ABSTRACT

Title of dissertation: ON THE GALOIS GROUPS OF THE 2-CLASS FIELD TOWERS OF SOME IMAGINARY QUADRATIC FIELDS

Aliza Steurer, Doctor of Philosophy, 2006

Dissertation directed by: Professor Lawrence Washington
Department of Mathematics

Let k be a number field, p a prime, and $k^{nr,p}$ the maximal unramified p-extension of k. Golod and Shafarevich focused the study of $k^{nr,p}/k$ on $Gal(k^{nr,p}/k)$. Let S be a set of primes of k (infinite or finite), and k_S the maximal p-extension of k unramified outside S. Nigel Boston and C.R. Leedham-Green introduced a method that computes a presentation for $Gal(k_S/k)$ in certain cases. Taking $S = \{(1)\}$, Michael Bush used this method to compute possibilities for $Gal(k^{nr,2}/k)$ for the imaginary quadratic fields $k = \mathbb{Q}(\sqrt{-2379}), \mathbb{Q}(\sqrt{-445}), \mathbb{Q}(\sqrt{-1015})$, and $\mathbb{Q}(\sqrt{-1595})$. In the case that $k = \mathbb{Q}(\sqrt{-2379})$, we illustrate a method that reduces the number of Bush's possibilities for $Gal(k^{nr,2}/k)$ from 8 to 4. In the last 3 cases, we are not able to use the method to isolate $Gal(k^{nr,2}/k)$. However, the results in the attempt reveal parallels between the possibilities for $Gal(k^{nr,2}/k)$ for each field. These patterns give rise to a class of group extensions that includes each of the 3 groups. We conjecture subgroup and quotient group properties of these extensions.

ON THE GALOIS GROUPS OF THE 2-CLASS FIELD TOWERS OF SOME IMAGINARY QUADRATIC FIELDS

by

Aliza Steurer

Dissertation submitted to the Faculty of the Graduate School of the
University of Maryland, College Park in partial fulfillment
of the requirements for the degree of
Doctor of Philosophy
2006

Advisory Committee:
Professor Lawrence Washington, Chair/Advisor
Professor William Adams
Professor Thomas Haines
Professor Don Perlis
Professor James Schafer

ACKNOWLEDGMENTS

I would especially like to thank my advisor, Larry Washington, for his thoughtful advice and helpful discussions. Also, I would like to thank Jim Schafer for his insight and helpful discussions. Also, I would also like to thank Bill Adams for his advice throughout my graduate career. Additionally, thank you to Don Perlis and Tom Haines for serving on my committee and making helpful suggestions.

I would like to thank my friends Corey Gonzalez, Angela Desai, Kate and Chris Truman, Tina Horvath, Dave Saranchak, Susan Schmoyer, Ben Howard, Andie Hodge, Chris Zorn, Eric Errthum, James Crispino, Pol Tangboondouangjit, Suzanne Sindi, and Sarah Brown.

Lastly, and most importantly, I would like to thank my family and friends Jessica Wescott, Jen Herrmann, Laura Lee and Shael Wolfson, Jasmine Yang, Sylvia Kaltreider, and J.T. Halbert.

TABLE OF CONTENTS

LIST OF FIGURES

Chapter 1

Introduction

A fundamental property of the integers is that any nonzero element different from ±1 can be factored uniquely (up to order and multiplication by -1) into a product of irreducibles. However, if k is a finite extension of $\mathbb{Q}$, the ring of algebraic integers in k need not have unique factorization. There is a naturally defined finite extension, H_1, of k called the Hilbert class field of k. A property of H_1 is that the degree of H_1 over k is equal to one (i.e. $H_1 = k$) if and only if the ring of algebraic integers in k is a unique factorization domain. That is, the degree of H_1 over k measures how much the ring of algebraic integers in k fails to have unique factorization.

One way to restore unique factorization is to embed k in a finite extension F whose ring of integers is principal ideal domain. To do this, we start with k and form H_1. We replace k by H_1 and form the Hilbert class field, H_2, of H_1. Continuing, we form the *Hilbert class field tower* of k,

$$k \subseteq H_1 \subseteq H_2 \ldots \subseteq H_n \subseteq \ldots.$$

This tower stops if and only if there is a finite extension F of k such that F has unique factorization. Let $k_\infty{:=}\cup_{i\geq 1} H_i$.

In 1964, Golod and Shafarevich gave a group theoretic condition necessary for k_∞ to be a finite extension of k [12]. Using this condition, they showed, for example, that $k = \mathbb{Q}(\sqrt{-2 \cdot 3 \cdot 5 \cdot 7 \cdot 9 \cdot 11})$ is such that k_∞/k is infinite.

It is standard to fix a prime p and look only at the *Hilbert p-class field tower* of k. This means that we take the largest subfield, k_i, of H_i that has degree a (possibly trivial) power of p over k. Again, this forms a tower of fields

$$k = k_0 \subseteq k_1 \subseteq k_2 \subseteq \ldots \subseteq k_n \subseteq \ldots$$

called the *Hilbert p-class field tower of k.*

Let $k^{nr,p}{:=}\cup_{i\geq 1} k_i$ ("nr" is French for "non ramifié"). Golod and Shafarevich actually gave a necessary condition on the Galois group $Gal(k^{nr,p}/k)$ for $k^{nr,p}/k$ to be finite. Their condition shows that the structure of $Gal(k^{nr,p}/k)$ is the most important object of study.

There is current interest in studying $Gal(k^{nr,2}/k)$. In 1996, Hajir [7] showed that if k is imaginary quadratic and its ideal class group has 4-rank 3 or greater, then k has an infinite 2-class field tower. More recently, Benjamin, Lemmermeyer, and Snyder [2] showed that $k^{nr,2} = k_2$ for certain k with $Gal(k^{nr,2}/k)$ of 2-rank 3. On the other hand, Gerth [6] gave conditions on $Gal(k^{nr,2}/k)$ for certain k which imply that $k^{nr,2}/k$ must be infinite.

Let S be a finite set of primes (finite or infinite) of k and let k_S/k denote the maximal 2-extension of k unramified outside S. Nigel Boston and C.R. Leedham-Green [4] introduced a general method that can compute presentations for $Gal(k_S/k)$ in certain cases. Because the presentations define finite groups, they are able to conclude that k_S/k is a finite extension. The method utilizes the fact that structure of the p-class groups of subfields of k_S can be obtained. This information corresponds to the abelianizations of subgroups of $Gal(k_S/k)$. The method then uses the p-group generation algorithm (to be discussed in detail in Section 2.1), which computes presentations for finite p-groups. The group $Gal(k_S/k)$ is searched for among the groups generated by the p-group generation algorithm.

Michael Bush [5] took $S = \{(1)\}$ and applied Boston and Leedham-Green's method to generate $Gal(k^{nr,2}/k)$ where k is one of the 4 imaginary quadratic fields $\mathbb{Q}(\sqrt{-2379})$, $\mathbb{Q}(\sqrt{-445})$, $\mathbb{Q}(\sqrt{-1015})$, and $\mathbb{Q}(\sqrt{-1595})$.

The field $k = \mathbb{Q}(\sqrt{-2379})$ has 2-class group $C_4 \times C_4$, and is the first such imaginary quadratic field. In light of Hajir's work mentioned above, Bush wondered whether $k^{nr,2}/k$ was finite. He showed that it is by generating presentations for 8 distinct groups of order 2^{11}, one of which must define $Gal(k^{nr,2}/k)$. This also enables him to conclude that k has a 2-class tower of length 2.

In the case where $k = \mathbb{Q}(\sqrt{-445})$, Bush generated 2 groups of order 2^8 as possibilities for $Gal(k^{nr,2}/k)$. This shows that k has a finite 2-class tower of length 3. Finally, for $k = \mathbb{Q}(\sqrt{-1015})$ and $k = \mathbb{Q}(\sqrt{-1595})$, he generates 2 groups which are possibilities for $Gal(k^{nr,2}/k)$ in each case. This shows that each field has a finite 2-class tower of length 3. The above 3 fields are the first known examples of imaginary quadratics with 2-class towers of length 3. However, his method could not determine the Galois group in any the above examples.

This dissertation studies Bush's possibilities for $Gal(k^{nr,2}/k)$ in each of his examples. We attempt to isolate the Galois group among the possibilities in each example. Also, we investigate the Galois groups of 2-class field towers. To study properties of these groups, we use the software package MAGMA [3]. To generate number theoretic information, we use the number theory package PARI [1].

Chapter 2 provides an explanation of basic results. Chapter 3 pertains to $k = \mathbb{Q}(\sqrt{-2379})$, which we refer to as Example One. We illustrate a method which explicitly identifies $Gal(k^{nr,2}/k)$ as one of 4 of the original 8 possibilities. We explain how this method should eventually isolate $Gal(k^{nr,2}/k)$ among the remaining 4 possibilities. However, current software cannot perform the computations we see necessary to show which possibility is actually $Gal(k^{nr,2}/k)$.

In Chapter 4, we attempt to apply Example One's method to $k = \mathbb{Q}(\sqrt{-445})$ (referred to as Example Two) to identify $Gal(k^{nr,2}/k)$ among the 2 possibilities. Unfortunately, the method does not isolate $Gal(k^{nr,2}/k)$. However, the results obtained during the attempt bear similarities to $\mathbb{Q}(\sqrt{-1015})$ and $\mathbb{Q}(\sqrt{-1595})$. Additionally, we highlight other distinctions between the two possibilities for $Gal(k^{nr,2}/k)$.

In Chapter 5, we attempt to apply Example One's method to each of $k = \mathbb{Q}(\sqrt{-1015})$ and $k = \mathbb{Q}(\sqrt{-1595})$ (the attempt for each is described in Example Three). Again, we are unsuccessful in isolating $Gal(k^{nr,2}/k)$ in either case. Using the results obtained in the attempt, we observe parallels between the possibilities in Examples Two and Three. We use these patterns to describe a class of group extensions by certain subgroup and quotient group properties. In doing so, we show that the two possibilities for $Gal(k^{nr,2}/k)$ have isomorphic subgroup lattices such that corresponding proper subgroups and quotients are isomorphic.

Chapter 2

Background

In this chapter, we discuss background material used in Chapters 3, 4, and 5.

2.1 The p-group generation algorithm

Let G be a finite p-group. The p-group generation algorithm computes a presentation for a certain extension (to be defined below) of G. For proofs and details of what follows, see [9] and also [10]. If $H \leq G$, then $[H, G]$ denotes the subgroup generated by the commutators $h^{-1}g^{-1}hg$ where $h \in H, g \in G$.

Definition 1. *Define $P_0(G)$ to be G. For each integer $i \geq 1$, define*

$$P_i(G) = [P_{i-1}(G), G]P_{i-1}(G)^p.$$

By induction, $P_i(G)$ is a characteristic subgroup of G for all $i \geq 0$. It follows that $P_{i-1}(G) \geq P_i(G)$ for $i = 0, 1, \ldots$. The series

$$G = P_0(G) \geq P_1(G) \geq \ldots \geq P_{i-1}(G) \geq P_i(G) \geq \ldots$$

is the *lower exponent-p central series* of G. If $P_c(G) = 1$ and c is the smallest such integer, then G has *exponent p-class c*. Consider $D_4 =< r, s | r^4, s^2, rsrs^{-1} >$, the dihedral group of order 8. Then D_4 has exponent-2 class 2: $P_1(D_4) =< r^2 >$ and $P_2(D_4) =< 1 >$.

Two properties of the p-central series are:

1. If ϕ is a homomorphism, then $\phi(P_i(G))$=$P_i(\phi(G))$ for all $i \geq 0$.
2. If $N \lhd G$ and G/N has exponent p-class c, then $P_c(G) \leq N$.

Property 1 follows by induction. Property 2 follows from Property 1. Let $\Phi(G)$ be the Frattini subgroup of G. We have:

Proposition 1. *If G is a finite p-group, then $P_1(G) = \Phi(G)$.*

Proof: If M is a maximal subgroup of G, we have by basic p-group theory that $G/M \cong C_p$. It follows that $P_1(G) \leq M$. Conversely, it is easy to see that $G/P_1(G)$ is elementary abelian. Suppose that $G/P_1(G)$ has dimension n with $\mathbb{F}_p$-basis $v_1, \ldots, v_n$. Consider the subspaces $< v_2, \ldots, v_n >, < v_1, v_3, \ldots, v_n >, \ldots, < v_1, \ldots, v_{n-1} >$. Suppose $x = a_1v_1 + \ldots + a_nv_n$. Then $x \in< v_2, \ldots, v_n >$ implies $a_1 = 0$. Next, $x \in< v_1, v_3, \ldots, v_n >$ implies $a_2 = 0$, etc. Let $\cap(M/P_1(G))$ be the intersection of all maximal subgroups of $G/P_1(G)$ (i.e. the intersection of all subspaces of codimension 1). Then, $\cap(M/P_1(G)) =< P_1(G) >$ and $\Phi(G)/P_1(G) \leq \cap(M/P_1(G))$ imply that $\Phi(G) \leq P_1(G)$. ■

Suppose G has exponent-p class c. By Property 1, we see that $G/P_i(G)$ has exponent-p class i for $1 \leq i \leq c$. Property 2 shows that $G/P_i(G)$ is the maximal exponent-p-class i quotient of G for $1 \leq i \leq c$. By Proposition 1, the minimal number of generators for G is given by the p-rank of $G/\Phi(G) = G/P_1(G)$. Throughout, we refer to this number as the *Frattini-quotient rank* of G.

