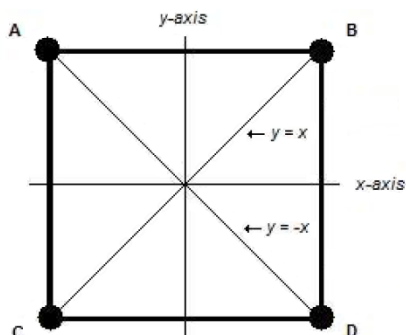
### 2.1 Groups

Symmetry plays a crucial role in mathematics as well as the physical sciences. Chemists, for example, study the self-similarity of crystal structures and physicists justify conservation laws using observations of symmetry in space-time. A **symmetry** of a geometric object is a distance-preserving transformation which leaves the shape visually unchanged.

As an example, consider a unit square centered about the origin (see Figure 2.1). The symmetries of the square are described as follows:

1. Clockwise rotation about the origin by  $0^\circ$ ; the identity transformation.
2. Clockwise rotation about the origin by  $90^\circ$ .
3. Clockwise rotation about the origin by  $180^\circ$ .
4. Clockwise rotation about the origin by  $270^\circ$ .
5. Reflection about the line  $x = 0$ .
6. Reflection about the line  $y = 0$ .
7. Reflection about the line  $y = x$ .

8. Reflection about the line  $y = -x$ .



**Figure 2.1:** Reflectional symmetries of the square

It is not hard to see, in fact, that any geometric object has an associated set of symmetries which satisfy several basic properties: every object has the trivial symmetry, every symmetry has an “inverse” symmetry which reverses the effect of the first symmetry, and the composition of any two symmetries is again a symmetry. Thus, composition defines an associative, binary operation on the symmetries of an object. This motivates the following definition.

**Definition.** A **group** is a nonempty set  $G$  along with a binary operation,  $*$ , that satisfies the following properties.

1. *Identity:* There exists an element  $1$  in  $G$  such that  $a * 1 = 1 * a = a$ .
2. *Inverses:* For each  $a$  in  $G$  there exists  $a^{-1}$  in  $G$  such that  $a * a^{-1} = a^{-1} * a = 1$ .
3. *Associativity:* If  $a$ ,  $b$ , and  $c$  are in  $G$  then  $(a * b) * c = a * (b * c)$ .

A group is formally an ordered pair  $(G, *)$ , but if the operation is clear, we simply denote the group by  $G$ . Similarly, when combining elements of a group, one typically suppresses the operation so that  $a * b$  is written  $ab$ .

Some common examples of groups are provided below.

1. The integers,  $\mathbb{Z}$ , is a group under standard addition.
2. The integers modulo  $n$ ,  $\mathbb{Z}_n$ , is a group under addition modulo  $n$ .
3. The non-zero rational numbers,  $\mathbb{Q}^*$ , is a group under standard multiplication.
4. A **permutation** of a set  $\Omega$  is a bijective function  $\rho : \Omega \rightarrow \Omega$ . Let  $\text{Sym}(\Omega)$  be the set of all permutations of  $\Omega$ . Then  $\text{Sym}(\Omega)$  is a group under function composition and we call  $\text{Sym}(\Omega)$  the **symmetric group on  $\Omega$** .
5. Generalizing our square example, the **dihedral group**,  $D_{2n}$ , is the group consisting of all symmetries of a regular  $n$ -gon under function composition. So,  $D_8$  is the group of symmetries of the square.

Observe that the group operation in examples 1, 2, and 3 is commutative whereas in examples 4 and 5 it is not. In  $D_8$ , for example, a  $90^\circ$  rotation followed by the reflection about the  $x$ -axis is not equal to the reflection about the  $x$ -axis followed by the  $90^\circ$  rotation. Those groups whose operation is commutative are special and are referred to as **abelian groups**.

If the underlying set of a group is finite, then its cardinality is called the **order** of the group, denoted  $|G|$ . If a finite group has order  $p^n$ , where  $p$  is prime, then it is called a  **$p$ -group**. As there are  $2^3 = 8$  symmetries of the square,  $D_8$  is a 2-group. The remainder of this paper assumes all groups are finite.

If we focus only on the rotational symmetries of the square, we note that the composition of two rotational symmetries is necessarily another rotational symmetry. The set of rotations of the square (including the identity symmetry) inherits the same function composition operation from the parent group and one can check that this subset is again a group. In general we say that a subset  $H$  of a group  $(G, *)$  is a **subgroup**, which we denote  $H \leq G$ , if  $(H, *)$  is a group. A subgroup  $H$  of  $G$  is **proper** if  $H \neq 1$  and  $H \neq G$ . The **center** of a group  $G$ , denoted  $Z(G)$ , is the set of elements which commute with all other elements, namely  $Z(G) = \{z \in G : zg = gz \text{ for all } g \in G\}$ . It is easy to verify that  $Z(G) \leq G$ .

In  $D_8$ , let  $r$  be the clockwise rotation by  $90^\circ$  and  $d$  the reflection over the  $x$ -axis. We see that every element of  $D_8$  may be obtained as a sequence of compositions of  $r$  and  $d$ . For example, rotation about the  $y$ -axis can be obtained by the sequence  $rrd = r^2d$ . In general a set  $S \subseteq G$  **generates** a group  $G$  if each element of  $G$  can be written as a product of elements (and their inverses) from  $S$ . We denote the group

generated by a set  $S$  by  $\langle S \rangle$ . For finite groups we often drop the set notation so that, for example,  $D_8 = \langle r, d \rangle$ . Groups which are generated minimally by  $d$  elements are called  **$d$ -generator groups**, and 1-generator groups are specially named **cyclic groups**.

## 2.2 Structure of Groups

It is possible to consider  $D_8$  as a group of permutations. Let  $(j k \ell \dots m)$  be the permutation which maps  $j \mapsto k \mapsto \ell \mapsto \dots \mapsto m \mapsto j$ . If we associate a letter to each corner of the square, then it is clear that each symmetry is simply a permutation of the set  $\{A, B, C, D\}$ . In particular, the rotational symmetry  $r$  is identified with  $(A B C D)$  and the reflectional symmetry with  $(A C)(B D)$ . Then the group  $\langle (A B C D), (A C)(B D) \rangle$  is a subgroup of  $\text{Sym}(\{A, B, C, D\})$  which is structurally equivalent to the group  $D_8$ .

A **homomorphism** between groups  $(G, *)$  and  $(H, \cdot)$  is a function  $\phi$  that is structure-preserving in the sense that for all  $g, g' \in G$ ,  $\phi(g * g') = \phi(g) \cdot \phi(g')$ . A surjective homomorphism is called an **epimorphism** and a bijective homomorphism is called an **isomorphism**. If an isomorphism exists between groups  $G$  and  $H$ , we say  $G$  and  $H$  are **isomorphic** and denote it  $G \cong H$ .

Although group structures can in general be quite complicated, we can gain insight by chopping them into basic pieces. This requires a special sort of subgroup called a normal subgroup. If  $H$  is any subgroup of a group  $G$  and  $g \in G$ , then the **left coset of  $H$  containing  $g$**  is

$$gH = \{gh : h \in H\}.$$

Each left coset has size equal to  $|H|$ . Given a group  $G$ , the **index** of a subgroup  $H \leq G$  is the number of cosets of  $H$  in  $G$ , denoted  $[G : H]$ . A famous result of Lagrange states that  $|G| = |H| \cdot [G : H]$ .

One can similarly define right cosets,  $Hg$ . In general it is not true that left and right cosets coincide for an arbitrary subgroup  $H$  of  $G$ ; subgroups that have this property are special and are crucial to understanding the structure of groups. We say that  $N$  is a **normal subgroup** of  $G$  if  $gN = Ng$  for all  $g \in G$ . Building upon the notation of subgroups, we write  $N \trianglelefteq G$  when  $N$  is a normal subgroup of  $G$ . Given a normal subgroup  $N$  of a group  $G$ , we can define the **quotient group**  $G/N$ , whose

elements are left cosets of  $N$  with group operation

$$(aN) \cdot (bN) = (ab)N.$$

Normality of  $N$  ensures that this operation is well-defined.

Thus, if  $N$  is a proper normal subgroup of  $G$ , we can hope to study  $G$  by considering  $N$  and  $G/N$ . Groups having no proper normal subgroups are the atoms of group theory: they are called **simple groups**. A simple abelian group is cyclic of prime order.

Given a group  $G$ , a normal subgroup  $N \trianglelefteq G$  is **maximal normal** if  $N \neq G$  and whenever a normal subgroup  $K$  satisfies  $N \trianglelefteq K \trianglelefteq G$  then either  $N = K$  or  $K = G$ . Choosing  $N_1 \trianglelefteq G$  to be a maximal normal subgroup, then  $G/N_1$  is simple. Next, choose  $N_2 \trianglelefteq N_1$  to again be a maximal normal subgroup. Iterating this process we get a chain of subgroups called a **composition series** for  $G$ :

$$G = N_1 \triangleright N_2 \triangleright \cdots \triangleright N_k = 1.$$

By a fundamental theorem of Jordan and Hölder, the *set* of simple quotients  $\{N_i/N_{i+1}\}$  is unique up to isomorphism. They are called the **composition factors** of  $G$ . Thus one can view  $G$  as being “built” from these basic building blocks; of course, there are many ways to glue these blocks together, which is to say that a group is not uniquely determined by its composition factors.

## 2.3 Nilpotent Groups and $p$ -Groups

The groups with which we will be concerned are ones whose composition factors are all abelian, and hence cyclic of prime order.

Given  $g, h \in G$ , the **commutator** of  $g$  and  $h$  is  $[g, h] := g^{-1}h^{-1}gh$ . Evidently, two elements commute precisely when  $[g, h] = 1$ . The **commutator subgroup** of subgroups  $K \leq G$  and  $H \leq G$  is

$$[K, H] := \langle [k, h] : k \in K, h \in H \rangle.$$

Note that this is the group generated by the commutators and not simply the set of them. As  $[h, k]^{-1} = [k, h]$ , it is clear that  $[H, K] = [K, H]$ . Further,  $[K, H] = 1$

precisely when all elements of  $K$  commute with all elements of  $H$ . So,  $[G, G] = 1$  if and only if when  $G$  is abelian.