Definition 2. *The group H is a **descendant** of G if $H/P_c(H) \cong G$.*

As an example, consider D_4. By the above, $c = 2$ and $D_4/P_2(D_4) \cong C_2 \times C_2$, the group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Thus, D_4 is an immediate descendant of $C_2 \times C_2$.

Definition 3. *The group H is an* ***immediate descendant*** *of G if H is a descendant of G and H has exponent-p class $c+1$.*

Above, we saw that D_4 is an immediate descendant of $C_2 \times C_2$.

Definition 4. *Suppose d is the Frattini-quotient rank of G and $G \cong F/R$, where F is the free group on d generators. Let $R^* = [F,R]R^p$, the subgroup of R generated by the set of commutators $[F,R]$ and pth powers of elements of R. The* ***p-covering group*** *of G is F/R^* and is denoted by G^*. The* ***p-multiplicator*** *of G is R/R^*. The* ***nucleus*** *of G is $P_c(G^*)$.*

It can be shown that G^* is independent of the choice of R. Also, note that $G^*/(R/R^*) \cong G$. It follows that G^* is finite. This is because R/R^* is finitely generated abelian and of exponent p, and G is finite. Also, Property 1 implies that $P_c(G^*) \leq R/R^*$.

Definition 5. *A subgroup $M/R^* < R/R^*$ is an* ***allowable subgroup*** *if it is a proper subgroup that supplements the nucleus.*

A subgroup $M/R^* < R/R^*$ supplements the nucleus if $(M/R^*)P_c(G^*) = R/R^*$. Let H be an immediate descendant of G. It can be shown that there is an allowable subgroup M/R^* such that $G^*/(M/R^*) \cong H$. Note that since R/R^* is finite, G can have only finitely many immediate descendants.

By Property 1, G^* has exponent-p class at least c. Since G^* surjects onto H and H has exponent-p class $c+1$, it follows that G^* has exponent-p class at most

$c+1$. We see that G has no immediate descendants whenever its nucleus is trivial. Such a group is called *terminal.* MAGMA shows that the quaternion group Q_8 has no immediate descendants, for example.

One question is: is there a unique allowable subgroup M/R^* such that we have $G^*/(M/R^*) \cong H$? The answer is: not necessarily. It can be shown that there are 3 distinct allowable subgroups of $(C_2 \times C_2)^*$ whose quotients are D_4. It is easy to see that $C_2 \times C_4$ is an immediate descendant of $C_2 \times C_2$. There is a unique allowable subgroup whose quotient is $C_2 \times C_4$. The algorithm selects allowable subgroups in such a way as to provide an irredundant list of immediate descendants. For more details, see [10].

For $i \geq c-1$, it is easy to see that the group $G/P_{i+1}(G)$ is an immediate descendant of $G/P_i(G)$ by Property 1. The p-group generation algorithm takes a finite p-group G and gives a method that computes the presentations of all immediate descendants of G. By starting with $G/P_1(G)$, the p-group generation algorithm can compute a presentation for $G/P_2(G)$. Applying the algorithm to $G/P_2(G)$ computes a presentation for $G/P_3(G)$, etc. After c iterations of the algorithm, one obtains a presentation for $G/P_c(G) \cong G$.

2.2 The standard presentation of a finite p-group

Newman [9] gives an outline of the p-group generation algorithm. In this outline, he shows that the presentation of G given by the algorithm is unique. We call this presentation the *standard presentation* of G. Therefore, whenever the standard presentations of the finite p-groups G and H (i.e. the presentations of G and H computed by the p-group generation algorithm) are different, then $G \ncong H$. We state this as a proposition for later use.

Proposition 2. *Two finite p-groups are isomorphic if and only if they have the same standard presentations.*

Proof: See [9]. ■

If G is a finite p-group of order p^n, then the standard presentation of G is given as the quotient of the free group $F(n)$ on n generators $x_1, \ldots, x_n$. The relations are words in pth powers and commutators of $x_1, \ldots, x_n$. Whenever a pth power or commutator is trivial, we omit it from the set of relations. As we will see in Section 2.2.1, the standard presentation of D_4 is

$$< x_1, x_2, x_3 | [x_2, x_1] = x_3 > .$$

For example, this indicates that x_1, x_2, and x_3 have order 2 and that $[x_3, x_1] = 1$. The standard presentation for Q_8 is

$$< x_1, x_2, x_3 | x_1^2 = x_3, x_2^2 = x_3, [x_2, x_1] = x_3 > .$$

This shows that x_1 and x_2 have order 4, x_3 has order 2, and $[x_3, x_2] = 1$.

2.2.1 Example: Generation of D_4 using the p-group generation algorithm.

As described in Section 2.1, we begin with a presentation of $D_4/P_1(D_4) \cong C_2 \times C_2$:

$$< x_1, x_2 \mid x_1^2 = 1, x_2^2 = 1, [x_1, x_2] = 1 > .$$

We apply the p-group generation algorithm to obtain D_4 as a quotient of $K = (C_2 \times C_2)^*$ by an allowable subgroup. First, the 2-multiplicator of $C_2 \times C_2$ is

$$R/R^2[R, F] = R/R^* =< x_1^2 R^*, x_2^2 R^*, [x_1, x_2]R^* > .$$

We refer to R/R^* later. MAGMA shows that K is defined by:

$$< x_1, x_2, x_3, x_4, x_5 \mid x_1^2 = x_3, x_2^2 = x_4, [x_2, x_1] = x_5 > .$$

As in Section 2.2, whenever the 2nd powers or commutators of x_1, x_2, x_3, x_4, x_5 are trivial, we omit them (e.g. $x_3^2 = 1$ and $[x_3, x_1] = 1$).

Recall that an allowable subgroup M/R^* is a proper subgroup of R/R^* that supplements the nucleus. MAGMA shows that $P_2(K) = R/R^*$, so any proper subgroup of R/R^* is an allowable subgroup. Let $M_1/R^* =< x_1^2 R^*, x_2^2 R^* >$ so that $K/(M_1/R^*)$ is given by

$$< \bar{x_1}, \bar{x_2}, \bar{x_5} | \bar{x_1}^2 = 1, \bar{x_2}^2 = 1, [\bar{x_2}, \bar{x_1}] = \bar{x_5} >$$

Consider $\overline{x_1 x_2}$ and $\bar{x_2}$. These generate $K/(M_1/R^*)$ and are such that $(\overline{x_1 x_2})^4 = 1$ and $(\overline{x_1 x_2})\bar{x_2}(\overline{x_1 x_2})\bar{x_2}^{-1} = 1$. Hence, $K/(M_1/R^*)$ is D_4. Recall that we can omit the first two relations from the presentation of $K/(M_1/R^*)$. This gives the standard presentation of D_4 from Section 2.2.

Additionally, let

$$M_2/R^* =< x_1^2[x_2, x_1]R^*, x_2^2[x_2, x_1]R^* >$$

Then, $K/(M_2/R^*)$ is Q_8. Let

$$M_3/R^* =< x_1^2R^*, [x_2, x_1]R^* > .$$

The group $K/(M_3/R^*)$ defines $C_2 \times C_4$. Lastly, let $M_4/R^* =< [x_2, x_1]R^* >$. It is easy to see that $C_4 \times C_4$ is an immediate descendant of $C_2 \times C_2$. The group

$$K/(M_4/R^*)$$

defines $C_4 \times C_4$.

We will see in Section 2.3 that $C_2 \times C_2$ has 7 immediate descendants. The other 3 are K and 2 groups H_3 and H_4 of order 16 given by:

$$H_3 =< x_1, x_2, x_3, x_4 | x_1^2 = x_4, [x_2, x_1] = x_2x_3 >,$$

$$H_4 =< x_1, x_2, x_3, x_4 | y_1^2 = y_4, y_2^2 = y_3, [y_2, y_1] = y_2y_3 > .$$

2.3 Bush's results

In this section, we describe the details and results of Bush's method presented in [5]. He considers the 2-class towers of each of the imaginary quadratic fields $\mathbb{Q}(\sqrt{-2379})$, $\mathbb{Q}(\sqrt{-445})$, $\mathbb{Q}(\sqrt{-1015})$, and $\mathbb{Q}(\sqrt{-1595})$. Let k denote one of these fields and $G = Gal(k^{nr,2}/k)$. He uses the p-group generation algorithm to compute $G/P_i(G)$ for $i \geq 1$. As the algorithm produces a large number of possibilities for $G/P_i(G)$, he establishes criteria that subgroups of a possibility must fulfill.

Note that G is a profinite 2-group and that $G/P_i(G)$ is a finite 2-group for all $i \geq 1$. This means that for each $i \geq 1$ a presentation for $G/P_i(G)$ can be computed using the p-group generation algorithm.

Let $G_1, G_2, \ldots, G_n$ denote a collection of closed subgroups of G such that for all j, we have $G_j \geq P_i(G)$ for all i greater than some i_0. Let $\bar{G}_j$ denote the image of G_j in $G/P_i(G), i \geq i_0$. At the ith iteration of the p-group generation algorithm, the goal is to find a group Q such that $Q \cong G/P_i(G)$. Suppose $(Q, \{Q_j\}_{j=1}^n)$ is an ordered pair such that $Q_1, \ldots, Q_n$ are subgroups of Q. Additionally, suppose there exists an isomorphism $\psi_i : Q \to G/P_i(G)$ such that $\psi_i(Q_j) = \bar{G}_j$ for each $j = 1, \ldots, n$. Such a group is called a *representative* of the pair $(G/P_i(G), \{\bar{G}_j\}_{j=1}^n)$. Suppose $(R, \{R_j\}_{j=1}^n)$ and $(Q, \{Q_j\}_{j=1}^n)$ are representatives for $G/P_i(G)$ and $G/P_{i-1}(G)$, respectively. Property 1 of the p-group generation algorithm, shows that ψ_i induces an isomorphism $R/P_{i-1}(R) \to G/P_{i-1}(G)$. Additionally, R has 2-class i. Therefore, R is an immediate descendant of Q. Let $\pi : G/P_i(G) \to G/P_{i-1}(G)$ be given by $gP_i(G) \mapsto gP_{i-1}(G)$. The composition $f = \psi_{i-1}^{-1} \circ \pi \circ \psi_i$ is an epimorphism such that $f(R_j) = P_j$ for all $i = 1, \ldots, n$.

What is the significance of the subgroups $\bar{G}_1, \ldots, \bar{G}_n$? In each case, the discriminant of the imaginary quadratic is the product $-p_1 \cdot p_2 \cdot p_3$, where p_1, p_2, p_3 are distinct positive primes. For example, $-1015 = -7 \cdot 5 \cdot 29$. By genus theory, the 2-class group $Cl_k^{(2)}$ of k (the 2-Sylow subgroup of the class group Cl_k of k) has Frattini-quotient rank 2 (i.e. has 2-rank 2). It follows from Class Field Theory that G has Frattini-quotient rank 2. By the remarks made in Section 2.1, we see that G is a descendant of $C_2 \times C_2$. Basic p-group theory shows that $k^{nr,2}/k$ contains exactly

3 quadratic extensions

$$L_2 = k(\sqrt{-p_1}), L_3 = k(\sqrt{p_2}), L_4 = k(\sqrt{p_3}).$$

Let $G_1 = G$ and $G_j = Gal(k^{nr,2}/L_j)$, so that $[G : G_j] = 2$ for $j = 2, 3, 4$. Since $G/P_1(G)$ is the largest quotient of G having exponent-2 class one, $P_1(G) \leq G_2, G_3, G_4$. It follows that $P_i(G) \leq G_j$ for $i \geq 1$. The field $L_5 = k(\sqrt{-p_1}, \sqrt{p_2}, \sqrt{p_3})$ is a subfield of $k^{nr,2}/k$. Let $G_5 = Gal(k^{nr,2}/L_5)$. Since $G/G_5 \cong C_2 \times C_2$, it follows that $P_1(G) = G_5$ and $P_i(G) \leq G_5$ for all $i \geq 1$. Let K denote the fixed field of $P_2(G)$. Using the number theory package KASH, Bush finds a generating polynomial for a subfield L_8 of degree 8 over k such that

$$\mathbb{Q}(\sqrt{-p1}, \sqrt{p_2}, \sqrt{p_3}) \subset L_8 \subset K.$$

The lattice of subfields of the extension L_8/k shows that $Gal(L_8/k)$ is a group having exponent-2 class 2. Therefore, $P_2 \leq Gal(k^{nr,2}/L_8)$. This implies that $P_i \leq Gal(k^{nr,2}/L_8)$ for $i \geq 2$. The field L_8 contains two fields L_6 and L_7 of degree 4 over k. Let G_6 and G_7 denote the subgroups of G fixing these subfields. Then $P_i(G) \leq G_6, G_7$ for $i \geq 2$.