The **lower central series** of a group  $G$  is a series

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

where  $\gamma_1(G) = G$  and, recursively,  $\gamma_i(G) = [G, \gamma_{i-1}(G)]$  for  $i \geq 2$ , is a normal subgroup of  $\gamma_{i-1}(G)$ . If  $\gamma_n = \{1\}$  for some  $n$ , we say that  $G$  is **nilpotent**. If  $G$  is nilpotent, the **nilpotency class** is  $c(G) := \min\{i : \gamma_{i+1}(G) = 1\}$ . Evidently, groups of nilpotency class 1 are abelian, and those of nilpotency class 2 may be thought of as being “close to abelian.”

An important class of nilpotent groups is the class of  $p$ -groups, introduced earlier. Consider, for example,  $D_8$ . Starting with  $D_8 = \gamma_1(D_8) = \langle r, d \rangle$ , we calculate  $\gamma_2(D_8) = [D_8, D_8] = \langle r^2 \rangle$ . It is then clear that  $\gamma_3(D_8) = [D_8, \langle r^2 \rangle] = 1$ , so  $D_8$  has nilpotency class 2.

A related invariant is the coclass of a  $p$ -group; a group of order  $p^n$  and nilpotency class  $c$  is said to have **coclass**  $n - c$ .

When computing with  $p$ -groups later on, it will be convenient to work with a refinement of the lower central series, called the **lower exponent- $p$  central series**. It is defined by the following sequence of subgroups

$$G = P_0(G) \geq \cdots \geq P_{i-1}(G) \geq P_i(G) \geq \cdots$$

with  $P_i(G) = [P_{i-1}(G), G]P_{i-1}(G)^p$  for each  $i \geq 1$ , where  $H^p = \{h^p : h \in H\}$ . As before,  $G$  has **exponent- $p$  class**  $c$ , or more simply **class**  $c$ , if  $c = \min\{i : P_i(G) = 1\}$ .

## 2.4 Automorphisms

An **automorphism** of a group  $G$  is an isomorphism from a group  $G$  to itself. The set of all automorphisms of  $G$  is denoted  $\text{Aut}(G)$ , which is itself a group under the operation of function composition. For  $\theta \in \text{Aut}(G)$  and  $x \in G$ , we write  $x\theta$  to denote the image of  $x$  under  $\theta$ . There is a rich source of automorphisms coming from within each group. Particularly, to each  $g \in G$  we associate a map  $\theta_g : G \rightarrow G$  called **conjugation by  $g$** , sending  $x \mapsto g^{-1}xg$  for each  $x \in G$ . For simplicity we write  $x^g$  to

represent  $x\theta_g$ . We call such automorphisms **inner automorphisms** and denote the set of all of them by  $\text{Inn}(G)$ . It is not hard to see that  $\text{Inn}(G)$  is isomorphic to the quotient  $G/Z(G)$ . Also by their very construction it is evident that  $\text{Inn}(G) \trianglelefteq \text{Aut}(G)$ . We call the quotient,

$$\text{Out}(G) := \text{Aut}(G)/\text{Inn}(G),$$

the **outer automorphism group** of  $G$ .



## Chapter 3

# Burnside's Problem

The question we address in this thesis - one first posed by Burnside - is concerned with the existence of groups that possess an automorphism which is not inner, yet behaves in a certain way like an inner automorphism. To introduce the main question we introduce a few more group theoretic concepts.

We say that  $x$  and  $y$  are **conjugates** if there exists some  $g \in G$  such that  $x^g = y$ . Conjugacy is an equivalence relation, and the equivalence classes under this relation are called **conjugacy classes**. For  $x \in G$ , let the conjugacy class represented by  $x$  be denoted by  $[x]$ ; that is,  $[x] = \{x^g : g \in G\}$ . Let  $\Omega$  be the set of conjugacy classes of  $G$ . Since  $(g^{-1}xg)\theta = (g\theta)^{-1}(x\theta)(g\theta)$  for all  $x, g \in G$  and all  $\theta \in \text{Aut}(G)$ , we see that each  $\theta \in \text{Aut}(G)$  induces a permutation  $\pi_\theta$  of  $\Omega$ , namely  $[x]\pi_\theta = [x\theta]$  for all  $[x] \in \Omega$ . Thus, one may define a homomorphism  $\pi : \text{Aut}(G) \rightarrow \text{Sym}(\Omega)$  sending  $\theta \mapsto \pi_\theta$ .

If  $\theta$  is an inner automorphism, then  $\theta$  only moves elements of a conjugacy class within the class, so  $\pi_\theta = 1$ . In particular,  $\text{Inn}(G)$  is in the kernel of  $\pi$ . We say that  $\theta \in \text{Aut}(G)$  is **nearly-inner** if  $\pi_\theta = 1$  (i.e. if  $\theta$  preserves conjugacy classes), so the kernel of  $\pi$  is the set of all nearly-inner automorphisms of  $G$ , often denoted  $\text{Aut}_c(G)$ . As  $\text{Aut}_c(G)$  is the kernel of a homomorphism, we conclude that  $\text{Aut}_c(G)$  is a normal subgroup of  $\text{Aut}(G)$ .

Burnside's question is the following: does there exist a group  $G$  such that  $\text{Aut}_c(G) \neq \text{Inn}(G)$ .

As  $\text{Inn}(G)$  is a normal subgroup of  $\text{Aut}_c(G)$ , we can construct

$$\text{Out}_c(G) := \text{Aut}_c(G)/\text{Inn}(G).$$

Clearly then,  $\text{Aut}_c(G) \neq \text{Inn}(G)$  precisely when  $\text{Out}_c(G) \neq 1$ . We shall henceforth refer to such groups as **NI-groups**.

Burnside first posed his question in 1911 [1]. In 1913, Burnside himself constructed an infinite family of  $p$ -groups which all are NI-groups [2], namely the groups of order  $p^6$  consisting of all  $3 \times 3$  matrices

$$M = \begin{pmatrix} 1 & 0 & 0 \\ x & 1 & 0 \\ z & y & 1 \end{pmatrix}$$

with  $x, y, z$  in the field  $\mathbb{F}_{p^2}$  of  $p^2$  elements, where  $p$  is an odd prime.

Since then, several other mathematicians have constructed new examples using a variety of tools. In 1947, Wall constructed a new family of NI-groups which contained an infinite family of 2-groups [17]. Other notable contributions include the work of Heineken [8], who, in 1980, constructed  $p$ -groups  $G$  with the property that  $\text{Aut}(G) = \text{Aut}_c(G)$ , so that all automorphisms of  $G$  are nearly-inner. Malinowska [11] constructed NI-groups of prime power order and nilpotency class  $r$  for all primes larger than 5 and  $r > 2$ . In the negative direction, Feit and Seitz [5] proved in 1988 that no finite simple group is an NI-group.

Recently Ono and Wada proved that none of the following are NI-groups: free groups;  $SL_n(R)$  or  $GL_n(R)$  where  $R$  is a Euclidean domain;  $S_n$  or  $A_n$ . Their motivation arose from the ‘‘Hasse principle’’ for smooth curves on a number field [13, 14, 15, 16]. The problem has connections with other areas of research. For example, the isomorphism problem for integral group rings asks if an isomorphism between integral group rings implies that the underlying groups are also isomorphic. Mazur [7] showed a connection between this problem and the existence of nearly-inner automorphisms in certain finite groups.

# Chapter 4

## Computational Methods

We have determined all NI-groups whose order is at most 1,000 (except those of order 384, 512, 640, 768, and 896). In this section we describe the computational methods we need to do this (and explain why some orders are missing from our catalog). To do this we used the library of small groups available within the computer algebra system MAGMA. The results are summarized in Table 4.1.

### 4.1 The Small Group Library

It is a non-trivial matter to construct all non-isomorphic groups of a given order. However both theoretical and computational results have been developed to classify groups of small order. The computer algebra system MAGMA has a small groups library developed by Besche, Eick, and O'Brien. The database contains all groups of order up to 2,000, excluding the groups of order 1,024 (due to the sheer number of groups of this order).

For our computational approach to Burnside's problem, we used the groups from this library and computed their automorphism groups. This is a notoriously difficult problem from the point of view of computational complexity. Nevertheless, for the modestly sized groups that we are considering here, the available computational tools are, for the most part, effective enough. One obstacle appears to be the construction of  $\text{Aut}(G)$  for certain "soluble" groups  $G$ . The missing orders 384, 640, 768, 896

consist entirely of such groups, and it seems infeasible to search through all of these groups using the current software.

For groups of order 512 the problem is one of scale. There are 10,494,213 groups of order 512: more than all of the remaining groups of order less than 1,000 put together. Fortunately, there are very efficient techniques to compute automorphism groups of  $p$ -groups. Thus, this task is at least a feasible one and is now almost complete.

## 4.2 Algorithms

Our problem is to construct, for a given group  $G$ , the group  $\text{Out}_c(G)$ , and to determine when this group is nontrivial. To this end, we recall that each automorphism  $\theta$  of  $G$  induces a permutation  $\pi_\theta$  of the conjugacy classes, where  $[x] \mapsto [x\theta]$ . Thus,  $\theta$  is nearly-inner if and only if  $\pi_\theta$  is the identity permutation. If  $\Omega = \{[x_1], \dots, [x_m]\}$  is the set of conjugacy classes of  $G$ , then the following algorithm computes the permutation induced by  $\theta$  on  $\Omega$ .

PERMUTATIONOFCLASSES( $G, \Omega, \theta$ )

**Input:** A group  $G$ , the set  $\Omega = \{[x_1], \dots, [x_m]\}$  of conjugacy classes of  $G$ , and  $\theta \in \text{Aut}(G)$ .