Let $i \geq 2$. Fix $j \in \{1, \ldots, 7\}$. By the remarks above, we may let $\bar{G}_j$ denote the image of G_j in $G/P_i(G)$. The abelianization $G_j/[G_j, G_j]$ surjects onto $\bar{G}_j/[\bar{G}_j, \bar{G}_j]$. By Proposition 1 in Chapter 3, $G_j/[G_j, G_j] \cong Cl^2_{L_j}$ for $j \geq 2$ and $G_1/[G_1, G_1] \cong Cl^2_k$. Hence, the abelianization of the image of G_j in $G/P_i(G)$ is a quotient of $Cl^2_{L_j}$. Let $(R, \{R_j\}_{j=1}^7)$ be a representative for $G/P_i(G)$. Recall from above that there is an isomorphism $\psi_i : R \rightarrow G/P_i(G)$ such that $\psi_i(R_j) = \bar{G}_j$ for $j = 1, \ldots, 7$. In particular, $R/[R, R]$ is a quotient of $G/[G, G]$. The group R must contain maximal subgroups R_2, R_3, R_4 whose abelianizations are quotients of $Cl^2_{L_2}$, $Cl^2_{L_3}$, and $Cl^2_{L_4}$, respectively. Lastly, R must have 3 index 4 subgroups R_5, R_6, R_7 whose abelianizations are quotients of $Cl^2_{L_5}$, $Cl^2_{L_6}$, and $Cl^2_{L_7}$.

Given a list $\mathcal{L}_{(i-1)}$ containing a representative of $(G/P_{i-1}(G), \{\bar{G}_j\}_{j=1}^7)$, Bush composes a list $\mathcal{L}_{(i)}$ of pairs containing a representative $(R, \{R_j\}_{j=1}^7)$ of the pair $(G/P_i(G), \{\bar{G}_j\}_{j=1}^7)$ as follows. Recall that there exists an isomorphism $\psi_i : R \to G/P_i(G)$ such that $\psi_i(R_j) = \bar{G}_j$ for all $j = 1, \ldots, 7$. Let $(Q, \{Q_j\}_{j=1}^7)$ be a pair on $\mathcal{L}_{(i-1)}$ (so that $(Q, \{Q_j\}_{j=1}^7)$ is a potential representative of $(G/P_{i-1}(G), \{\bar{G}_j\}_{j=1}^7)$). In Section 2.1 above, we showed that Q has finitely many immediate descendants $R_1, \ldots, R_{l_Q}$. Let $l_0 \in \{1, \ldots, 7\}$ be such that $R_{l_0} \cong G/P_i(G)$. Fix a $k \in \{1, \ldots, l_Q\}$ and an epimorphism $f : R_k \to Q$. If for each $j = 1, \ldots, 7$ the abelianization of $f^{-1}(Q_j)$ is a quotient of $G_j/[G_j, G_j]$, then the pair $(R_k, \{f^{-1}(Q_j)\}_{j=1}^7$ gets added to $\mathcal{L}_{(i)}$. This way, $\mathcal{L}_{(i)}$ will contain a representative of $(G/P_i(G), \{\bar{G}_j\}_{j=1}^7)$.

Suppose m is the smallest such integer such that $\mathcal{L}_{(m)}$ is empty. In this case, $\mathcal{L}_{(i)}$ is empty for all $i \geq m$. The lists $L_{(i)}, 1 \leq i \leq m$ form a finite collection of finite groups containing G. In particular, G must be finite. A group R is called a *candidate* for G is there exists a pair $(R, \{R_j\}_{j=1}^7)$ such that $R_j/[R_j, R_j] \cong G_j/[G_j, G_j]$ for all $j = 1, \ldots, 7$. Hence, G will be among the candidates contained on the lists.

2.3.1 Example of Bush's computations: $k = \mathbb{Q}(\sqrt{-445})$

The field k has class group $C_2 \times C_4$. The quadratic extensions of k are

$$L_2 = k(\sqrt{-1}), L_3 = k(\sqrt{5}), L_4 = k(\sqrt{89}).$$

The field $L_5 = \mathbb{Q}(\sqrt{-1}, \sqrt{5}, \sqrt{89})$ is a subfield of $k^{nr,2}$ such that $Gal(L_5/k) \cong C_2 \times C_2$. Bush computes the 2-class groups of these fields using KASH:

$$G_1/[G_1, G_1] \cong Cl_{L_1} \cong Cl_k \cong C_2 \times C_4$$

$$G_2/[G_2, G_2] \cong Cl_{L_2} \cong C_2 \times C_8$$

$$G_3/[G_3, G_3] \cong Cl_{L_3} \cong C_4 \times C_4 \times C_8$$

$$G_4/[G_4, G_4] \cong Cl_{L_4} \cong C_2 \times C_2 \times C_2$$

$$G_5/[G_5, G_5] \cong Cl_{L_5} \cong C_4 \times C_4.$$

Since $G/[G, G] \cong C_2 \times C_4$, we see that $G/P_1(G) \cong C_2 \times C_2$. Moreover, $Gal(L_5/k) = P_1(G)$. A representative of $(G/P_1(G), \{\bar{G}_j\}_{j=1}^5)$ is $(C_2 \times C_2, \{R_j\}_{j=1}^5)$ where $R_1 = C_2 \times C_2$, and R_2, R_3, R_4 are the three subgroups of order 2, and $R_5 =< 0 >$. Let $\mathcal{L}_{(1)}$ consist of this single pair.

Recall from Section 2.2.1 that the group $C_2 \times C_2$ has 7 immediate descendants. They are the groups:

$C_2 \times C_4, \quad D_4, \quad Q_8, \quad C_4 \times C_4,$

$H_3 =< x_1, x_2, x_3, x_4 | x_1^2 = x_4, [x_2, x_1] = x_2x_3 >,$

$H_4 =< x_1, x_2, x_3, x_4 | y_1^2 = y_4, y_2^2 = y_3, [y_2, y_1] = y_2y_3 >,$

$K = (C_2 \times C_2)^*.$

MAGMA computes that $K/[K, K] \cong C_4 \times C_4$. Since $C_4 \times C_4$ is not a quotient of $C_2 \times C_4$, this implies that K does not appear in a pair on $\mathcal{L}_{(2)}$. Similarly, $C_4 \times C_4$ does not appear in a pair on $\mathcal{L}_{(2)}$.

Next, we consider H_4. Computations show that each index 2 subgroup of H_4 has the abelianization $C_2 \times C_4$. Since $C_2 \times C_4$ is not a quotient of $C_2 \times C_2 \times C_2 \cong Cl_{L_4}$, we cannot have H_4 appear in a pair on $\mathcal{L}_{(2)}$.

The group Q_8 is terminal (i.e. has no immediate descendants). Hence, in order for $G/P_2(G) \cong Q_8$, it would have to be that $G/P_2(G) \cong G$. Since, $Q_8/[Q_8, Q_8] \cong C_2 \times C_2$, this cannot occur.

Now consider D_4 and $C_2 \times C_4$. Bush finds subfields F_1 and F_2 of $k^{nr,2}/k$ such that $Gal(F_1/k) \cong C_2 \times C_4$ and $Gal(F_2/k) \cong D_4$. Both groups have exponent-2 class 2. By the second property of the lower p-central series, $G/P_2(G)$ surjects onto any quotient of G having exponent-2 class 2. Therefore, $G/P_2(G)$ can be neither $C_2 \times C_4$ nor D_4. Hence, $G/P_2(G)$ must be H_3.

Let $f : H_3 \to C_2 \times C_2$ be a surjection. The group H_3 is such that $H_3/[H_3, H_3] \cong C_2 \times C_4$. It has three maximal subgroups M_1, M_2, M_3 such that $M_1/[M_1, M_1] \cong M_2/[M_2, M_2] \cong C_2 \times C_4$ and $M_3/[M_3, M_3] \cong C_2 \times C_2$. Computations show that any normal index 4 subgroups has abelianization $C_2 \times C_2$. Therefore, if f is a surjection such that $f^{-1}(R_j) = M_j$, the pair $(H_3, \{f^{-1}(R_j)\})$ is appended to $\mathcal{L}_2$. Since H_3 is an immediate descendant of $C_2 \times C_2$, we have that $H_3/P_1(H_3) \cong C_2 \times C_2$. The map f with kernel $P_1(H_3)$ is surjection satisfying the necessary requirements. Bush iterates his method and the sequence of lists terminates to give 81 candidates for G.

To further isolate G, Bush incorporates two more subgroups G_6 and G_7 defined below. He begins by computing an unramified degree 8 extension L_8 over k with generating polynomial over $\mathbb{Q}$ given by

$$x^{16} + 12x^{14} + 4554x^{12} + 17928x^{10} + 2231251x^8 +$$
$$13625880x^6 - 10866150x^4 - 143437500x^2 + 244140625.$$

such that $Gal(L_8/k) \cong C_2 \times C_4$. The remarks above imply $P_i \leq Gal(k^{nr,2}/L_8)$ for all $i \geq 2$. Bush shows that the fields $L_6 = k(\sqrt{-\mu})$ and $L_7 = k(\sqrt{\mu})$ are subfields of L_8/k, where $\mu = -3 + 4\sqrt{-5}$. Hence, $P_i(G) \leq G_6, G_7$ for all $i \geq 2$. Computations show that $Cl_{L_6} \cong C_2 \times C_2 \times C_4$ and $Cl_{L_7} \cong C_4 \times C_4$

Next, Bush computes all surjections $f : H_3 \rightarrow C_2 \times C_4$ (instead of all surjections $H_3 \rightarrow C_2 \times C_2$), and adjoins pairs accordingly. This gives him $\mathcal{L}_2$. Reiterating this procedure, he finds that $\mathcal{L}_6$ is empty. Computations in MAGMA show that the groups in $\mathcal{L}_5$ are terminal. Among the collection of groups on $\mathcal{L}_1, \ldots, \mathcal{L}_5$, there are 12 candidates, each having exponent-2 class 5. Therefore, G must be one of these 12 groups. In particular, $G \cong G/P_5(G)$, and has exponent-2 class 5.

He finds that exactly 2 of the 12 groups have index 4 subgroups with abelianizations $C_2 \times C_{16}$. We denote the two groups by $C_{2,1}$ and $C_{2,2}$. Bush's computations indicate that the field $k(\sqrt{13 + 4\sqrt{5}})$ is a subfield of $k^{nr,2}/k$ with 2-class group $C_2 \times C_{16}$. As we will show later, $C_{2,1}$ and $C_{2,2}$ have different standard presentations, so that they are not isomorphic.

Similar considerations apply to each of the fields $\mathbb{Q}(\sqrt{-2379})$, $\mathbb{Q}(\sqrt{-1015})$ and $\mathbb{Q}(\sqrt{-1595})$. The main results of Bush's method are summarized in the following theorems.

Theorem 1. *The field $k = \mathbb{Q}(\sqrt{-445})$ has finite 2-class tower of length 3, i.e. $k = k_0 \subset k_1 \subset k_2 \subset k_3 = k^{nr,2}$. We have $Gal(k_1/k_0) \cong C_2 \times C_4$, $Gal(k_2/k_1) \cong C_2 \times C_2 \times C_4$, and $Gal(k_3/k_2) \cong \mathbb{Z}/2\mathbb{Z}$.*

The two candidates are quotients of the free group, $F(8)$, on 8 generators,

$x_1, x_2, \ldots x_8$. With $r \in \{0, 1\}$, they are defined by $F(8)/R_r$, where R_r is the normal subgroup generated by the set

$$\begin{array}{ll} x_1^2 x_4^{-1}, & [x_2, x_1] x_3^{-1} \\ x_2^2 (x_5 x_7)^{-1}, & [x_3, x_1] x_5^{-1} \\ x_3^2 (x_6 x_7)^{-1}, & [x_3, x_2] x_6^{-1} \\ x_6^2 x_8^{-1}, & [x_4, x_2](x_5 x_6 x_7 x_8)^{-1} \\ x_4^2 (x_8^r)^{-1}, & [x_4, x_3] x_7^{-1} \\ [x_5, x_1] x_7^{-1}, & [x_5, x_4] x_8^{-1} \\ [x_5, x_2] x_8^{-1}, & [x_7, x_1] x_8^{-1} \\ [x_5, x_3] x_8^{-1}, & [x_7, x_2] x_8^{-1}. \end{array}$$

Proceeding with $k = \mathbb{Q}(\sqrt{-2379})$ as in the above example, Bush obtains 8 candidates for $Gal(k^{nr,2}/k)$. He does not further isolate $Gal(k^{nr,2}/k)$ among these groups.

Theorem 2. *The field* $k = \mathbb{Q}(\sqrt{-2379})$ *has finite 2-class tower of length 2, i.e.* $k = k_0 \subset k_1 \subset k_2 = k^{nr,2}$*. We have* $Gal(k_1/k_0) \cong C_4 \times C_4$ *and* $Gal(k_2/k_1) \cong C_2 \times C_4 \times C_{16}$.

Each candidate is the quotient of the free group $F(9)$ on 9 generators. The sets of relations defining each candidate are the same except for two elements. We give one set of relations below. The variables $r, s, t \in \{0, 1\}$ denote the exponents below. Let $C_{1,rst}$ denote the candidate with exponents r, s, t. The group $C_{1,rst}$ is defined by $F(9)/R_{rst}$ where R_{rst} is the normal subgroup generated by the relations

$$\begin{array}{ll}
x_1^2x_4^{-1}, & [x_2,x_1]x_3^{-1} \\
x_2^2x_5^{-1}, & [x_3,x_1]x_6^{-1} \\
x_3^2(x_6x_8x_9x_{10})^{-1}, & [x_3,x_2]x_7^{-1} \\
x_4^2(x_7x_{11}^r)^{-1}, & [x_4,x_2]x_8^{-1} \\
x_5^2(x_6x_9x_{10}^sx_{11}^t)^{-1}, & [x_4,x_3]x_{10}^{-1} \\
x_6^2(x_9x_{10}x_{11})^{-1}, & [x_5,x_1](x_6x_7x_8x_9x_{10})^{-1} \\
x_7^2(x_{10}x_{11})^{-1}, & [x_5,x_3](x_{10}x_{11})^{-1} \\
x_9^2x_{11}^{-1}, & [x_6,x_1]x_9^{-1} \\
[x_5,x_4](x_{10}x_{11})^{-1}, & [x_8,x_2](x_{10}x_{11})^{-1} \\
[x_8,x_1]x_{10}^{-1}, & [x_9,x_1]x_{11}^{-1}.
\end{array}$$

Bush refines his method with $k = \mathbb{Q}(\sqrt{-1015})$. He computes 3 degree 8 subextensions $L_{8,1}, L_{8,2}$, and $L_{8,3}$ of $k^{nr,2}/k$. Fixing $r \in \{1,2,3\}$, he proceeds with $L_{8,r}$ as he did in the above example with L_8. This gives him 3 sets of subgroups. He applies his procedure using all 3 sets and obtains two candidates for $Gal(k^{nr,2}/k)$. Bush finds that $k = \mathbb{Q}(\sqrt{-1595})$ has 3 degree 8 subextensions with subfield lattices and corresponding 2-class groups identical to the ones considered for $k = \mathbb{Q}(\sqrt{-1015})$. Therefore, $Gal(k^{nr,2}/k)$ must be one of the two candidates above. He does not further isolate the Galois group in either case.

Theorem 3. *The fields $k = \mathbb{Q}(\sqrt{-1015})$ and $k = \mathbb{Q}(\sqrt{-1595})$ have finite 2-class towers of length 3, i.e. $k = k_0 \subset k_1 \subset k_2 \subset k_3 = k^{nr,2}$. In both cases, we have $Gal(k_1/k_0) \cong C_2 \times C_8$, $Gal(k_2/k_1) \cong C_2 \times C_2 \times C_4$, and $Gal(k_3/k_2) \cong C_2$.*

The candidates for each field are quotients of the free group, $F(9)$ on 9 generators. Let $r \in \{0, 1\}$. Each candidate is defined by $F(9)/R_r$ where R_r is the normal subgroup generated by the words

$$\begin{array}{ll}
x_1^2x_4^{-1}, & [x_2, x_1]x_3^{-1} \\
x_2^2(x_5x_7)^{-1}, & [x_3, x_1]x_5^{-1} \\
x_3^2(x_7x_8)^{-1}x_9^{r-1}, & [x_3, x_2]x_6^{-1} \\
x_4^2x_6^{-1}, & [x_4, x_2]x_8^{-1}x_9^{r-1} \\
x_6^2x_8^{-1}, & [x_4, x_2](x_5x_7x_8x_9^r)^{-1} \\
x_8^2x_9^{-1}, & [x_4, x_3]x_7^{-1} \\
[x_5, x_1]x_7^{-1} & [x_5, x_4]x_9^{-1} \\
[x_5, x_2]x_9^{-1} & [x_7, x_1]x_9^{-1} \\
[x_5, x_3]x_9^{-1} & [x_7, x_2]x_9^{-1}.
\end{array}$$

2.4 Partially ordered sets and lattices

We briefly recall some elementary facts about partially ordered sets and lattices. For more details, see [8].

Definition 6 (Lattice). *Let P be a partially ordered set (poset) with partial ordering $\leq$. Let $x, y \in P$ and*

$$\{x, y\}^u = \{w \in P | x \leq w, y \leq w\}.$$

*If there is some $w \in \{x, y\}^u$ such that $w \leq z$ for all $z \in \{x, y\}^u$, then w is called a **supremum** of x and y, denoted by $x \vee y = w$. An **infimum** of x and y is defined similarly, and is denoted by $x \wedge y$. We say that P is a **lattice** if $x \vee y$ and $x \wedge y$*

exist for all $x, y \in P$.

It follows from the definitions that $x \vee y$ and $x \wedge y$ are unique. As an example of a lattice, consider the set of subgroups of a group ordered by inclusion. For any subgroups H and K, $H \vee K$ is the subgroup generated by H and K, and $H \wedge K$ is the subgroup $H \cap K$.

Definition 7 (Order-isomorphism). *Let P and Q be partially ordered sets with partial orderings $\leq, \leq'$, respectively, and $f : P \to Q$ a map of sets. Then f is an* ***order-isomorphism*** *if f is surjective and $x \leq y$ in P iff $f(x) \leq' f(y)$ in Q.*

Definition 8 (Lattice-isomorphism). *Let L and K be lattices and $f : L \to K$ a map of sets. Then f is a* ***lattice-isomorphism*** *if f is bijective and $f(x \vee y) = f(x) \vee f(y)$ and $f(x \wedge y) = f(x) \wedge f(y)$, for all $x, y \in L$.*

Proposition 3. *Let L, K be lattices and $f : L \to K$ be a map of sets. Then, f is an order-isomorphism if and only if f is a lattice isomorphism.*

Proof: This follows from the definitions of $\vee$, $\wedge$, order-isomorphism, and lattice isomorphism. ■

For an arbitrary group, G, a partial ordering, $\leq$, can be placed on the set of conjugacy classes of subgroups, S, of G. Let $a, b \in S$. This ordering is given by $a \leq b$ if given any $H \in a$, there exists $K \in b$ such that $H \subseteq K$. Reflexivity and transitivity are clear. If $a \leq b$ and $b \leq a$, then order considerations imply that $a = b$. We will use that S is a poset in Chapters 3 and 5.

Chapter 3

Example One: $k = \mathbb{Q}(\sqrt{-2379})$

Bush takes $k = \mathbb{Q}(\sqrt{-2379})$ and shows that $G = Gal(k^{nr,2}/k)$ is one of 8 groups. In this Chapter, we isolate $Gal(k^{nr,2}/k)$ among 4 of the original 8 candidates. In doing so, we develop a general method that can actually identify $Gal(k^{nr,2}/k)$ provided that current technology could make the necessary computations.

Throughout, we refer to any one of the 8 groups as a *candidate* for G. Each candidate is the quotient of the free group $F(11)$ on 11 generators $x_1, \ldots, x_{11}$. The sets of relations defining each candidate are the same except for two elements. We give one set of relations below. The variables $r, s, t \in \{0, 1\}$ denote the exponents in the relations $(*)$ and $(*')$ below. Let $C_{1,rst}$ denote the candidate with exponents r, s, t. The "1" in the subscript signifies the first example. For instance, $C_{1,011}$ is defined by the relations $x_4^2(x_7x_{11}^r)^{-1} = x_4^2(x_7)^{-1}$ and $x_5^2(x_6x_9x_{10}^s x_{11}^t)^{-1,} = x_5^2(x_6x_9x_{10}x_{11})^{-1}$. The group $C_{1,rst}$ is defined by $F(11)/R_{rst}$ where R_{rst} is the normal subgroup generated by the words

$$\begin{array}{lll}
 & x_1^2x_4^{-1}, & [x_2,x_1]x_3^{-1} \\
 & x_2^2x_5^{-1}, & [x_3,x_1]x_6^{-1} \\
 & x_3^2(x_6x_8x_9x_{10})^{-1}, & [x_3,x_2]x_7^{-1} \\
(*) & \mathbf{x_4^2(x_7x_{11}^r)^{-1}}, & [x_4,x_2]x_8^{-1} \\
(*') & \mathbf{x_5^2(x_6x_9x_{10}^s x_{11}^t)^{-1}}, & [x_4,x_3]x_{10}^{-1} \\
 & x_6^2(x_9x_{10}x_{11})^{-1}, & [x_5,x_1](x_6x_7x_8x_9x_{10})^{-1} \\
 & x_7^2(x_{10}x_{11})^{-1}, & [x_5,x_3](x_{10}x_{11})^{-1} \\
 & x_9^2x_{11}^{-1}, & [x_6,x_1]x_9^{-1} \\
 & [x_5,x_4](x_{10}x_{11})^{-1}, & [x_8,x_2](x_{10}x_{11})^{-1} \\
 & [x_8,x_1]x_{10}^{-1}, & [x_9,x_1]x_{11}^{-1}.
\end{array}$$

The above gives the standard presentation for G. As indicated in Section 2.2, if the 2nd power of a generator does not appear above, then it is trivial, and similarly for the commutators of two generators. For example, the images of x_8, x_{10}, and x_{11} in a candidate each have order 2. As additional examples, we see that in any candidate the image of x_4 commutes with the image of x_1 and that the image of x_9 commutes with the image of x_m, where $2 \leq m \leq 11$. Note that each group has order 2^{11}. Also, each group has Frattini-quotient rank 2 because each is a descendant of $C_2 \times C_2$, as we showed in Section 2.3.

Our goal is to show that G is one of $C_{1,000}, C_{1,100}, C_{1,011}$, and $C_{1,111}$. In other words, we will decrease the number of possibilities for G by one-half and explicitly state the remaining possibilities for G. We start with an outline of our strategy. The first step is to use MAGMA to show that G contains a unique abelian subgroup

H of index 8. If F is any subfield of $k^{nr,2}$, we let $Cl_F^{(2)}$ denote the 2-class group of F. Let F^H denote the fixed field of H. The second step is to compute the action of $Gal(F^H/k)$ on $Cl_{F^H}^{(2)}$. The third and last step is to observe that this action gives rise to a set $\mathcal{E}_0$ of groups. We show that one of these groups must be G. Finally, Frattini-quotient rank information about the groups in $\mathcal{E}_0$ shows that G is one of $C_{1,000}, C_{1,100}, C_{1,011}$, and $C_{1,111}$.

Before executing the strategy, we make some briefly give some background about three topics: MAGMA and conjugacy classes of subgroups of a finite group, subfields of $k^{nr,2}$, and group extensions. The material presented in these remarks will be used to carry out our strategy. If F is a number field, we let $F^{(2)}$ denote the Hilbert 2-class field of F.

Proposition 4. *Let F be such that $k \subseteq F \subseteq k^{nr,2}$. Let $H = Gal(k^{nr,2}/F)$, and L be an unramified 2-extension of F. Then, $k \subseteq F \subseteq L \subseteq k^{nr,2}$. In particular, $k \subseteq F \subseteq F^{(2)} \subseteq k^{nr,2}$ and $Gal(F^{(2)}/F) \cong H/H' \cong Cl_{F^{(2)}}^{(2)}$.*

Proof: We have that $F \subseteq L \bigcap k^{nr,2} \subseteq L$. Then, L/F is an unramified 2-extension implies $L/(L \bigcap k^{nr,2})$ is also such an extension (by Galois theory and the multiplicative property of ramification index). Hence, $Lk^{nr,2}/k^{nr,2}$ is an unramified 2-extension by lifting. If $Lk^{nr,2} \neq k^{nr,2}$, then $Lk^{nr,2}/k^{nr,2}$ is a nontrivial unramified 2-extension and $Gal(Lk^{nr,2}/k^{nr,2})$ is a finite 2-group. A basic result in p-group theory implies that $Gal(Lk^{nr,2}/k^{nr,2})$ contains a subgroup, K, of index 2. The fixed field, B, of K then gives an unramified quadratic extension of $k^{nr,2}$, which is a contradiction. It follows that $L \subseteq k^{nr,2}$. In particular, $k \subseteq F \subseteq F^{(2)} \subseteq k^{nr,2}$, so let

$M = Gal(k^{nr,2}/F^{(2)}) \trianglelefteq H$. Since $F^{(2)}$ is the maximal abelian unramified 2-extension of F, $Gal(F^{(2)}/F) \cong H/H'$. Lastly, $Gal(F^{(2)}/F) \cong Cl^{(2)}_{F^{(2)}}$ by the Artin map. ■

We saw in Section 2.4 that the set of conjugacy classes of a group forms a poset. Recall that these sets have a partial ordering given by $x \leq y$ in P_l if and only if for each subgroup $M \in x$, there is some subgroup $K \in y$ such that $M \leq K$. Let C denote a candidate for G and S the partially ordered set of conjugacy classes of subgroups of C. MAGMA can compute S. In the output of these computations, MAGMA uses a positive integer to identify a conjugacy class of subgroups of C, so throughout we let i denote the ith conjugacy class of subgroups of C. A computation in MAGMA indicates that $\#S = 272$. In other words, C has 272 conjugacy classes of subgroups. For example, 1 denotes the class of $< id_C >$ and 272 denotes the class of C.