**Output:** The permutation,  $\pi_\theta$ , induced by  $\theta$  on  $\Omega$ .

```

1  $I := []$  /*Empty list*/
2 for  $i$  in  $\{1, \dots, m\}$  do
3   Set  $y_i := x_i\theta$ 
4   Find  $j \in \{1, \dots, m\}$  such that  $y_i \in [x_j]$ 
5   Set  $I[i] := j$ 
6 end for
7 return  $\pi_\theta$ , the permutation of  $\{1, \dots, m\}$  such that  $i\pi_\theta = I[i]$ 

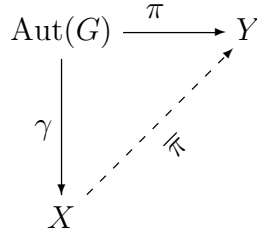
```

So PERMUTATIONOFCLASSES returns the identity permutation precisely when  $\theta$  is nearly-inner. We recall the homomorphism  $\pi : \text{Aut}(G) \rightarrow \text{Sym}(\Omega)$  which sends  $\theta \mapsto \pi_\theta$ . As is standard in computational group theory, we construct the image of  $\pi$  by computing  $\pi_\theta$  for each  $\theta$  in some generating set of  $\text{Aut}(G)$ .

Each element  $\theta \in \text{Aut}(G)$  clearly induces a permutation of the set  $G$ , namely the permutation  $\gamma_\theta : G \rightarrow G$ , sending  $g \mapsto g\theta$ . Let  $\gamma : \text{Aut}(G) \rightarrow \text{Sym}(G)$  be the

homomorphism sending  $\theta \mapsto \gamma_\theta$ . Let  $X = \text{Aut}(G)\gamma$  denote the isomorphic image of  $\text{Aut}(G)$  in  $\text{Sym}(G)$ , and  $Y = \text{Aut}(G)\pi$  the image of  $\text{Aut}(G)$  in  $\text{Sym}(\Omega)$ . Then there is a unique homomorphism  $\bar{\pi} : X \rightarrow Y$  such that the following diagram commutes.

**Figure 4.1:** Commutative diagram of permutation representation



The reason for converting from  $\text{Aut}(G)$  to the permutation representation,  $X$ , is merely to utilize the permutation group machinery of MAGMA.

We note that the order of  $\text{Sym}(G)$  is at most 1,000. MAGMA handles such permutation groups very easily; it can compute efficiently with permutation groups whose degrees are in the millions, so our upper bound ensures that these computations are trivial for MAGMA.

When applied to a set of generators for  $\text{Aut}(G)$ , the following algorithm constructs the group  $Y$  in Figure 4.1.

**ACTIONONCLASSES**( $A, \Omega$ )

**Input:** A list  $A = [\theta_1, \dots, \theta_t]$  of automorphisms of a group  $G$ , and  $\Omega$ , the set of conjugacy classes of  $G$ .

**Output:** The group induced by  $\langle A \rangle$  on  $\Omega$  and a map  $\pi : \langle A \rangle \rightarrow \text{Sym}(\Omega)$ .

- 1  $S := []$  /\*empty list\*/
- 2 for  $j$  in  $[1, \dots, t]$  do
- 3  $\pi_{\theta_j} := \text{PERMUTATIONOFCLASSES}(G, \theta_j)$
- 4 Add  $\pi_{\theta_j}$  to  $S$
- 5 end for
- 6 Let  $\pi : \langle A \rangle \rightarrow \text{Sym}(\Omega)$  sending  $\theta_i \mapsto \pi_{\theta_i}$ .
- 7 **return**  $\langle S \rangle \leq \text{Sym}(\Omega), \pi$

We can now present our algorithm to construct  $\text{Out}_c(G)$ .

OUTC( $G$ )

**Input:** A group  $G$ .

**Output:**  $\text{Out}_c(G)$ .

- 1 Construct  $\text{Aut}(G) = \langle \theta_1, \dots, \theta_t \rangle$
- 2 Compute  $\Omega$
- 3 Construct  $\gamma: \text{Aut}(G) \rightarrow \text{Sym}(G)$ , and put  $X := \text{Aut}(G)\gamma$
- 4 Construct  $X_I := \text{Inn}(G)\gamma$
- 5 Construct  $Y, \pi := \text{ActionOnClasses}([\theta_1, \dots, \theta_t], \Omega)$
- 6 for  $i$  in  $[1, \dots, t]$  do
  - 7 Compute  $\bar{\pi}: X \rightarrow Y$ , sending  $\theta_i\gamma \mapsto \theta_i\pi$
  - 8 end for
- 9 Construct  $K := \ker(\bar{\pi})$  /\* so that  $X_I \leq K \leq X$  \*/
- 10 Put  $\bar{K} := K/X_I$ , let  $\phi: K \rightarrow \bar{K}$  denote the natural map, and choose a generating set  $\bar{U}$  for  $\bar{K}$
- 11 Put  $U := \{(\bar{u}\phi^{-1})\gamma^{-1} : \bar{u} \in \bar{U}\} \leq \text{Aut}(G)$
- 12 **return**  $\langle U \rangle$

Note that  $|\text{Out}_c(G)| = |\langle \bar{K} \rangle|$  is computed in line 10, and  $G$  is an NI-group if and only if  $|\text{Out}_c(G)| \neq 1$ .

Using  $\text{OUTC}(G)$  we can calculate  $\text{Out}_c(G)$  for each group  $G$  with order less than 1,000. To ease the calculation, we note that  $\text{Out}_c(G) = 1$  if  $G$  is abelian, since  $[g] = \{g\}$  for all  $g \in G$ . Thus, the only automorphism fixing every conjugacy class fixes every element, which implies that the only class preserving automorphism is the identity automorphism. Thus we first test if a given group  $G$  is abelian and, if it is, we do not process it.

### 4.3 Computational Results

Below we list the results of our computations. The first column of the table lists those orders for which there exists at least one NI-group. For each order, we give the proportion of groups which are NI-groups out of the total number of groups of that order as well as the set of possible values of  $|\text{Out}_c(G)|$ .

In the table we let  $T_n$  be the number of groups of order  $n$  and  $N_n$  be the number of NI-groups of order  $n$ . Then, clearly  $P_n = |N_n|/|T_n|$  is the proportion of groups of

order  $n$  that are NI-groups. So, for any  $n$  not in this table,  $N_n = P_n = 0$ . Finally,  $O_n = \{|\text{Out}_c(G)| : |G| = n\} \setminus \{1\}$ .

We have observed several patterns from these data. One class of interesting groups consists of those for which  $\text{Aut}_c(G) = \text{Aut}(G)$ . From the data available, there are only five groups for which all automorphisms are class-preserving. In particular, there is one of order 128, one of order 468, and three of order 729. Other interesting patterns arose around NI-groups of prime-power order. Using the *p-group generation algorithm* (a concept introduced in the next chapter) and found that certain groups belong to infinite families of NI-groups. In the next two chapters we introduce one such family and prove that it consists entirely of NI-groups.

**Table 4.1:** The NI-groups of order  $\leq 1000^{(*)}$ 

$n$	$T_n$	$N_n$	$P_n$	$O_n$
32	51	2	0.03922	{ 2 }
64	267	40	0.14981	{ 2, 4, 16 }
96	231	8	0.03463	{ 2 }
128	2,328	767	0.32947	{ 2, 4, 8, 16, 64 }
160	238	8	0.03361	{ 2 }
192	1,543	233	0.15100	{ 2, 4, 16 }
200	52	1	0.01923	{ 2 }
224	197	8	0.04061	{ 2 }
243	67	8	0.11940	{ 3 }
256	56,092	34,112	0.60814	{ 2, 4, 8, 16, 32, 64 }
288	1,045	28	0.02679	{ 2 }
300	49	1	0.02041	{ 2 }
320	1,640	243	0.14817	{ 2, 4, 16 }
352	195	8	0.04103	{ 2 }
400	221	5	0.02262	{ 2 }
416	235	8	0.03404	{ 2 }
448	1,396	231	0.16547	{ 2, 4, 16 }
480	1,213	32	0.02638	{ 2 }
486	261	12	0.04598	{ 3 }
544	246	8	0.03252	{ 2 }
576	8,681	932	0.10736	{ 2, 4, 16 }
600	205	4	0.01951	{ 2 }
608	195	8	0.04103	{ 2 }
672	1,280	40	0.03125	{ 2 }
704	1,387	231	0.16655	{ 2, 4, 16 }
720	840	4	0.00476	{ 2 }
729	504	133	0.26389	{ 3, 9, 81 }
736	195	8	0.04103	{ 2 }
800	1,211	48	0.03964	{ 2 }
832	1,630	243	0.14908	{ 2, 4, 16 }
864	4,725	108	0.02286	{ 2 }
900	150	1	0.00667	{ 2 }
928	235	8	0.03404	{ 2 }
960	11,394	1,112	0.09760	{ 2, 4, 16 }
972	900	46	0.05111	{ 3 }
992	196	8	0.04082	{ 2 }
1,000	199	1	0.00503	{ 2 }

(\*) Except for orders 384, 512, 640, 768, and 896.



# Chapter 5

## $p$ -Group Generation

### 5.1 Generating $p$ -Groups

Recall from Chapter 3 that several researchers have produced infinite families of  $p$ -groups that are NI-groups. Our approach is rather different than those of earlier constructions in that we use a modern - but now fairly standard - method for constructing families of  $p$ -groups. The method, first developed by Havas and Newman, and later refined by O'Brien and others, is constructive, and is commonly known as the  $p$ -group generation algorithm. In this chapter we give an abbreviated description of this algorithm in order to provide the necessary theoretical platform for our main result in the next chapter.

A **word** on a set  $S$  is a finite product of elements and inverses from  $S$ . The **free group** on a finite set  $S$ , denoted  $F_S$ , is the group consisting of all words on  $S$ . If  $R$  is a subset of  $F = F_S$  then the smallest normal subgroup containing  $R$  is the **normal closure** of  $R$ , denoted  $\langle R \rangle^F$ .

A group  $G$  has a **finite presentation**  $\mathcal{S}$  if there exists  $R \subset F$  such that

$$G \equiv \langle \mathcal{S} \mid R \rangle := F / \langle R \rangle^F.$$

Elements of  $\mathcal{S}$  are called **generators** and elements of  $R$  are called **relations**.

## 5.2 Polycyclic Groups

A group  $G$  is **polycyclic** if it has a series

$$G = G_0 \triangleright G_1 \triangleright \cdots \triangleright G_n = 1,$$

where each  $G_i$  is a normal subgroup in  $G_{i-1}$  and  $G_i/G_{i+1}$  is a cyclic group for each  $0 \leq i \leq n-1$ .

For each  $i \in \{1, \dots, n\}$ , as  $G_i/G_{i+1}$  is cyclic, there exists some  $x_i \in G$  such that  $\langle x_i G_{i+1} \rangle = G_i/G_{i+1}$ . The sequence  $[x_1, \dots, x_n]$  is called a **polycyclic sequence** for  $G$ . One can show that for every  $g \in G$ , there exists a sequence of non-negative integers  $[e_1, \dots, e_n]$  such that  $g = x_1^{e_1} \cdots x_n^{e_n}$ . This representation of  $g$  is called the **normal form** of  $g$ . Commutators similarly have normal forms, which, in conjunction with the former forms, provide **polycyclic presentations** of polycyclic groups.

## 5.3 Power-conjugate Presentations

As our study focuses principally on  $p$ -groups, we focus on a specialized type of polycyclic presentation called a power-conjugate presentation. Such presentations provide a very efficient computational model for  $p$ -groups.

A **power-conjugate presentation** (or **pc-presentation**) of a finite  $p$ -group has as a generating set a finite set  $\{a_1, \dots, a_n\}$  with defining relations:

$$a_i^p = \prod_{k=i+1}^n a_k^{\beta(i,k)} \quad (0 \leq \beta(i,k) < p, \quad 1 \leq i \leq n)$$

$$a_j^{a_i} = a_j \prod_{k=j+1}^n a_k^{\beta(i,j,k)} \quad (0 \leq \beta(i,j,k) < p, \quad 1 \leq i < j \leq n.)$$

A  **$d$ -generator  $p$ -group** is a  $p$ -group which is minimally generated by  $d$  elements. Given a  $d$ -generator  $p$ -group, additional structure is imposed on the pc-presentation so that for each  $a_k \in \{a_{d+1}, \dots, a_n\}$  there is at least one relation involving  $a_k$  on the right hand side. We manipulate exactly one of these to be the **definition** of  $a_k$  by isolating the  $a_k$  term. If a power or commutator relation is omitted from the

pc-presentation, then it is assumed to be trivial. That is, an omitted power relation of  $a_i$  implies that  $a_i$  has order  $p$ , and an omitted commutator relation of  $a_j$  and  $a_i$  implies that  $a_j$  and  $a_i$  commute.

A presentation is **consistent** if the associated normal form is unique for each element. This implies that the order of the  $p$ -group is  $p^n$ . Every group of order  $p^n$  has a consistent power-conjugate presentation on  $n$  generators.

To every power-conjugate presentation,  $G = \langle S \mid R \rangle$ , there exists a **weight function** on the generators defined as follows:

$$w(a_j) = \max\{i \in \{1, \dots, c\} \mid a_j \in P_i(G)\},$$

where we recall that  $P_i(G)$  is the  $i$ th subgroup of the lower exponent- $p$  central series of  $G$ .

If a  $d$ -generator  $p$ -group has a consistent pc-presentation, then the following assignments determine the weights of generators:

1.  $w(a_i) = 1$  for  $i = 1, \dots, d$ .
2. If the definition of  $a_k$  is  $a_i^p = a_k$ , then  $w(a_k) = w(a_i) + 1$ .
3. If the definition of  $a_k$  is  $[a_j, a_i] = a_k$ , then  $w(a_k) = w(a_j) + w(a_i)$ .

An arbitrary word in the generators of a pc-group can be reduced to a normal form using the group relations. As originally described by Hall [6], given a word  $g = a_i a_j \cdots a_k a_\ell$ , if  $k > \ell$  we then write  $g = a_i a_j \cdots a_\ell a_k [a_k, a_\ell]$ , where the commutator  $[a_k, a_\ell]$  is equal to a product of generators with indices greater than  $k$  and  $\ell$ . Continuing in this fashion, this process must terminate, leaving  $g$  in normal form. This process is known as **collection** and is crucial to show the consistency of a pc-presentation. The following result, although true in more generality, has been tailored to suit our needs:

**Consistency Lemma** [9, p. 360]. *A weighted power-conjugate presentation of a 2-group with generators  $[a_1, \dots, a_n]$  is consistent if the following words collect to the*

trivial word:

$$\begin{aligned}
(a_k a_j) a_i &= a_k (a_j a_i) & 1 \leq i < j < k \leq m \text{ and } i \leq d, \\
& & w(a_i) + w(a_j) + w(a_k) \leq c. \\
(a_j a_j) a_i &= a_j (a_j a_i) & 1 \leq i < j \leq m \text{ and } i \leq d, w(a_i) + w(a_j) < c. \\
(a_j a_i) a_i &= a_j (a_i a_i) & 1 \leq i < j \leq m, w(a_i) + w(a_j) < c. \\
(a_i a_i) a_i &= a_i (a_i a_i) & 1 \leq i \leq m, 2w(a_i) < c.
\end{aligned}$$

where words in inner parentheses are collected first.

## 5.4 The $p$ -Covering Group

Let  $G$  be a  $p$ -group with generating number  $d$  and class  $c$ . A group  $H$  is a **descendant** of  $G$  if  $H$  has generating number  $d$  and the quotient  $H/P_c(H)$  is isomorphic to  $G$ . A descendant is an **immediate descendant** of  $G$  if it has class  $c + 1$ .

The construction of immediate descendants from  $G$  is completed by the computation of a group,  $G^*$ , called the  **$p$ -covering group** of  $G$ . The  $p$ -covering group has the property that each immediate descendant of  $G$  is isomorphic to a quotient of  $G^*$ .

In order to write a pc-presentation of the  $p$ -covering group, a total of  $q := d + \binom{n}{2}$  new generators,  $a_{n+1}, \dots, a_{n+q}$ , are introduced together with relations which make them central and of order  $p$ . We also must add definitions of each new generator. The following algorithm is extracted from [9, p. 360]:

P-COVERINGGROUP( $G$ )

**Input:** Consistent pc-presentation for a  $p$ -group  $G$ .

**Output:** Pc-presentation for its covering group  $G^*$ .

- 1  $A^* := A$
- 2  $R^* :=$  all relations from  $R$  which are definitions
- 3 Modify each non-defining relation  $a_i^p = w_i$  or  $[a_j, a_i] = w_{i,j}$  to be  $a_i^p = w_i a_r$  or  $[a_j, a_i] = w_{i,j} a_r$  for  $r \in \{n+1, \dots, n+q\}$ , where different relations are modified by different  $a_r$ .
- 4 Add each  $a_r$  to  $A^*$
- 5 Add  $a_r^p = 1$  to  $R^*$  for  $r \in \{n+1, \dots, n+q\}$
- 6 Add  $[a_r, a_i] = 1$  to  $R^*$  for  $r \in \{n+1, \dots, n+q\}$  and  $i \in \{1, r-1\}$
- 7 **return**  $G^* := \langle A^* \mid R^* \rangle$

Note that in general this presentation is not consistent.

If  $G$  and  $G^*$  are defined as above, we let  $K$  be the kernel of the natural map from  $G^* \rightarrow G$ ; we call  $K$  the ***p*-multiplier** of  $G$ , so that  $G \equiv G^*/K$ . We call  $P_c(G^*) \leq K$  the **nucleus** of  $G$ . Then,  $G$  has immediate descendants if and only if the nucleus is nontrivial, and each is obtained as  $G^*/M$  where  $M$  is a supplement to the nucleus in  $K$ . If the nucleus is trivial then the group  $G$  is **terminal**; otherwise it is **capable**.

We require the following lemma, which shows that automorphisms of  $H$  lift to automorphisms of  $H^*$  in a natural way.

**Lifting Lemma.** *If  $\theta \in \text{Aut}(G)$  maps  $\alpha_i \mapsto w_i(\alpha_1, \dots, \alpha_n)$  for  $i = 1, \dots, d$ , then  $\theta^*$  defined by  $a_i \mapsto w_i(a_1, \dots, a_n)$  for  $i = 1, \dots, d$  is an automorphism of  $G^*$ .*

## Chapter 6

# A New Family of NI-Groups

In this chapter we prove our main result, which is to establish that a certain family of finite presentations are in fact pc-presentations for a family of 2-groups which are all NI-groups. The construction arose from experimentation with the  $p$ -group generation algorithm described in the previous chapter, and the proof we give is by induction, based on a detailed analysis of the application of the algorithm to the groups in our family. The presentation of our proof is organized as follows.

In Section 6.1 we introduce our family of groups as a family of finite presentations  $\langle \mathcal{S}_n \mid \mathcal{R}_n \rangle$ , and state the main theorem. Sections 6.2 through 6.5 set up the inductive step of our proof of the main theorem. We assume throughout those sections that, for some  $n$ ,  $H = H_n = \langle \mathcal{S}_n \mid \mathcal{R}_n \rangle$  behaves as stated in the main theorem. In particular, the defining presentation is a consistent pc-presentation for  $H$ .

In Section 6.2, we give a pc-presentation for  $H^*$ , the 2-covering group of  $H$  (as described in Chapter 5). In Section 6.3 we identify a particular descendant of  $H$  as a quotient of  $H^*$ , and show that it is isomorphic to the group  $H_{n+1} = \langle \mathcal{S}_{n+1} \mid \mathcal{R}_{n+1} \rangle$ .

In order to prove that  $H_{n+1}$  is an *immediate* descendant of  $H_n$ , we must show that it has the right order, namely that  $|H_{n+1}| = 2|H_n|$ . This is done in Section 6.4 by proving that the presentations  $\langle \mathcal{S}_n \mid \mathcal{R}_n \rangle$  are, in fact, *consistent* pc-presentations.

It remains to show that each group  $H = H_n$  in our infinite family is an NI-group. To that end we exhibit a particular nearly-inner automorphism of  $H$  that is not inner. This we do again by induction, first lifting the automorphism from  $H$  to  $H^*$ , and then

inducing it on the distinguished quotient. The details are given in Section 6.5.

Finally, in Section 6.6, we give our proof of the main theorem, which follows easily from the preceding sections.