Next, suppose that subgroup class i is such that $i = \{H_1, \ldots, H_{m_i}\}$, where $H_1, \ldots, H_{m_i}$ are subgroups of C. We write *length*(i)=m_i. For example,

$$\textit{length}(272) = \textit{length}(1) = 1.$$

More generally, if $H \trianglelefteq C$ and i denotes the subgroup class containing H, then *length*(i)=1. We write *index*$(i) = r$ if $[G : H] = r$ for $H \in i$. For example, *index*(1)=$[C :< id_C >] = 2^{11}$ (recall from above) and *index*(272)=$[C : C]$=1.

The next proposition pertains to group extensions.

Proposition 5. *Suppose we are given an extension, e, of groups*

$$e : 1 \longrightarrow M \xrightarrow{j} E \xrightarrow{p} G \longrightarrow 1,$$

where M is abelian. This extension gives rise to an action of G on M, denoted by $\cdot$ and given by, for $g \in G$ and $m \in M$, $g \cdot m = \tilde{g}j(m)\tilde{g}^{-1}$, where $p(\tilde{g}) = g$. This action is independent of the choice of $\tilde{g}$.

Recall that this follows from the exactness of e and the fact that M is abelian. Given such an extension e, we will refer to E as the *extension group* of e. Whenever G acts on M, there is a resulting second cohomology group $H^2(G, M)$. This abelian group is in 1-1 correspondence with the set $\mathcal{E}$ of equivalence classes of extensions giving rise to the action of G on M. When G and M are finite, MAGMA can compute $H^2(G, M)$. Additionally, in our case, MAGMA can compute all extension groups. For example, if $G = M = C_2 =< \sigma >$ and C_2 acts trivially on C_2, then there are two equivalence classes of extensions of C_2 by C_2 giving rise to the trivial action. A representative, e_1, for the trivial class is

$$e_1 : 1 \longrightarrow C_2 \xrightarrow{j_1} C_2 \times C_2 \xrightarrow{p_1} C_2 \longrightarrow 1,$$

where $j_1 : \sigma \mapsto (\sigma, 1)$ and $p_1 : (\sigma, 1) \mapsto 1, (1, \sigma) \mapsto \sigma$. For the second class, let $C_4 =< \tau >$. A representative e_2 for the nontrivial class is

$$e_2 : 1 \longrightarrow C_2 \xrightarrow{j_2} C_4 \xrightarrow{p_2} C_2 \longrightarrow 1,$$

where $j_2 : \sigma \mapsto \tau^2$ and $p_2 : \tau \mapsto \sigma$. Hence, $\mathcal{E} = \{e_1, e_2\}$, the extension groups are $C_2 \times C_2$ and C_4, and MAGMA therefore outputs presentations for these two groups.

We now carry out our strategy. In the the first step, we will show that G contains a unique abelian normal subgroup H of index 8. The fixed field F^H with have 2-class field $k^{nr,2}$ by Proposition 1. The field F^H has degree 16 over $\mathbb{Q}$, which is a low enough degree to perform computations with F^H and $Cl^{(2)}_{F^H}$. In step two we will be use PARI to compute a generating polynomial for F^H over the $\mathbb{Q}$.

To find such an H, we show that each candidate contains the subgroup $C_2 \times C_8 \times C_{16}$ and this is the unique largest abelian subgroup of the candidate. This gives us the necessary H. Let C denote an arbitrary candidate.

Let S denote the set of conjugacy classes of subgroups of C. Subgroup classes 233 through 272 form the subset of S of subgroup classes of index at most 8.

A sequence of commands in MAGMA which tests whether a representative subgroup is abelian shows that class 235 is the only class whose representative is abelian. We compute that $length(235) = 1$. Let K_{235} denote the subgroup in class 235. Then $K_{235} \lhd C$. We compute that $K_{235} \cong C_2 \times C_8 \times C_{16}$. Finally, we see that the quotient $C/K_{235} \cong D_4$, the dihedral group of order 8.

Since C is an arbitrary candidate, G contains a unique abelian normal subgroup, $H \cong C_2 \times C_8 \times C_{16}$ such that $G/H \cong D_4$. As mentioned above, F^H/k is a normal extension of degree 8 such that and $Cl^{(2)}_{F^H} \cong C_2 \times C_8 \times C_{16}$ and has 2-class field $k^{nr,2}$. We remark also that $F^H/\mathbb{Q}$ is a normal extension of degree 16. This follows from the fact that $k^{nr,2}/\mathbb{Q}$ is Galois with normal subgroup G and H is unique hence characteristic in G.

The second step of our strategy is to find a generating polynomial over $\mathbb{Q}$ for F^H. The purpose of this step is to use the generating polynomial to compute in PARI the 2-class group of F^H. The method used in the second step can be broken down into three parts. In the first part, we show that H is a maximal subgroup of a subgroup J. In the second part, we show that J has fixed field

$E := \mathbb{Q}(\sqrt{-3}, \sqrt{13}, \sqrt{61})$. This implies that F^H is a quadratic subfield of $E^{(2)}$ that contains E. In the third part, we compute in MAGMA the generating polynomials of all unramified quadratic subfields of $E^{(2)}$ that contain E. This gives us a generating polynomial for F^H.

We start with the first part. Let C be an arbitrary candidate. MAGMA indicates that $235 \leq 260$ (as in our description of the poset of conjugacy classes of a group in Section 2.4), $index(260) = 4$, and $length(260) = 1$. Let M_{260} denote the subgroup in class 260, so $M \lhd C$ and $|M| = 2^9$. Let K_{235} be as above. Then, $K_{235} \leq M_{260}$ and $[K_{235} : M_{260}] = 2$. We compute the invariant factors of the abelianizations of all index 4 subgroups. Evidently, M_{260} is the unique normal subgroup of index 4 in G whose abelianization is $C_4 \times C_4 \times C_8$

We have that G contains a unique index 4 subgroup J with abelianization $C_4 \times C_4 \times C_8$ such that $H \leq J$. The fixed field F^J has 2-class group $C_4 \times C_4 \times C_8$.

We begin the second part of the second step, where we show that F^H is a quadratic extension of $E = \mathbb{Q}(\sqrt{-3}, \sqrt{13}, \sqrt{61})$. So far, we only know that H is a subgroup of index 2 of J. We show further that $J = Gal(k^{nr,2}/E)$.

We verify in PARI that E is an unramified 2-extension of k such that $Cl_E^{(2)} \cong C_4 \times C_4 \times C_8$. Also, we remark that the class group of E is equal to $Cl_E^{(2)}$. By the first part of Proposition 1, E is a subfield of $k^{nr,2}$, so let $I = Gal(k^{nr,2}/E)$. Then, $I \lhd G$, has index 4 in G, and abelianization $C_4 \times C_4 \times C_8$. The uniqueness of J shows that $I = J$ and $E = F^J$. Since H is a subgroup of index 2 of J, we have that F^H is a quadratic extension of E. It follows that F^H is a quadratic extension of E that is contained in $E^{(2)}$.

The third part is to use MAGMA to compute generating polynomials over $\mathbb{Q}$ of all quadratic subfields of $E^{(2)}$ containing E, and isolate among these the one that generates F^H. First, $Cl_E^{(2)}$ was computed in MAGMA. Evidently (and it can be shown using basic p-group theory), this group has seven subgroups $N_1, N_2, \ldots, N_7$ of index 2. Let $m \in \{1, \ldots, 7\}$ and F_m denote the fixed field of N_m. A sequence of commands computing class fields in MAGMA outputs a generating polynomial, p_m, of F_m over $\mathbb{Q}$.

We use these polynomials to compute in PARI the 2-class groups of the subfields $F_1, F_2, \ldots, F_7$. By the uniqueness of H, the polynomial p_{m_0}, where $m_0 \in \{1, \ldots, 7\}$, that generates a field having 2-class group $C_2 \times C_8 \times C_{16}$ is guaranteed to generate F^H.

The field, F_2, generated by

$$\begin{aligned} p_2(x) = x^{16} + 338x^{14} + 105445x^{12} + 2973386x^{10} + 77308156x^8 \\ + 2973386x^6 + 105445x^4 + 338x^2 + 1 \end{aligned}$$

has 2-class group $C_2 \times C_8 \times C_{16}$. (Moreover, the class group, Cl_L, of L is such that $Cl_L = Cl_L^{(2)}$.) We see that $F^H = F_2$, which we denote by L. As we mentioned above, $L/\mathbb{Q}$ is Galois. This concludes the second step of our strategy.

Now that we have a generating polynomial for $L/\mathbb{Q}$, we generate in PARI the class group information for L. The roots in L of $x^2 + 2379$ are also generated. PARI can compute ideals, I, J, K, representing generators for $Cl_L^{(2)}$. Let $[I]$ denote the class of I in $Cl_L^{(2)}$, and similarly for J and K. These ideals are such that order$([I]) = 2$, order$([J]) = 8$, and order$([K]) = 16$, and $Cl_L^{(2)} \cong < [I] > \times < [J] > \times < [K] >$.

The first goal is to find in PARI a pair of generators for $Gal(L/k)$. Since we observed in the first step that $Gal(L/k) \cong D_4$, it suffices to find a pair $\sigma, \tau \in Gal(L/\mathbb{Q})$ that satisfies:

1. σ, τ fix a root of $x^2 + 2379$,
2. σ has order 4, τ has order 2, and
3. $\sigma^2 \neq \tau$.

For 1., we test σ, τ on a root, α, of $x^2 + 2379$ to check if they fixed α. For 2., we check that σ^2 was not the identity. Once we find two distinct such σ, any other automorphism τ satisfying 1. must have order two by the structure of D_4. We then verify that $\sigma^2 \neq \tau$, thereby satisfying 3. Once a pair σ, τ is found, we compute the actions of σ and τ on the generators of $Cl_L^{(2)}$. The results are:

$$\begin{aligned}
\sigma([I]) &= [I][J]^4 \\
\sigma([J]) &= [J]^3[K]^4 \\
\sigma([K]) &= [J]^6[K]^7 \\
\tau([I]) &= [I][J]^4[K]^8 \\
\tau([J]) &= [J]^3[K]^4 \\
\tau([K]) &= [K].
\end{aligned}$$

Let $\delta : Gal(L/k_1) \to Aut(Cl_L^{(2)})$ denote this action.

We observed above that

$$Cl_L^{(2)} \cong Gal(k^{nr,2}/L) \cong C_2 \times C_8 \times C_{16} \quad \text{and} \quad Gal(L/k) \cong D_4.$$

MAGMA can compute the corresponding set of extension groups, as mentioned after

Proposition 5. Let $\mathcal{E}_0$ denote this set. Also, denote the Artin map by

$$\Phi : Cl_F \to Gal(L^{(2)}/L) = Gal(k^{nr,2}/L).$$

We showed in step one of our strategy that these last two groups are equal. Recall that the Artin map is a $Gal(L/k)$-module homomorphism. Also recall that the $Gal(L/k)$-module structure on Cl_F arises from the sequence

$$e_0' : 1 \longrightarrow Cl_F \cong Gal(k^{nr,2}/L) \xrightarrow{\subseteq} G \xrightarrow{res} Gal(L/k) \longrightarrow 1,$$

where the isomorphism is given by the Artin map and res denotes the restriction map. Since the Artin map is a $Gal(L/k)$-module homomorphism, e_0' gives rise to δ, the action of $Gal(L/k)$ on Cl_L computed in PARI.

We thus compute in MAGMA $H^2(D_4, C_2 \times C_8 \times C_{16})$ and the set $\mathcal{E}_0$ of extension groups. The remarks in the previous paragraph imply that $Gal(k^{nr,2}/k) \in \mathcal{E}_0$. We find that

$$H^2(D_4, C_2 \times C_8 \times C_{16}) \cong C_2 \times C_2 \times C_2.$$

By comparing the standard presentations of the extension groups, we find that $\mathcal{E}_0$ consists of 8 distinct groups. We also find that 4 of the groups are $C_{1,000}, C_{1,100}, C_{1,011}$, and $C_{1,111}$. The remaining 4 are not candidates. We have therefore achieved our goal.

Theorem 4. *G is one of the four groups $C_{1,000}, C_{1,100}, C_{1,011}$, and $C_{1,111}$.*

The question is whether or not it is possible to further isolate G among the remaining 4 candidates. Computations in MAGMA show that G contains the subgroup $C_8 \times C_{16}$ and that $C/(C_8 \times C_{16}) \cong Q$, a group of order 16. Fix C. When we compute $H^2(Q, C_8 \times C_{16})$ and the set $\mathcal{E}_\mathcal{C}$ extension groups, we find that C is the unique candidate in $\mathcal{E}_\mathcal{C}$. Proceeding as we did above, we would like to compute the generating polynomial of the fixed field M of $C_8 \times C_{16}$. From there, we could compute the action of $Gal(M/k)$ on $Cl_M^{(2)}$. Let $\mathcal{E}_0$ denote the corresponding set of extension groups. There is a candidate C_0 among the remaining 4 such that $\mathcal{E}_0 = \mathcal{E}_{C_0}$. Then, $G \in \mathcal{E}_{C_0}$. But this set contains exactly one candidate, and so $G = C_0$. However, current technology cannot compute a field of degree 32 over $\mathbb{Q}$.

Chapter 4

Example Two: $k = \mathbb{Q}(\sqrt{-445})$

Bush obtains two candidates for $G = Gal(k^{nr,2}/k)$, where $k = \mathbb{Q}(\sqrt{-445})$. Ideally, we would apply the method we used in Example One and obtain a set of extensions containing exactly one of the candidates. This candidate would be G. Unfortunately, we obtain a set of extension groups that contains both candidates. However, we describe the results from the attempt with the reason being that they relate to Example Three. Lastly, we describe distinctions between the two candidates that can be utilized to isolate G. Unfortunately, current technology cannot perform what we see to be the necessary computations to achieve this.

The two possibilities for G are quotients of the free group, $F(8)$, on 8 generators. With $r \in \{0, 1\}$, they are defined by $C_{2,r} = F(8)/R_r$, where R_r is the normal subgroup generated by the words

$$\begin{array}{ll}
x_1^2x_4^{-1}, & [x_2,x_1]x_3^{-1} \\
x_2^2(x_5x_7)^{-1}, & [x_3,x_1]x_5^{-1} \\
x_3^2(x_6x_7)^{-1}, & [x_3,x_2]x_6^{-1} \\
x_6^2x_8^{-1}, & [x_4,x_2](x_5x_6x_7x_8)^{-1} \\
x_4^2(x_8^r)^{-1}, & [x_4,x_3]x_7^{-1} \\
[x_5,x_1]x_7^{-1}, & [x_5,x_4]x_8^{-1} \\
[x_5,x_2]x_8^{-1}, & [x_7,x_1]x_8^{-1} \\
[x_5,x_3]x_8^{-1}, & [x_7,x_2]x_8^{-1}.
\end{array}$$

Note that the above set of relations gives the standard presentations for the candidates. The remarks made about powers and commutators of generators in Chapter 3 apply here. Also, we shall continue using the word *candidate* to describe any one of the possibilities for $Gal(k^{nr,2}/k)$. Each candidate has order 2^8, 2-class 5, and Frattini-quotient rank two. The two groups are indistinguishable up until the very last step of the p-group generation algorithm. Equivalently,

$$C_{2,1}/P_i(C_{2,1}) \cong C_{2,2}/P_i(C_{2,2}) \quad \text{for } 1 \leq i \leq 4.$$

At the last step we have that

$$C_{2,1}/P_5(C_{2,1}) \cong C_{2,1} \quad \text{and} \quad C_{2,2}/P_5(C_{2,2}) \cong C_{2,2},$$

but we see from the above that $C_{2,1} \ncong C_{2,2}$ since their standard presentations are not identical. It is the case that $P_4(C_{2,1})$ is a normal subgroup of order two of $C_{2,1}$, and similarly for $C_{2,2}$. That is, modulo an order two subgroup, the groups are identical. Moreover, $P_4(C_{2,i})$ is the unique normal subgroup of order two in $C_{2,i}$ for $i = 1, 2$.

Let C denote an arbitrary candidate. We proceed as in Example One by testing whether a subgroup of index at most 8 is abelian. Fix $i \in \{1, 2\}$. There exists an abelian subgroup $A_i \leq C_{2,i}$ such that $[C_{2,i} : A_i] = 8$ and

$$A_i \cong C_2 \times C_2 \times C_8,$$

Moreover, A_i is the unique abelian subgroup of $C_{2,i}$ of index eight, hence normal in $C_{2,i}$. There is no abelian subgroup of $C_{2,i}$ of greater order. Computations reveal that $C_{2,i}/A_i \cong D_4$. Hence, G is an extension of D_4 by $C_2 \times C_2 \times C_8$.

Let $a_{i,1}, a_{i,2}, a_{i,3} \in A_i$ of orders 2, 2, and 8, respectively, be such that A_i is the internal direct product of $< a_{i,1} >, < a_{i,2} >$, and $< a_{i,3} >$. Suppose that $Q_i = C_{2,i}/A_i$ is defined by

$$< r_i, s_i | r_i^4 = 1, s_i^2 = 1, r_i s_i r_i s_i^{-1} = 1 > .$$

Let $\circ_i$ denote the action of Q_i on A_i by conjugation. Computations in MAGMA show that

$$\begin{aligned}
r_i \circ_i a_{i,1} &= a_{i,1} + a_{i,2} + 4a_{i,3} \\
r_i \circ_i a_{i,2} &= a_{i,2} + 4a_{i,3} \\
r_i \circ_i a_{i,3} &= a_{i,1} + a_{i,2} + a_{i,3} \\
s_i \circ_i a_{i,1} &= a_{i,1} + 4a_{i,3} \\
s_i \circ_i a_{i,2} &= a_{i,2} + 4a_{i,3} \\
s_i \circ_i a_{i,3} &= a_{i,1} + a_{i,2} + a_{i,3}.
\end{aligned}$$

Let $\pi_i : C_{2,i} \to Q_i$ denote the quotient map and $\psi : A_1 \to A_2$ be the homomorphism given by

$$\psi : a_{1,l} \mapsto a_{2,l}, \quad l \in \{1,2,3\}.$$

Let $\phi : Q_1 \to Q_2$ be the homomorphism given by

$$\begin{aligned} \phi : r_1 &\mapsto r_2 \\ s_1 &\mapsto s_2 \end{aligned}$$

Then ψ and ϕ are isomorphisms that make the following diagram commute:

$$\begin{tikzcd} A_1 \arrow[r, "\subset"] \arrow[d, "\cong \psi"'] & C_{2,1} \arrow[r, "\pi_1"] & Q_1 \arrow[d, "\phi \cong"] \\ A_2 \arrow[r, "\subset"] & C_{2,2} \arrow[r, "\pi_2"] & Q_2. \end{tikzcd}$$

That is, the action of Q_1 on A_1 is isomorphic to the action of Q_2 on A_2. Let $\mathcal{E}_i$ denote the set of extension groups corresponding to the action of Q_i on $A_i, i = 1, 2$. Then we have that $\mathcal{E}_1 = \mathcal{E}_2$. In particular, each set contains both candidates.

Proceeding as we did in Example One, let F^K denote the fixed field of $K \leq G$ found above. Let $\mathcal{E}_0$ denote the set of extension groups arising from the action of $Gal(F^K/k_2)$ on $Cl_{F^K}^{(2)}$. We have that $\mathcal{E}_0 = \mathcal{E}_1 = \mathcal{E}_2$, so $C_{3,1}, C_{3,2} \in \mathcal{E}_0$. Therefore, no new information results from computing $\mathcal{E}_0$.

Nonetheless, we make a few observations about cohomology and the groups in $\mathcal{E}_0$. A computation yields

$$H^2(D_4, C_2 \times C_2 \times C_8) \cong C_2 \times C_2 \times C_2.$$

The set $\mathcal{E}_0$ consists of 8 groups distinct up to isomorphism. Four of these groups have Frattini-quotient rank 2, and the remaining 4 have Frattini-quotient rank 3.

Note that the semi-direct product has Frattini-quotient rank 3, so that neither of the candidates are the semi-direct product.

These results are similar to those obtained in Example Three. Because of this, various patterns can be detected among the two examples. In Chapter 5, we further discuss Example Three and explore these patterns.

Since Example One's method fails to isolate G, we search for other differences between the two candidates. In MAGMA, we compute that $C_{2,1}$ has 64 elements of order eight and $C_{2,2}$ has 128 elements of order eight. Suppose we could compute the cyclic subfields of $k^{nr,2}/k$ of degree 32 over k (there are either 16 or 32 of them). The candidate having the correct number of such elements would be G. However, any such subfield has degree 64 over $\mathbb{Q}$, which makes computations difficult.

The question becomes whether or not a similar disparity occurs in the set of elements having order $m > 8$. It turns out that 16 is the greatest order of any element. Since an element of order 16 corresponds to a cyclic subgroup with fixed field having degree 32 over $\mathbb{Q}$, our technology again fails to help. Regardless, both groups have the same number of elements of order 16.

Another distinction occurs with the set of conjugacy classes of subgroups of each candidate. The subgroup posets of the two candidates have cardinalities that differ only by two: $C_{2,1}$ has 85 conjugacy classes of subgroups and $C_{2,2}$ has 87 conjugacy classes of subgroups. This is because of the difference in the number of conjugacy classes of order 4. Recall that the order of a conjugacy class is the order of a subgroup in that class. The candidate $C_{2,1}$ has 11 conjugacy classes of order 4, while $C_{2,2}$ has 13. Consequently, $C_{2,2}$ has 32 more subgroups of order 4. The numbers of conjugacy classes having order different from 4 are the same for each candidate. By the above, these 32 subgroups must be cyclic. As a result, $C_{2,1}$ has 279 subgroups and $C_{2,1}$ has 311 subgroups. We have not yet found distinctions in addition to these.

Chapter 5

Example Three: $k = \mathbb{Q}(\sqrt{-1015})$, $k = \mathbb{Q}(\sqrt{-1595})$

5.1 Description of Candidates

In this example, Bush takes $k = \mathbb{Q}(\sqrt{-1015})$ and uses his method to generate two possibilities for $G = Gal(k^{nr,2}/k)$. As we noted in Chapter 2, he shows that the same two groups are candidates for G, where $k = \mathbb{Q}(\sqrt{-1595})$. We demonstrate our attempt at applying the method from Example One. Although the method fails to isolate G, the attempt does reveal certain parallels with Example Two.

The two possibilities for G are $C_{3,1}$ and $C_{3,2}$. Each group has order 2^9, exponent-2 class 5, and Frattini-quotient rank 2. Each candidate is a quotient of the free group $F(9)$ on 9 generators. Let $r \in \{0, 1\}$. Each candidate is defined by $F(9)/R_r$ where R_r is the normal subgroup generated by the words

$$\begin{array}{ll}
x_1^2x_4^{-1}, & [x_2,x_1]x_3^{-1} \\
x_2^2(x_5x_7)^{-1}, & [x_3,x_1]x_5^{-1} \\
x_3^2(x_7x_8)^{-1}x_9^{r-1}, & [x_3,x_2]x_6^{-1} \\
x_4^2x_6^{-1}, & [x_4,x_2]x_8^{-1}x_9^{r-1} \\
x_6^2x_8^{-1}, & [x_4,x_2](x_5x_7x_8x_9^r)^{-1} \\
x_8^2x_9^{-1}, & [x_4,x_3]x_7^{-1} \\
[x_5,x_1]x_7^{-1} & [x_5,x_4]x_9^{-1} \\
[x_5,x_2]x_9^{-1} & [x_7,x_1]x_9^{-1} \\
[x_5,x_3]x_9^{-1} & [x_7,x_2]x_9^{-1}.
\end{array}$$

The above gives the standard presentation of the two candidates. The remarks about powers and commutators of generators made in Chapter 3 apply here.

Like in Example Two, the candidates are indistinguishable through the fourth iteration of the p-group generation algorithm. After the fifth iteration, the two groups are generated. Also, $P_4(C_{3,1})$ is the unique normal subgroup of order two of $C_{3,1}$, and similarly for $C_{3,2}$. Hence, modulo a unique normal subgroup of order two, the groups are identical.

We proceed as we did in Chapter 3. Let C denote either $C_{3,1}$ or $C_{3,2}$. By examining the poset of conjugacy classes of C, we find that C contains a abelian subgroup, K, of index 8, and this is the largest abelian subgroup. It is the case that $K \lhd C$ and $K \cong C_2 \times C_2 \times C_{16}$. Additionally, $C/K \cong D_4$. Thus, G is an extension of D_4 by $C_2 \times C_2 \times C_{16}$.

Fix $i \in \{1,2\}$. Denote by A_i the subgroup of $C_{3,i}$ isomorphic to $C_2 \times C_2 \times C_{16}$.