## 6.1 A Family of Groups

Let  $n \geq 2$  be an integer and consider  $\mathcal{S}_n = \{\gamma_1, \dots, \gamma_4, \zeta, \alpha_1, \dots, \alpha_n\}$ , a set of  $n + 5$  generators. Our choice of notation reflects the fact that our groups are all 4-generated by the elements  $\gamma_1, \dots, \gamma_4$ . Consider  $\mathcal{R}_n$ , the following set of  $3n + 1$  relations on  $\mathcal{S}_n$ :

$$(P) \alpha_{n-1}^2 = \alpha_n, \text{ and, if } n > 2, \alpha_i^2 = \alpha_{i+1}\alpha_{i+2}, \text{ for } i \in \{1, \dots, n-2\}.$$

$$(D) [\gamma_2, \gamma_1] = \zeta, [\gamma_3, \gamma_1] = \alpha_1 \text{ and } [\alpha_i, \gamma_1] = \alpha_{i+1} \text{ for } i \in \{1, \dots, n-1\}.$$

$$(C) [\gamma_3, \gamma_2] = \zeta, [\gamma_4, \gamma_1] = \zeta \text{ and } [\alpha_i, \gamma_3] = \alpha_{i+1} \text{ for } i \in \{1, \dots, n-1\}.$$

Relations of type (P) are called “power relations” (there are  $n-1$  of them). Relations of type (D) are called “definitions” (there are  $n+1$  of them). Relations of type (C) are called “commutators” (there are  $n+1$  of them). We recall that these relations will be part of a pc-presentation, so missing commutator relations are trivial. For example,  $[\gamma_4, \gamma_2] = 1$ .

Our main theorem is the following.

**Main Theorem.** *For each  $n \geq 2$ , the group  $H = H_n = \langle \mathcal{S}_n \mid \mathcal{R}_n \rangle$  has order  $2^{n+5}$  and class  $n+1$ . Furthermore, the following hold:*

(a)  $\langle \mathcal{S}_n \mid \mathcal{R}_n \rangle$  is a consistent pc-presentation for  $H$ .

(b) If  $P_i = P_i(H)$  denotes the  $i^{\text{th}}$  term in the exponent-2-central series for  $H$ , then

$$(i) P_0/P_1 = \langle \gamma_1 P_1, \gamma_2 P_1, \gamma_3 P_1, \gamma_4 P_1 \rangle \cong \mathbb{Z}_2^4;$$

$$(ii) P_1/P_2 = \langle \zeta P_2, \alpha_1 P_2 \rangle \cong \mathbb{Z}_2^2; \text{ and}$$

$$(iii) P_i/P_{i+1} = \langle \alpha_i P_{i+1} \rangle \cong \mathbb{Z}_2 \text{ for each } i = 2, \dots, n.$$

$$(c) Z(H) = \langle \zeta, \alpha_n \rangle \cong \mathbb{Z}_2^2.$$

(d) The map sending  $\gamma_4 \mapsto \gamma_4 \zeta$  and  $\beta \mapsto \beta$  for  $\beta \in \mathcal{S}_n \setminus \{\gamma_4\}$  extends to  $\theta = \theta_n \in \text{Aut}(H)$ . Furthermore,  $\theta$  is nearly-inner but not inner, so  $H$  is an NI-group.

## 6.2 Constructing the 2-Covering Group

Let  $n \geq 2$ , and  $H = H_n = \langle \mathcal{S}_n \mid \mathcal{R}_n \rangle$ . Suppose that  $H$  behaves as stated in the main theorem. In this section we build the 2-covering group of  $H$ , using the PCOVERING-GROUP algorithm as discussed in Section 5.4. We denote the pc-generators for  $H^*$  collectively as  $\mathcal{S}^*$  and individually as follows:

$g_1, \dots, g_4, z, a_1, \dots, a_n$	preimages of the generators for $H$
$b, d_1, d_2, d_3$	generators for the nucleus of $H$
$x_1, \dots, x_8$	remaining generators of the 2-multiplicator of $H$
$y_1, \dots, y_t$	generators that turn out to be trivial

The pc-relations,  $\mathcal{R}^*$ , for  $H^*$  are defined as follows:

1.  $[g_2, g_1] = z$ ,  $[g_3, g_1] = a_1$  and  $[a_i, g_1] = a_{i+1}$  for  $i \in \{1, \dots, n-1\}$ . Of course, these relations are simply the definitions of the analogous elements in  $H$ .
2. Definitions of the new generators:
  - (i)  $[a_n, g_1] = b$ ,  $a_{n-1}^2 = a_n d_1$ ,  $a_n^2 = d_2$ ,  $[a_n, g_3] = d_3$ .
  - (ii)  $g_i^2 = x_i$  for  $i \in \{1, \dots, 4\}$ ,  $[g_3, g_2] = z x_5$ ,  $[g_4, g_1] = z x_6$ ,  $[g_4, g_2] = x_7$ ,  $[g_4, g_3] = x_8$ .
  - (iii) One new generator for each remaining square, or commutator pair,  $[a_j, g_i]$ .
3. Powers of, and commutators involving each new generator are omitted from the pc-presentation, implying that each is central in  $H^*$  of order at most 2.

The subgroup,  $R$ , of  $H^*$  generated by the new generators is the 2-multiplicator of  $H^*$ , namely the kernel of the map  $H^* \rightarrow H$ , sending  $g_i \mapsto \gamma_i$  ( $i = 1, 2, 3, 4$ ).

**Lemma A.** *The nucleus of  $H$ , namely the group  $P_{n+1}(H^*)$ , is generated by the single generator  $b$ .*



*Proof.* Recall that  $P_n(H) = \langle \alpha_n \rangle$ , so  $P_n(H^*) = \langle a_n, R \rangle$ . Since  $R$  is elementary abelian and central in  $H^*$ , it follows that  $\{a_n^2, [a_n, g_i] : i = 1, 2, 3, 4\}$  is a generating set for  $P_{n+1}(H^*)$ . We now use associativity in  $H^*$  to deduce relations among those generators. Observe first that

$$a_{n-1}(a_{n-1}g_2) = a_{n-1}g_2a_{n-1}y_{2,n-1} = g_2a_{n-1}^2(y_{2,n-1})^2 = g_2a_nd_1,$$

while

$$(a_{n-1}a_{n-1})g_2 = a_nd_1g_2 = a_ng_2d_1 = g_2a_nd_1[a_ng_2].$$

Hence  $[a_n, g_2] = 1$ . Similarly,  $[a_n, g_4] = 1$ , so we have  $P_{n+1} = \langle b, d_2, d_3 \rangle$ . Next, we compute

$$\begin{aligned} a_{n-1}(g_1g_1) &= a_{n-1}x_1 \\ (a_{n-1}g_1)g_1 &= g_1a_{n-1}a_ng_1 = g_1a_{n-1}g_1a_nb = g_1^2a_{n-1}a_n^2b = a_{n-1}bd_2x_1, \end{aligned}$$

$$\begin{aligned} a_{n-1}(g_3g_3) &= a_{n-1}x_3 \\ (a_{n-1}g_3)g_3 &= (g_3a_{n-1}a_n)g_3[a_{n-1}, g_3] = g_3a_{n-1}g_3a_nd_3[a_{n-1}, g_3] = g_3^2a_{n-1}a_n^2d_3([a_{n-1}, g_3])^2 \\ &= a_{n-1}d_2d_3x_3, \end{aligned}$$

and

$$\begin{aligned} a_{n-2}(g_1g_1) &= a_{n-2}x_1 \\ (a_{n-2}g_1)g_1 &= g_1a_{n-2}a_{n-1}g_1 = g_1a_{n-2}g_1a_{n-1}a_n = g_1^2a_{n-2}a_{n-1}^2a_n = a_{n-2}a_n^2d_1x_1 \\ &= a_{n-2}d_1d_2x_1, \end{aligned}$$

from which we deduce that  $b = d_1 = d_2 = d_3$ . Hence, the nucleus  $P_{n+1}(H^*) = \langle b \rangle$ .  $\square$

### 6.3 A Distinguished Descendant

In this section we continue to assume that  $H = H_n$  is as stated in the theorem. Let  $H^*$  denote the 2-covering group of  $H$  described in the previous section.

**Lemma B.** *There is an epimorphism  $\phi : H^* \rightarrow H_{n+1}$ , so  $H_{n+1}$  is a descendant of  $H$ .*

*Proof.* Let  $M$  be the subgroup of  $R$  generated by all those new generators that are not equal to  $b$ . Thus  $M$  is a supplement to  $\langle b \rangle$  in  $R$ , and as such is an allowable subgroup of  $R$ . It follows that  $H^*/M$  is a descendant of  $H$  of order at most  $2^{5+n+1}$  (since  $[R : M] \leq 2$ ).

An examination of the defining relations for  $H^*$  reveals that, when we pass to the quotient  $H^*/M$ , denoting  $gM$  by  $\bar{g}$ , the only relations that remain are the following:

1. All of the analogues of the definitions from  $H$ .
2. (i)  $[\bar{a}_n, \bar{g}_1] = \bar{b} = [\bar{a}_n, \bar{g}_3] = \bar{a}_n^2$  and  $\bar{a}_{n-1}^2 = \bar{a}_n \bar{b}$ .  
(ii)  $[\bar{g}_3, \bar{g}_2] = \bar{z}$  and  $[\bar{g}_4, \bar{g}_1] = \bar{z}$ .  
(iii)  $[\bar{a}_i, \bar{g}_3] = \bar{a}_{i+1}$  for  $i \in \{1, \dots, n-1\}$ .

It is now easy to see that the assignment

$$\begin{array}{lll}
\bar{g}_i & \mapsto & \gamma_i \quad (i = 1, \dots, 4) \\
\bar{z} & \mapsto & \zeta \\
\bar{a}_j & \mapsto & \alpha_j \quad (j = 1, \dots, n) \\
\bar{b} & \mapsto & \alpha_{n+1}
\end{array}$$

extends to an isomorphism from  $H^*/M$  to  $H_{n+1} = \langle \mathcal{S}_{n+1} \mid \mathcal{R}_{n+1} \rangle$ .  $\square$

## 6.4 Consistency of the Immediate Descendant

In the previous two sections we assumed (inductively) that  $H = H_n$  is a group having pc-presentation  $\langle \mathcal{S}_n \mid \mathcal{R}_n \rangle$  and behaving as in the main theorem. We then showed that  $H$  has a descendant isomorphic to a group  $H_{n+1}$  with pc-presentation  $\langle \mathcal{S}_{n+1} \mid \mathcal{R}_{n+1} \rangle$ . To show that  $H_{n+1}$  is an *immediate* descendant (i.e. has order  $2^{n+5}$ ) we must show that the presentations  $\langle \mathcal{S}_n \mid \mathcal{R}_n \rangle$  are consistent.

**Lemma C.** *The pc-presentation for  $H_n$  is consistent.*

*Proof.* We use the Consistency Lemma stated in the previous chapter, manually carrying out the necessary collections.

Observe that any collection in which all three elements commute with each other

is trivial, so these are all excluded. We first consider relations involving  $\gamma_1$ .

$$\begin{aligned}(\gamma_3\gamma_2)\gamma_1 &= (\gamma_2\gamma_3z)\gamma_1 = \gamma_2\gamma_3\gamma_1z = \gamma_2\gamma_1\gamma_3\alpha_1z = \gamma_1\gamma_2\gamma_3\alpha_1z^2 = \gamma_1\gamma_2\gamma_3\alpha_1. \\ \gamma_3(\gamma_2\gamma_1) &= \gamma_3(\gamma_1\gamma_2z) = \gamma_1\gamma_3\alpha_1\gamma_2z = \gamma_1\gamma_3\gamma_2\alpha_1z = \gamma_1\gamma_2\gamma_3\alpha_1z^2 = \gamma_1\gamma_2\gamma_3\alpha_1.\end{aligned}$$

$$\begin{aligned}(\gamma_4\gamma_2)\gamma_1 &= (\gamma_2\gamma_4)\gamma_1 = \gamma_2\gamma_1\gamma_4z = \gamma_1\gamma_2\gamma_4z^2 = \gamma_1\gamma_2\gamma_4. \\ \gamma_4(\gamma_2\gamma_1) &= \gamma_4(\gamma_1\gamma_2z) = \gamma_1\gamma_4\gamma_2z^2 = \gamma_1\gamma_2\gamma_4.\end{aligned}$$

$$\begin{aligned}(\alpha_k\gamma_2)\gamma_1 &= (\gamma_2\alpha_k)\gamma_1 = \gamma_2\gamma_1\alpha_k\alpha_{k+1} = \gamma_1\gamma_2z\alpha_k\alpha_{k+1} \\ \alpha_k(\gamma_2\gamma_1) &= \alpha_k(\gamma_1\gamma_2z) = \gamma_1\alpha_k\alpha_{k+1}\gamma_2z = \gamma_1\gamma_2z\alpha_k\alpha_{k+1}.\end{aligned}$$

$$\begin{aligned}(\gamma_4\gamma_3)\gamma_1 &= (\gamma_3\gamma_4)\gamma_1 = \gamma_3\gamma_1\gamma_4z = \gamma_1\gamma_3\alpha_1\gamma_4z = \gamma_1\gamma_3\gamma_4z\alpha_1 \\ \gamma_4(\gamma_3\gamma_1) &= \gamma_4(\gamma_1\gamma_3\alpha_1) = \gamma_1\gamma_4z\gamma_3\alpha_1 = \gamma_1\gamma_4\gamma_3z\alpha_1 = \gamma_1\gamma_3\gamma_4z\alpha_1.\end{aligned}$$

$$\begin{aligned}(\alpha_k\gamma_3)\gamma_1 &= (\gamma_3\alpha_k\alpha_{k+1})\gamma_1 = \gamma_3\alpha_k\gamma_1\alpha_{k+1}\alpha_{k+2} = \gamma_3\gamma_1\alpha_k\alpha_{k+1}^2\alpha_{k+2} = \gamma_1\gamma_3\alpha_1\alpha_k\alpha_{k+1}^2\alpha_{k+2} \\ \alpha_k(\gamma_3\gamma_1) &= \alpha_k(\gamma_1\gamma_3\alpha_1) = \gamma_1\alpha_k\alpha_{k+1}\gamma_3\alpha_1 = \gamma_1\alpha_k\gamma_3\alpha_{k+1}\alpha_{k+2}\alpha_1 = \gamma_1\gamma_3\alpha_1\alpha_k\alpha_{k+1}^2\alpha_{k+2}.\end{aligned}$$

$$\begin{aligned}(\alpha_k\gamma_4)\gamma_1 &= (\gamma_4\alpha_k)\gamma_1 = \gamma_4\gamma_1\alpha_k\alpha_{k+1} = \gamma_1\gamma_4z\alpha_k\alpha_{k+1} \\ \alpha_k(\gamma_4\gamma_1) &= \alpha_k(\gamma_1\gamma_4z) = \gamma_1\alpha_k\alpha_{k+1}\gamma_4z = \gamma_1\gamma_4z\alpha_k\alpha_{k+1}.\end{aligned}$$

$$\begin{aligned}(\alpha_k\alpha_j)\gamma_1 &= (\alpha_j\alpha_k)\gamma_1 = \alpha_j\gamma_1\alpha_k\alpha_{k+1} = \gamma_1\alpha_j\alpha_{j+1}\alpha_k\alpha_{k+1} \\ \alpha_k(\alpha_j\gamma_1) &= \alpha_k(\gamma_1\alpha_j\alpha_{j+1}) = \gamma_1\alpha_k\alpha_{k+1}\alpha_j\alpha_{j+1} = \gamma_1\alpha_j\alpha_{j+1}\alpha_k\alpha_{k+1}.\end{aligned}$$

$$\begin{aligned}(\alpha_j\alpha_j)\gamma_1 &= \alpha_{j+1}\alpha_{j+2}\gamma_1 = \alpha_{j+1}\gamma_1\alpha_{j+2}\alpha_{j+3} = \gamma_1\alpha_{j+1}\alpha_{j+2}^2\alpha_{j+3} \\ \alpha_j(\alpha_j\gamma_1) &= \alpha_j(\gamma_1\alpha_j\alpha_{j+1}) = \gamma_1\alpha_j\alpha_{j+1}\alpha_j\alpha_{j+1} = \gamma_1\alpha_j^2\alpha_{j+1}^2 = \gamma_1\alpha_{j+1}\alpha_{j+2}^2\alpha_{j+3}.\end{aligned}$$

For the cases regarding  $\gamma_3$ , we simply observe that the definitions and commutator relations involving  $\gamma_3$  are the same as  $\gamma_1$ , so all calculations follow similarly.

We now consider collections involving  $\gamma_2$ .

$$\begin{aligned}(\gamma_4\gamma_3)\gamma_2 &= \gamma_3\gamma_4\gamma_2 = \gamma_3\gamma_2\gamma_4 = \gamma_2\gamma_3z\gamma_4 = \gamma_2\gamma_3\gamma_4z \\ \gamma_4(\gamma_3\gamma_2) &= \gamma_4(\gamma_2\gamma_3z) = \gamma_2\gamma_4\gamma_3z = \gamma_2\gamma_3\gamma_4z.\end{aligned}$$

$$\begin{aligned}(\alpha_k\gamma_3)\gamma_2 &= (\gamma_3\alpha_k\alpha_{k+1})\gamma_2 = \gamma_3\gamma_2\alpha_k\alpha_{k+1} = \gamma_2\gamma_3z\alpha_k\alpha_{k+1} \\ \alpha_k(\gamma_3\gamma_2) &= \alpha_k(\gamma_2\gamma_3z) = \gamma_2\alpha_k\gamma_3z = \gamma_2\gamma_3\alpha_k\alpha_{k+1}z = \gamma_2\gamma_3z\alpha_k\alpha_{k+1}.\end{aligned}$$

The remaining cases are described completely as follows:

$$(i) \quad (\zeta\gamma_j)\gamma_i = \zeta(\gamma_j\gamma_i) \text{ and } (\alpha_k\zeta)\gamma_i = \alpha_k(\zeta\gamma_i),$$

- (ii)  $(hh)g = h(hg)$ ,
- (iii)  $(hg)g = h(gg)$ , and
- (iv)  $(gg)g = g(gg)$ ,

where  $j \in \{1, \dots, 4\}$ ,  $k \in \{1, \dots, n\}$  and  $g, h \in \{\gamma_1, \dots, \gamma_4, \zeta\}$ . These are easy to verify, as  $\zeta$  is central and each element in  $\{\gamma_1, \dots, \gamma_4, \zeta\}$  has order 2.  $\square$

## 6.5 Constructing a Nearly-Inner Automorphism

In this section we consider the automorphism  $\theta$  described in the main theorem. We first show, again by induction, that  $\theta_n$  is an automorphism of  $H_n$ .

Once again, suppose that the given assignment on generators extends to an automorphism,  $\theta$ , of  $H = H_n$  behaving as in part (e) of the main theorem. By the Lifting Lemma,  $\theta$  lifts to an automorphism of  $H^*$  that sends  $g_i \mapsto g_i$  ( $i = 1, 2, 3$ ), and  $g_4 \mapsto g_4z$ . We compute the image under  $\theta^*$  of the remaining pc-generators of  $H^*$ . We first prove the following lemma.