Let $a_{i,1}, a_{i,2}, a_{i,3} \in A_i$ of orders 2, 2, and 16, respectively, be such that $A_i \cong < a_{i,1} > \times < a_{i,2} > \times < a_{i,3} >$. Define $Q_i = C_{2,i}/A_i$ by the presentation

$$< r_i, s_i | r_i^4 = 1, s_i^2 = 1, r_i s_i r_i s_i^{-1} = 1 > .$$

Let $\circ_i$ denote the action of Q_i on A_i by conjugation. Computations in MAGMA show that

$$\begin{aligned}
r_i \circ_i a_{i,1} &= a_{i,1} + a_{i,2} + 8a_{i,3} \\
r_i \circ_i a_{i,2} &= a_{i,2} + 8a_{i,3} \\
r_i \circ_i a_{i,3} &= a_{i,1} + a_{i,2} + a_{i,3} \\
s_i \circ_i a_{i,1} &= a_{i,1} + 8a_{i,3} \\
s_i \circ_i a_{i,2} &= a_{i,2} + 8a_{i,3} \\
s_i \circ_i a_{i,3} &= a_{i,1} + a_{i,2} + a_{i,3}
\end{aligned}$$

Note that if we replace each 8 above by a 4, we obtain the action in Example Two. As with Example Two, the actions are isomorphic and the method applied in Example One fails to isolate G.

Nonetheless, we use MAGMA to compute the resulting second cohomology group and corresponding set of extensions. Interestingly, we continue to obtain results similar to those from Example Two. Indeed, we compute that

$$H^2(D_4, C_2 \times C_2 \times C_{16}) \cong C_2 \times C_2 \times C_2.$$

The set $\mathcal{E}$ of extension groups consists of 8 groups, distinct up to isomorphism. Four of the groups have Frattini-quotient rank two. The remaining four have Frattini-quotient rank three and include the semi-direct product.

Next, we examine the subgroup posets of $C_{3,1}$ and $C_{3,2}$. We find that the subgroup lattices are isomorphic. We show this now.

5.2 Subgroup Lattice Isomorphism for $C_{3,1}$ and $C_{3,2}$

Fix $m \in \{1, 2\}$. Let P_m denote the set of conjugacy classes of subgroups of $C_{3,m}$. Recall from Section 2.4 that these sets have a partial ordering given by $x \leq y$ in P_m if and only if for each subgroup $M \in x$, there is some subgroup $K \in y$ such that $M \leq K$. Let L_m denote the subgroup lattice of $C_{3,m}$. We saw in Chapter 3 that MAGMA can compute P_1 and P_2. We continue to use an integer to denote a conjugacy class of subgroups. We extend to subgroups the idea of identifying a subgroup class by an integer. Let $i.j$ denote the jth subgroup in the ith subgroup class of P_1. Similarly, let $i'.j$ denote the jth subgroup in subgroup class i' of P_2. For example, 24.3 denotes the 3rd subgroup in the 24th subgroup class of $C_{3,1}$ as output in MAGMA, and $24'.3$ denotes the 3rd subgroup in subgroup class $24'$ of $C_{3,2}$.

We give some definitions of terms which we will use to describe subgroups of $C_{3,1}$ and $C_{3,2}$. Let C be one of Bush's final candidates and P its partially ordered set of subgroup classes.

Definition 9. *Subgroup class* $i = \{i.1, i.2, \ldots, i.j_i\} \in P$ *has* ***order*** s*, denoted by order(*i*)* $= s$*, if* $|i.1| = |i.2| = \ldots = |i.j_i| = s$*.*

In other words, order(i) is just the order of any subgroup in i.

Definition 10. *Let $i, k \in P$. If $i \leq k$ and order(k)=order(i)/2, then we say that i is a **maximal subclass** of k.*

This second definition was inspired by the term *maximal subgroup.* We have that i is a maximal subclass of k if given $i.j \in i$, there is some $k.l \in k$ such that $[k.l : i.j] = 2$. Also, $[k.l : i.j] = 2$ if and only if $i.j$ is a maximal subgroup of $k.l$. This is by the fact about finite p-groups that a subgroup H of a finite p-group G is a maximal subgroup of G if and only if $[G : H] = p$.

Definition 11. *We say that $k.l$ is a **minimal overgroup** of $i.j$ is a maximal subgroup of $k.l$.*

Using MAGMA, we find that P_1 and P_2 are very similar. Specifically, we find that $\#P_1 = \#P_2 = 95, \#L_1 = \#L_2 = 252$. Recall that we denote the number of subgroups in subgroup class i by $length(i)$. We find that $order(i) = order(i')$ and $length(i) = length(i')$ for all $1 \leq i, i' \leq 95$. This shows that for each subgroup $i.j \in L_1$, there is a corresponding subgroup $i'.j \in L_2$. Additionally, we run an iterative loop to compare the standard presentation of a subgroup representing class i with the standard presentation of a subgroup representing class i'. Interestingly, we find it is the case that for all $1 \leq i, i' \leq 94$, the subgroups of class i are of the same isomorphism class as the subgroups of class i'. Since for all $1 \leq i, i' \leq 94$, $length(i) = length(i')$, this shows that $i.j \cong i'.j$ for all $1 \leq j \leq length(i)$. In other words, for any $i.j \in L_1$, we have that $i.j$ is isomorphic to its corresponding subgroup $i'.j \in L_2$. Using an iterative loop in MAGMA, we also find that $i \leq j$ in P_1 if and only if $i' \leq j'$ in P_2. This implies that the map

$$\begin{aligned} h: \quad P_1 \to & \quad P_2, \quad \text{given by} \\ i \mapsto & \quad i' \end{aligned}$$

is an order-isomorphism. Some additional results are that in $C_{3,1}$ there are 9 subgroups of order 2, 35 of order 4, 35 of order 8, 59 of order 16, 59 of order 32, 39 of order 64, 7 of order 128, 3 of order 256, and 1 of order 512. The same is true of $C_{3,2}$.

Recall that P_1 and P_2 are the conjugacy classes of subgroups, while L_1 and L_2 are the subgroup lattices. Because P_1 and P_2 are order-isomorphic and $\#L_1 = \#L_2$, the natural question is whether L_1 and L_2 are lattice isomorphic. We find that the answer to this question is yes. We show this is true by constructing a lattice isomorphism $f : L_1 \to L_2$. The rest of this section is devoted to defining this map f and then verifying that f so defined is a lattice isomorphism.

The goal is to show that L_1 and L_2 are isomorphic as lattices by first showing that they are order-isomorphic and then using Proposition 3 in Chapter 2. Computationally, it seems easier to test if a map is an order-isomorphism then if it is a lattice isomorphism. The map h above inspires the idea for the map $\widetilde{h} : L_1 \to L_2$ defined by $\widetilde{h} : i.j \mapsto i'.j$. It turns out to be that $\widetilde{h}$ is not an order-isomorphism, so nor is $\widetilde{h}$ a lattice isomorphism by Proposition 3. However, we are able to use the idea of $\widetilde{h}$ to define a map $f : L_1 \to L_2$ such that f is an order-isomorphism. There are 3 steps here. The first step is to determine on which pairs of subgroups $\widetilde{h}$ fails to be an order-isomorphism. The second step is to change the definition of $\widetilde{h}$ on a subset of L_1 to a map f. To do this, we use minimal overgroup and maximal subgroup information provided by MAGMA. The third step is to verify that f is an order isomorphism. Then by Proposition 3, f will be a lattice isomorphism.

The first step is to see on which subgroups of $C_{3,1}$ the map $\widetilde{h}$ fails to be an order-isomorphism. To do this, we write a loop to test if the Boolean $(i.j \leq k.l)$ equals the Boolean $(i'.j \leq k'.l)$ for all subgroups $i.j, k.l, i'.j, k'.l$ and run it in MAGMA. The result is that $i.j \leq l.k$ has the same truth value as $i'.j \leq l'.k$ for all $i.j, k.l, i'.j, k'l$, except for $i = 3, i' = 3'$ and $k = 12, k' = 12'$. For $i = i' = 3$ and $k = k' = 12$, it is the case that:

$$3.1 \leq 12.2, 12.3, 12.4, 12.6, \quad 3.2 \leq 12.1, 12.5, 12.7, 12.8 \quad \text{in} \quad L_1, \quad (*)$$

while the reverse held in L_2:

$$3'.1 \leq 12'.1, 12'.5, 12'.7, 12'.8, \quad 3'.2 \leq 12'.2, 12'.3, 12'.4, 12'.6 \quad \text{in} \quad L_2. \quad (*')$$

The second step is to figure out how to change $\widetilde{h}$ to a map f that is an order-isomorphism $f : L_1 \to L_2$. Therefore, we would like it to be that $f : i.j \mapsto i'.l$, where $i'.l$ is some subgroup that is conjugate to $i'.j$. This way, we have that $i.j \cong f(i.j)$, for $1 \leq i \leq 94$ and $1 \leq j \leq \mathit{length}(i)$, by the remarks made above. The issue is that if we define $f(i.j) = i'.m \neq i'.j$ and $i.j$ is a maximal subgroup of $k.l$, then we may need to define $f(k.l) \neq k'.l$ for $i \neq 3, k \neq 12$. For example, in L_1 we have that $3.1 \leq 10.1, 10.3$ and $3.2 \leq 10.2, 10.4$. We know the analogous containments $3'.1 \leq 10'.1, 10'.3$ and $3'.2 \leq 10'.2, 10'.4$ hold in L_2 by the output in MAGMA. Hence, if we define $f(3.1) = 3'.2$, then we are forced to also define $f(10.1) = 10'.2$ or $10'.4$. Similarly, if we define $f(k.l) = k'.n \neq k'.l$ and $k.l$ is a minimal overgroup of $i.j$, then we may need to define $f(i.j) \neq i'.j$ In L_1, we have that $4.1, 4.4 \leq 10.1$

and $4.3, 4.4 \leq 10.2$, and as above, the analogous containments hold in L_2. Thus, if we choose that $f(10.1) = 10'.2$, then we must also define $f(4.1) = 4'.3$ or $4'.4$. In light of these examples, our first move is to define

$$\begin{aligned} f: \quad 3.1 \mapsto & \quad 3'.1 \quad \text{and} \\ 3.2 \mapsto & \quad 3'.2, \end{aligned}$$

By $(*)$, and $(*')$, we see that f must be such that $f(12.1) = 12'.2, 12'.3, 12'.4$, or $12'.6$, so in particular, $f(12.1) \neq 12'.1$. Now, in MAGMA $12 \leq 24$ and $12.1 \leq 24.1$, and the analogous containments hold in P_2 and L_2. As we will see below, if we first define $f(24.1)$, this restricts $f(12.1)$ to two of four of the above subgroups. Hence, we explain first how to define $f(24.1)$ and then define $f(12.1)$ after this.

To define $f(24.1)$, we first examine the minimal overgroups of the subgroups in classes 12 and 24. We compute in MAGMA that 12 is a maximal subclass of 24, and 24 is a maximal subclass of 35,38, and 39. In the table below, the subgroups in these classes and their maximal subgroups are enumerated. For $H = i.j$ where $i \in \{24, 35, 38, 39\}$, the ratio $H : m_1.n_1, m_2.n_2, \ldots, m_{r_H}.n_{r_H}$ in the table indicates that the maximal subgroups of H are $m_1.n_1, m_2.n_2, \ldots, m_{r_H}.n_{r_H}$. Similar ratios hold for the corresponding subgroups in L_2.

$H \leq C_{1,3}$	: maximal subg. of H	$H \leq C_{1,3}$	: maximal subg. of H
24.1	: 6.1, 12.1, 12.5	35.1	: 14.1, 24.1, 24.2
24.2	: 6.1, 12.2, 12.3	35.2	: 14.1, 24.3, 24.4
24.3	: 6.1, 12.4, 12.6	38.1	: 15.1, 24.1, 24.3
24.4	: 6.1, 12.7, 12.8	38.2	: 15.1, 24.2, 24.4
		39.1	: 16.1, 24.1, 24.4
		39.2	: 16.1, 24.2, 24.3

For example, the first row in the right-hand column indicates that the maximal subgroups of 35.1 are 14.1, 24.1, and 24.2. In particular, 35.1 has three maximal subgroups.

Additionally, $35, 39$ are maximal subclasses of 49 only, while 38 is a maximal subclass of each of 49, 54, and 57. Recall that the analogous containments are true for P_2 by the map h above. Moreover, *length*(49)=1, so 49.1 is a normal subgroup of $C_{3,1}$ and hence contains all the subgroups in classes 35, 38, and 39,and the same is true for P_2. We see that if we define $f : 49.1 \mapsto 49'.1$, we are free to define $f(35.1) = 35'.1$ or $f(35.1) = 35'.2$. With either choice, the biconditional $35.1 \leq 49.1$ if and only if $f(35.1) \leq f(49.1)$, holds. We have similar freedom in defining f on the subgroups 35.2, 39.1, and 39.2. Since 38 is a maximal subclass of 49,54, and 57, and $\mathit{length}(54) = \mathit{length}(57) = 2$, we do not have the same kind of freedom with

38. Hence, we define

$$\begin{aligned} f:\ \ 38.1 \mapsto &\ \ 38'.1 \\ 38.2 \mapsto &\ \ 38'.2 \\ i.j \mapsto &\ \ i'.j, \quad i.j \quad \text{is any (other) maximal subg. of 54.1, 54.2, 57.1, or 57.2.} \end{aligned}$$

This way, we can define

$$\begin{aligned} f: 54.1 &\mapsto 54'.1, \\ f: 54.2 &\mapsto 54'.2, \\ f: 57.1 &\mapsto 57'.1, \\ f: 57.2 &\mapsto 57'.2 \end{aligned}$$

and have that $38.1 \leq 54.1$ if and only if $f(38.1) \leq f(54.1)$, etc. hold.