**Lemma D.** *The element  $z^2$ , and all commutators  $[z, g_i]$  and  $[a_i, z]$ , are trivial in  $H^*$ .*

*Proof.* First, we compute

$$\begin{aligned} g_4(g_3g_2) &= g_4(g_2g_3zx_5) = g_2g_4g_3zx_5x_7 = g_2g_3g_4zx_5x_7x_8 \\ (g_4g_3)g_2 &= (g_3g_4)g_2x_8 = g_3g_2g_4x_7x_8 = g_2g_3zg_4x_5x_7x_8 = g_2g_3g_4z[z, g_4]x_5x_7x_8. \end{aligned}$$

It follows that  $[z, g_4] = 1$ . Next,

$$\begin{aligned} (g_4g_4)g_1 &= x_4g_1 = g_1x_4 \\ g_4(g_1g_1) &= g_4(g_1g_4zx_6) = g_1g_4zg_4zx_6^2 = g_1g_4zg_4z = g_1g_4^2z[z, g_4]z = g_1z^2[z, g_4]x_4, \end{aligned}$$

so that  $z^2 = [z, g_4] = 1$ . Also,

$$\begin{aligned} (g_4g_1)g_1 &= g_1g_4zg_1x_6 = g_1g_4g_1z[z, g_1]x_6 = g_1^1g_4z^2[z, g_1]x_6^2 = g_4x_1z^2[z, g_1] \\ g_4(g_1g_1) &= g_4x_1, \end{aligned}$$

so  $[z, g_1] = z^2 = 1$ . Next,

$$\begin{aligned} g_4(g_2g_1) &= g_4(g_1g_2z) = g_1g_4zx_6g_2z = g_1g_4g_2z[z, g_2]zx_6 = g_1g_2g_4z[z, g_2]zx_6x_7 \\ (g_4g_2)g_1 &= (g_2g_4x_7)g_1 = g_2g_1g_4zx_6x_7 = g_1g_2zg_4zx_6x_7 = g_1g_2g_4z[z, g_4]zx_6x_7, \end{aligned}$$

so that  $[z, g_2] = [z, g_4] = 1$ . Next,

$$\begin{aligned} g_3(g_3g_2) &= g_3(g_2g_3zx_5) = g_2g_3zx_5g_3zx_5 = g_2g_3g_3z[z, g_3]zx_5^2 = g_2z[z, g_3]zx_3 \\ (g_3g_3)g_2 &= x_3g_2 = g_2x_3, \end{aligned}$$

so that  $[z, g_3] = z^2 = 1$ . Also,

$$\begin{aligned} (zg_3)g_1 &= g_3zg_1[z, g_3] = g_3g_1z[z, g_1][z, g_3] = g_1g_3a_1z[z, g_1][z, g_3] = g_1g_3za_1[a_1, z][z, g_1][z, g_3] \\ z(g_3g_1) &= zg_1g_3a_1 = g_1zg_3a_1[z, g_1] = g_1g_3za_1[z, g_1][z, g_3], \end{aligned}$$

so  $[a_1, z] = 1$ . Finally, for  $i \in \{1, \dots, n-1\}$ , let  $y_i$  denote the generator of  $H^*$  defined by  $[a_i, g_3] = a_{i+1}y_i$ . Then,

$$\begin{aligned} a_i(zg_3) &= a_i g_3 z [z, g_3] = g_3 a_i a_{i+1} z [z, g_3] y_i = g_3 z a_i a_{i+1} [z, g_3] [a_i, z] y_i [a_{i+1}, z] \\ (a_i z) g_3 &= z a_i [a_i, z] g_3 = z g_3 a_i a_{i+1} [a_i, z] y_i = g_3 z a_i a_{i+1} [z, g_3] [a_i, z] y_i, \end{aligned}$$

so  $[a_{i+1}, z] = 1$  for  $i = 1, \dots, n-1$ . □

**Lemma E.** *The automorphism  $\theta^*$  fixes every generator of  $H^*$  except for  $g_4$ .*

*Proof.* First, since the definitions of  $z, a_1, \dots, a_n$  are precisely the same as those of  $\zeta, \alpha_1, \dots, \alpha_n$  in  $H$ , it is clear that  $\theta^*$  fixes each of these generators. Moreover, the only new generators that are potentially not fixed are those whose definition involves  $g_4$ . Using Lemma D where appropriate,

$$x_4\theta^* = (g_4^2)\theta^* = (g_4\theta^*)^2 = (g_4z)^2 = g_4^2z[z, g_4]z = x_4z^2 = x_4.$$

Next,

$$\begin{aligned} z(x_6\theta^*) &= (z\theta^*)(x_6)\theta^* = (zx_6)\theta^* &= [g_4, g_1]\theta^* \\ & &= [g_4z, g_1] \\ & &= [g_4, g_1]^z[z, g_1] = (zx_6)^z = zx_6, \end{aligned}$$

so that  $x_6\theta^* = x_6$ . Similarly,  $\theta^*$  fixes each new generator defined as a commutator with  $g_4$ . □

From Lemma B, it follows that  $\theta^*$  induces an automorphism  $\bar{\theta}$  on  $\bar{H} := H^*/M$  which, as we have seen, is isomorphic to  $H_{n+1}$ . Furthermore it is clear that  $\bar{\theta}$  is precisely the map  $\theta_{n+1}$  in the main theorem. Thus, if  $\theta_m \in \text{Aut}(H_m)$  for some  $m \geq 2$ , then  $\theta_n \in \text{Aut}(H_n)$  for all  $n \geq m$ . It remains to show that the automorphism,  $\theta = \theta_n$ , of  $H_n$  is nearly-inner but not inner.

**Lemma F.**  $\theta \in \text{Aut}(H_n)$  is not inner.

*Proof.* If  $\theta$  is inner, then there exists  $\delta \in H$  such that  $\gamma_4^\delta = \gamma_4\zeta$ . Since the presentation for  $H$  is consistent, we can write  $\delta$  uniquely as  $\delta = \gamma_1^\epsilon \gamma_2^{\epsilon_2} \dots \gamma_n^{\epsilon_n} = \gamma_1^\epsilon \mu$ , where  $\mu := \gamma_2^{\epsilon_2} \dots \gamma_n^{\epsilon_n}$  must commute with  $\gamma_4$ . As  $\delta$  does not commute with  $\gamma_4$ , we have  $\epsilon = 1$ , so  $\gamma_4^\delta = \gamma_4^{\gamma_1 \mu} = (\gamma_4 \zeta)^\mu = \gamma_4 \zeta$ , as required. However, if we let  $\xi = \gamma_4^{\epsilon_4} \dots \gamma_n^{\epsilon_n}$ , then

$$\gamma_3 = \gamma_3^\delta = \gamma_3^{\gamma_1 \gamma_2^{\epsilon_2} \gamma_3^{\epsilon_3} \xi} = (\gamma_3 \alpha_1)^{\gamma_2^{\epsilon_2} \gamma_3^{\epsilon_3} \xi} = (\gamma_3 \zeta^{\epsilon_2} \alpha_1)^{\gamma_3^{\epsilon_3} \xi} = (\gamma_3 \zeta^{\epsilon_2} \alpha_1 \alpha_2^{\epsilon_3})^\xi.$$

As  $\xi$  commutes with  $\zeta$ ,  $\alpha_1$ , and  $\alpha_2$ , we can write  $\gamma_3^\delta = \gamma_3 \alpha_1 \alpha$ , where  $\alpha \in \langle \zeta, \alpha_2, \dots, \alpha_n \rangle$ . In particular,  $\gamma_3^\delta \neq \gamma_3$ . It follows that  $\theta$  is not inner.  $\square$

To prove that  $\theta$  is nearly-inner, we first prove the following lemma.

**Lemma G.** For all  $i = i, \dots, n-1$ , it holds that  $\alpha_i^2 \alpha_{i+1} = 1$  and  $\alpha_i^4 \alpha_{i+1}^2 = 1$

*Proof.* Since  $\alpha_i^2 \alpha_{i+1} = (\alpha_{i+1} \alpha_{i+2}) \alpha_{i+1} = \alpha_{i+1}^2 \alpha_{i+2}$ , by induction  $\alpha_i^2 \alpha_{i+1} = \alpha_{n-1}^2 \alpha_n = \alpha_n \alpha_n = 1$ . Similarly,  $\alpha_i^4 \alpha_{i+1}^2 = (\alpha_{i+1} \alpha_{i+2}^2) \alpha_{i+1}^2 = \alpha_{i+1}^4 \alpha_{i+2}^2$ , so by induction  $\alpha_i^4 \alpha_{i+1}^2 = \alpha_{n-1}^4 \alpha_n^2 = 1$ .  $\square$

**Lemma H.**  $\theta \in \text{Aut}(H_n)$  is nearly-inner.

*Proof.* We must show that, for all  $g \in H$ , there exists  $h = h(g) \in G$  such that  $g\theta = g^h$ . Since each  $g \in H$  has a unique normal form, namely

$$g = \gamma_1^{\delta_1} \dots \gamma_4^{\delta_4} \zeta^\epsilon \alpha_1^{\epsilon_1} \alpha_2^{\epsilon_2} \dots \alpha_n^{\epsilon_n},$$

where  $\delta_i, \epsilon, \epsilon_j \in \{0, 1\}$ . If  $\delta_4 = 0$ , then it is clear that  $g\theta = g = g^1$ . So, we only consider the cases when  $\delta_4 = 1$ . In these cases,  $g\theta = g \cdot \zeta$ , so we seek an  $h \in H$

satisfying  $g^h = g \cdot \zeta$ .

**Case 1:** *The parity of  $\delta_1 + \delta_3$  is odd.* Let  $h = \gamma_2$ . If  $\delta_1 = 1$  then  $\delta_3 = 0$ , so

$$g = \gamma_1 \gamma_2^{\delta_2} \gamma_4 \zeta^\epsilon \alpha_1^{\epsilon_1} \cdots \alpha_n^{\epsilon_n}.$$

Then,

$$\begin{aligned} g^{\gamma_2} &= \gamma_1^{\gamma_2} (\gamma_2^{\delta_2})^{\gamma_2} \gamma_4^{\gamma_2} (\zeta^\epsilon)^{\alpha_2} (\alpha_1^{\epsilon_1})^{\gamma_2} \cdots (\alpha_n^{\epsilon_n})^{\alpha_2} \\ &= (\gamma_1 \zeta) (\gamma_2^{\delta_2}) (\gamma_4) \cdots (\alpha_n^{\epsilon_n}) = g \cdot \zeta. \end{aligned}$$

In the other case  $\delta_1 = 0$  and  $\delta_3 = 1$ , and the result holds similarly.

Before proving the second case, we establish the following claims:

**Claim:** For each  $x \in \{\gamma_2, \zeta, \alpha_1, \dots, \alpha_n\}$ , it holds that  $x^{\gamma_1 \gamma_3} = x$ .

The claim is easy proved by considering the cases  $\gamma_2, \zeta$ , and  $\alpha_i$  separately. In particular, for  $\alpha_i$  it holds that

$$\begin{aligned} (\alpha_i^{\gamma_1})^{\gamma_3} &= (\alpha_i \alpha_{i+1})^{\gamma_3} = \alpha_i^{\gamma_3} \alpha_{i+1}^{\gamma_3} = (\alpha_i \alpha_{i+1}) (\alpha_{i+1} \alpha_{i+2}) \\ &= \alpha_i \alpha_{i+1}^2 \alpha_{i+2} = \alpha_i, \end{aligned}$$

where the last equality holds by Lemma G.

**Claim:**  $\alpha_1 \alpha_2 \gamma_3 \alpha_1 \alpha_2 = \gamma_3$ .

The claim is proved similarly, noting that

$$\begin{aligned} \alpha_1 \alpha_2 \gamma_3 \alpha_1 \alpha_2 &= \alpha_1 (\gamma_3 \alpha_2 \alpha_3) \alpha_1 \alpha_2 = (\gamma_3 \alpha_1 \alpha_2) \alpha_2 \alpha_3 \alpha_1 \alpha_2 = \gamma_3 (\alpha_1^2 \alpha_2^3 \alpha_3) \\ &= \gamma_3 ((\alpha_2 \alpha_3) \alpha_2^3 \alpha_3) = \gamma_3 (\alpha_2^4 \alpha_3^2) = \gamma_3, \end{aligned}$$

where again, the last equality holds by Lemma G.

These two claims are sufficient to prove the second case of our lemma.

**Case 2:** *The parity of  $\delta_1 + \delta_3$  is even.* Let  $h = \gamma_1 \gamma_3$ . If  $\delta_1 = 0$  then  $\delta_3 = 0$ , so

$$g = \gamma_2^{\delta_2} \gamma_4 \zeta^{\delta_5} \cdots \alpha_n^{\epsilon_n}.$$

Thus,

$$g^{\gamma_1 \gamma_3} = (\gamma_2^{\delta_2})^{\gamma_1 \gamma_3} (\gamma_4)^{\gamma_1 \gamma_3} (\zeta^{\delta_5})^{\gamma_1 \gamma_3} \cdots (\alpha_n^{\epsilon_n})^{\gamma_1 \gamma_3} = \gamma_2^{\delta_2} (\gamma_4 \zeta) (\zeta^{\delta_5}) \cdots (\alpha_n^{\epsilon_n}).$$

If  $\delta_1 = \delta_3 = 1$  then we still take  $h = \gamma_1\gamma_3$ , but note that  $\gamma_1^{\gamma_1\gamma_3} = \gamma_1\alpha_1\alpha_2$ , and  $\gamma_3^{\gamma_1\gamma_3} = \gamma_1\alpha_1\alpha_2$ . As  $g = \gamma_1\gamma_2^{\delta_2}\gamma_3\gamma_4\zeta^{\delta_5} \cdots \alpha_n^{\epsilon_n}$ , we have

$$\begin{aligned} g^{\gamma_1\gamma_3} &= (\gamma_1^{\gamma_1\gamma_3})(\gamma_2^{\delta_2})^{\gamma_1\gamma_3}(\gamma_3^{\gamma_1\gamma_3})(\gamma_4^{\gamma_1\gamma_3})(\zeta^{\delta_5})^{\gamma_1\gamma_3} \cdots (\alpha_n^{\epsilon_n})^{\gamma_1\gamma_3} \\ &= (\gamma_1\alpha_1\alpha_2)(\gamma_2^{\delta_2})(\gamma_3\alpha_1\alpha_2)(\gamma_4\zeta)(\zeta^{\delta_5}) \cdots \alpha_n^{\epsilon_n}. \end{aligned}$$

Since  $\alpha_1$  and  $\alpha_2$  commute with  $\gamma_2$ , we have

$$g^{\gamma_1\gamma_3} = \gamma_1\gamma_2^{\delta_2}(\alpha_1\alpha_2\gamma_3\alpha_1\alpha_2)(\gamma_4\zeta)(\zeta^{\delta_5}) \cdots \alpha_n^{\epsilon_n} = \gamma_1\gamma_2^{\delta_2}\gamma_3\gamma_4\zeta^{\delta_5} \cdots \alpha_n^{\epsilon_n}\zeta.$$

□

## 6.6 Proof Of Main Theorem

As suggested by the structure of the foregoing sections, the proof is by induction on  $n$ .

It is easy to verify on the computer that there are groups  $H_2$  (of order  $2^7$ ) and  $H_3$  (of order  $2^8$ ) behaving exactly as in the theorem statement. The combined results of Sections 6.2-6.5 show that if  $H_n$  (of order  $2^{n+5}$ ) behaves as in the theorem statement, then it has an immediate descendant (of order  $2^{n+6}$ ) isomorphic to  $H_{n+1}$ , and this group also behaves as in the theorem statement. The theorem now follows by induction. □

*Remark.*  $H_2$  and  $H_3$  are the groups identified as  $\langle 2^7, 1918 \rangle$  and  $\langle 2^8, 26740 \rangle$ , respectively, in the MAGMA small group library.

*Remark.* We proved that  $H_n$  has class  $n + 1$ ; in fact, the lower central series and 2-central series coincide for  $H_n$ . Therefore,  $H_n$  has nilpotency class  $n + 1$  and hence coclass 4.



# Chapter 7

## Conclusion

In this project we have successfully determined, for almost all  $n \leq 1,000$ , the NI-groups of order  $n$ , and discovered a new infinite family of NI-groups, all linked by a constant coclass. We reiterate that our data seems to suggest that NI-groups are much more “common” than one might have expected. From the orders completed, approximately 38% of all groups are NI-groups. Our main theorem introduces a new infinite family of NI-groups.

Eick and duSautoy [3, 4] have completed work on *coclass graphs* to help understand  $p$ -groups. Let  $\mathcal{G}(p, r)$  be a directed graph whose vertices are all  $p$ -groups (up to isomorphism) of coclass  $r$ . There is an edge from a group  $P$  to  $Q$  if and only if  $P/\gamma(P)$  is isomorphic to  $Q$ , where  $\gamma(P)$  is the last non-trivial term in the exponent-2 central series of  $P$ . Evidently, an edge exists from  $P$  to  $Q$  precisely when  $Q$  is a descendant of  $P$ . The structure of  $\mathcal{G}(p, r)$  is, in general, not well understood. It is known, however, that there are families of “infinitely capable” groups that lie on infinite chains in  $\mathcal{G}(p, r)$ . Each such family corresponds to a unique infinite pro- $p$ -group, and there are finitely many of these. The families are called “mainline families,” and their members are called “mainline groups”. Our main theorem describes a mainline family in the coclass graph  $\mathcal{G}(2, 4)$ . In particular, each mainline group in this family is an NI-group.

The uniqueness of this family seems extremely unlikely, and we expect that a thorough analysis of our data will lead to new infinite families of NI-groups. Indeed, we have already identified three other possible sources of infinite families. These, however, would also be examples of coclass 4; we would like to find families with other coclass values.

Of course, questions raised in Chapter 4 also lend themselves to future areas of study. In particular, we wish to discover more groups for which  $\text{Aut}_c(G) = \text{Aut}(G)$ . Recall that we have only found 5 examples in the data collected thus far. Further, we require improvements on the generation of automorphism groups in order to compute  $\text{Out}_c(G)$  for “larger” soluble groups  $G$  in order to complete Table 4.1.

## References

- [1] W. Burnside, *Theory of groups of finite order*, 2nd Ed. Dover Publications, Inc., 1955. Reprint of the 2nd edition (Cambridge, 1911).
- [2] W. Burnside, *On the outer automorphisms of a group*, Proc. London Math. Soc. (2) **11** (1913), 40–42.
- [3] M. du Sautoy, *Counting  $p$ -groups and nilpotent groups*, Publications Mathématiques. Institut de Hautes Études Scientifiques **92** (2001), 63–112.
- [4] B. Eick and C. R. Leedham-Green, *On the classification of prime-power groups by coclass*, The Bulletin of the London Mathematical Society **40** (2008), 274–288.
- [5] W. Feit and G. M. Seitz, *On finite rational groups and related topics*, Illinois J. Math., **33** (1988), 103–131.
- [6] P. Hall, *A contribution to the theory of groups of prime power order*, Proc. London Math. Soc. **36** (1934), 29–95.
- [7] M. Hertweck, *Contributions to the integral representation theory of groups*, (<http://elib.uni-stuttgart.de/opus/volltexte/2004/1638/>), 2004, Habilitationsschrift.
- [8] H. Heineken, *Nilpotente Gruppen, deren sämtliche Normalteiler charakteristisch*, Arch. Math. (Basel) **33** (1980), No. 6, 497–503.
- [9] D. F. Holt, B. Eick and E. A. O’Brien, *Handbook of Computational Group Theory*, Chapman and Hall, 2005.
- [10] C. R. Leedham-Green and M. F. Newman, *Space groups and groups of prime power order I*. Arch. Math. (Basel) **35** (1980), 193–202.

- [11] I. Malinowska, *On quasi-inner automorphisms of a finite  $p$ -group*, Publ. Math. Debrecen **41** (1992), No. 1-2, 73–77.
- [12] E.A. O'Brien, *The  $p$ -group generation algorithm*, J. Symbolic Comput. **9** (1990), 677–698.
- [13] T. Ono and H. Wada, *“Hasse principle” for free groups*, Proc. Japan Acad., **75** Ser. A (1999), 1–2.
- [14] T. Ono and H. Wada, *“Hasse principle” for symmetric and alternating groups*, Proc. Japan Acad., **75** Ser. A (1999), 61–62.
- [15] H. Wada, *“Hasse principle” for  $SL_n(D)$* , Proc. Japan Acad. **75** Ser. A (1999), 67–69.
- [16] H. Wada, *“Hasse principle” for  $GL_n(D)$* , Proc. Japan Acad. **76** Ser. A (2000), 44–46.
- [17] G.E. Wall, *Finite groups with class preserving outer automorphisms*, J. London Math. Soc. **22** (1947), 315–320.
- [18] M. Yadav, *Class preserving automorphisms of finite  $p$ -groups*, Proceedings of Groups–St. Andrews 2009, Vol. 2 (C.M. Campbell et al., eds), London Math. Soc. Lecture Note Series. Cambridge University Press, 2011.