By the table above and that $f(38.1) = 38'.1$, we must have that $f : 24.1 \mapsto 24'.1$ or $f : 24.1 \mapsto 24'.3$. Now, we have that $12.1 \leq 24.1$, the analogous containment in L_2, and that the possible images for 12.1 are $12'.2, 12'.3, 12'.4, 12'.6$. The table above indicates that $12'.2, 12'.3, 12'.4, 12'.6 \leq 24'.2$ or $24'.3$. Hence, we are forced to define $f(24.1) = 24'.3$. Similarly, we are forced to have

$$\begin{aligned} f: 24.2 &\mapsto 24'.4, \\ f: 24.3 &\mapsto 24'.1, \\ f: 24.4 &\mapsto 24'.2. \end{aligned}$$

Next, we define f on the subgroups of 12. Defining f on the remaining subgroups of L_1 follows easily after this. Because $f : 24.1 \mapsto 24'.3$, we must define

$f(12.1) = 12'.4$ or $f(12.1) = 12'.6$. We choose $f(12.1) = 12'.4$. We make similar choices for the remaining subgroups of 12. For the subgroups in L_1 whose images were not specified above, we define $f(i.j) = i'.j$. Then, $f : L_1 \to L_2$ is given by

$$f(i.j) \quad = \quad \begin{cases} i.j & if\ i \notin \{12, 24, 35, 39\} \\ 12'.4 & if \quad i.j = 12.1 \\ 12'.7 & if \quad i.j = 12.2 \\ 12'.8 & if \quad i.j = 12.3 \\ 12'.1 & if \quad i.j = 12.4 \\ 12'.6 & if \quad i.j = 12.5 \\ 12'.5 & if \quad i.j = 12.6 \\ 12'.2 & if \quad i.j = 12.7 \\ 12'.3 & if \quad i.j = 12.8 \\ 24'.3 & if \quad i.j = 24.1 \\ 24'.4 & if \quad i.j = 24.2 \\ 24'.1 & if \quad i.j = 24.3 \\ 24'.2 & if \quad i.j = 24.4 \\ 35'.2 & if \quad i.j = 35.1 \\ 35'.1 & if \quad i.j = 35.2 \\ 39'.2 & if \quad i.j = 39.1 \\ 39'.1 & if \quad i.j = 39.2 \end{cases}$$

We have that f is surjective. Suppose we are given any subgroup $k'.l \in k'$ of $C_{3,2}$. If $k' \in \{12, 24, 35, 39\}$, then by definition of f we have that $k'.l = f(k.j_l)$ for some subgroup $k.j_l \in k$. If $k' \notin \{12, 24, 35, 39\}$, then $k'.l = f(k.l)$. Hence, f is surjective.

Since $\#L_1 = \#L_2$, it must also be that f is injective. We note that $f = \widetilde{h}$ on the set $L_1 - \tilde{S}$, where $\tilde{S} = \{12.1, 12.2, \ldots, 12.8, 24.1, \ldots, 24.4, 35.1, 35.2, 39.1, 39.2\}$.

The last step is to verify that f defines an order-isomorphism. From there, we will have that f defines a lattice isomorphism by Claim 1. This last step is divided into four parts. We want to show that $i.j \leq k.l$ in L_1 if and only if $f(i.j) \leq f(k.l)$ in L_2. To show this, the first part is to show that $i.j \leq k.l$ if and only if $f(i.j) \leq f(k.l)$ is true on maximal subgroups, then this biconditional is true for any pair of subgroups $i.j, k.l \leq C_{3,1}$. More precisely, we show that if

(1) $i.j$ is a maximal subgroup of $k.l$ if and only if

$f(i.j)$ is a maximal subgroup of $f(k.l)$

then

(2) $i.j \leq k.l$ if and only if

$f(i.j) \leq f(k.l)$ for every pair of subgroups $i.j, k.l \in L_1$.

Our ultimate goal is to prove (2), so that by first showing (1) implies (2), we reduce our work in this step to showing that (1) holds. Hence, the first part is showing that (1) implies (2). We are then left with showing that (1) holds. The second part is to construct a set S, given explicitly below, where S consists of the subgroups on which we have changed the definition of $\widetilde{h}$ together with each of these subgroups' minimal overgroups. The third part is to show that (1) holds in the case that $k.l \in S$. The fourth part then is to show that holds for $k.l \notin S$. This covers the two possible cases for $k.l$, and thus shows that (1) holds.

We begin by showing that (1) implies (2). This implication follows from

Proposition 6. *Let p be a prime, G a finite p-group, and any subgroups H, K of G for which $H \leq K$. Then there is a subnormal series $H = H_1 \trianglelefteq H_2 \trianglelefteq \cdots \trianglelefteq H_{s-1} \trianglelefteq H_s = K$ such that each factor has order p.*

Proof: This follows from basic properties of finite p-groups. ■

We now use Proposition6 to prove (1) implies (2). The point here is that $i.j \leq k.l$ in L_1, then $i.j$ is a maximal subgroup of $k.l$ if and only if $[k.l : i.j] = 2$, and similarly for L_2. We assume (1) holds and start by proving the forward direction of (2). If $i.j \lneqq k.l$, then by Claim 2 there exist subgroups $i_1.j_1, i_2.j_2, \ldots, i_s.j_s$ of $k.l$ such that

$$i.j = i_1.j_1 \trianglelefteq i_2.j_2 \trianglelefteq \cdots \trianglelefteq i_s.j_s = k.l$$

whose factors have order 2. In other words, for all $t \in \{2, \ldots, s\}, i_{t-1}.j_{t-1}$ is a maximal subgroup of $i_t.j_t$. Then by the forward direction of (1), we have that for all $t \in \{2, \ldots, s\}, i_{t-1}.j_{t-1} \leq i_t.j_t$ implies that $f(i_{t-1}.j_{t-1}) \leq f(i_t.j_t)$. Transitivity then gives $f(i.j) \leq f(k.l)$. For the reverse direction, apply the above with f^{-1}.

The second part is to construct the set S described above. As mentioned, we let S consist of all $k.l \in L_1$ such that either $f(k.l) \neq k'.l$ or $k.l$ is the minimal overgroup of some $i.j$ such that $f(i.j) \neq i'.j$. For example, $12.1 \in S$ since $f(12.1) = 12'.4$. Also, $38.1 \in S$: although $f(38.1) = 38'.1$, by the table above, 24.1 is a maximal subgroup of 38.1 and $f(24.1) = 24'.3$. By the definition of f and the discussion on the minimal overgroups of classes $35, 38, 39$ above, we see that

$$
\begin{aligned}
S = \{&12.1, 12.2, 12.3, 12.4,\\
&12.5, 12.6, 12.7, 12.8,\\
&24.1, 24.2, 24.3, 24.4,\\
&35.1, 35.2, 38.1, 38.2,\\
&39.1, 39.2,\\
&49.1\}
\end{aligned}
$$

In other words, S consists of the subgroups of classes $\{12, 24, 35, 38, 49\}$. To show that (1) holds for $k.l \in S$, we use a 3-column table. The idea is to use this table to show that for $k.l \in S$,

$i_1.j_1, \ldots, i_{q_{k.l}}.j_{q_{k.l}}$ are the maximal subgroups of $k.l$ if and only if

$f(i_1.j_1), \ldots, f(i_{q_{k.l}}.j_{q_{k.l}})$ are the maximal subgroups of $f(k.l)$. $\quad (**)$

Since $(**)$ clearly implies (1), we will then have (1) holds for $k.l \in S$.

In the first column of the table is a ratio

$$k.l : i_1.j_1, \ldots, i_{q_{k.l}}.j_{q_{k.l}},$$

where $i_1.j_1, \ldots, i_{q_{k.l}}.j_{q_{k.l}}$ are the maximal subgroups of $k.l \in S$. This is just like the ratio used in the table above. For example, the ratio $24.1 : 6.1, 12.1, 12.5$ appears in a row of the first column since 6.1, 12.1, and 12.5 comprise the maximal subgroups of 24.1 in L_1. The second column is the ratio $f(k.l) : a'_1.b_1, \ldots a'_{q_{k.l}}.b_{q_{k.l}}$, where $a'_1.b_1, \ldots a'_{q_{k.l}}.b_{q_{k.l}}$ are the maximal subgroups in L_2 of $f(k.l)$. Note that $k.l$

and $f(k.l)$ have the same number of maximal subgroups since the isomorphism class of the subgroups in k is the same as the isomorphism class of the subgroups in k'. Keeping with the same example, the second column is $24'.3 : 6'.1, 12'.4, 12'.6$ since $f(24.1) = 24'.3$ and in L_2 the maximal subgroups of $24'.3$ are $6'.1, 12'.4, 12'.6$. The purpose of the second column will only be to use it to write the third column. The third column is the ratio $f(k.l) : f(m_1.n_1), \ldots, f(m_{q_{k.l}}.n_{q_{k.l}})$, where $f(m_1.n_1) = a'_1.b_1, \ldots, f(m_{q_{k.l}}.n_{q_{k.l}}) = a'_{q_{k.l}}.b_{q_{k.l}}$. In other words, the third column is the second column rewritten as its image under f. In the example above, the third column reads $f(24.1) : f(6.1), f(12.1), f(12.5)$ since $24'.3 = f(24.1), 6'.1 = f(6.1), 12'.4 = f(12.1)$, and $12'.6 = f(12.5)$. Note that this last column is well-defined since f is bijective. The table is:

H:maximal subgroups of H	$f(H)$:maximal subgroups of $f(H)$	$f(H)$:maximal subgroups of $f(H)$ rewritten as image under f
12.1:3.2	12'.4:3'.2	$f(12.1) : f(3.2)$
12.2:3.1	12'.7:3'.1	$f(12.2) : f(3.1)$
12.3:3.1	12'.8:3'.1	$f(12.3) : f(3.1)$
12.4:3.1	12'.1:3'.1	$f(12.1) : f(3.1)$
12.5:3.2	12'.6:3'.2	$f(12.5) : f(3.2)$
12.6:3.1	12'.5:3'.2	$f(12.6) : f(3.1)$
12.7:3.2	12'.2:3'.2	$f(12.7) : f(3.2)$
12.8:3.2	12'.3:3'.2	$f(12.8) : f(3.2)$
$24.1 : 6.1, 12.1, 12.5$	$24'.3 : 6'.1, 12'.4, 12'.6$	$f(24.1) : f(6.1),$ $f(12.1), f(12.5)$
$24.2 : 6.1, 12.2, 12.3$	$24'.4 : 6'.1, 12'.7, 12'.8$	$f(24.2) : f(6.1),$ $f(12.2), f(12.3)$
$24.3 : 6.1, 12.4, 12.6$	$24'.1 :' 6'.1, 12'.1, 12'.5$	$f(24.3) : f(6.1),$ $f(12.4), f(12.6)$
$24.4 : 6.1, 12.7, 12.8$	$24'.2 : 6'.1, 12'.2, 12'.3$	$f(24.4) : f(6.1),$ $f(12.4), f(12.1)$
$35.1 : 14.1, 24.1, 24.2$	$35'.2 : 14'.1, 24'.3, 24'.4$	$f(35.1) : f(14.1),$ $f(24.1), f(24.2)$
35.2:14.1,24.3,24.4	35'.1:14'.1,24'.1,24'.2	$f(35.2) : f(14.1),$ $f(24.3), f(24.4)$
38.1:15.1,24.1,24.3	38'.1:15'.1,24'.3,24'.1	$f(38.1) : f(15.1),$ $f(24.1), f(24.3)$
38.2:15.1,24.2,24.4	38'.2:15'.1,24'.4,24'.2	$f(38.2) : f(15.1),$ $f(24.2), f(24.4)$
39.1:16.1,24.1,24.4	39'.2:16'.1,24'.3,24'.2	$f(39.1) : f(16.1),$ $f(24.1), f(24.4)$
$39.2 : 16.1, 24.2, 24.3$	$39'.1 : 16'.1, 24'.4, 24'.1$	$f(39.2) : f(16.1),$ $f(24.2), f(24.3)$
$49.1 : 28.1, 35.1, 35.2, 38.1,$ $38.2, 39.1, 39.2$	$49'.1 : 28'.1, 35'.1, 35'.2, 38'.1$ $38'.2, 39'.1, 39'.2$	$f(49.1) : f(28.1), f(35.2), f(35.1),$ $f(38.1), f(38.2),$ $f(39.2), f(39.1)$

After composing this table, we inspect it line-by-line to see that

$$\{i_1.j_1, \ldots, i_{q_{k.l}}.j_{q_{k.l}}\} = \{m_1.n_1, \ldots, m_{q_{k.l}}.n_{q_{k.l}}\} \quad (**')$$

holds for each $k.l$ listed in the table. Again, $i_1.j_1, \ldots, i_{q_{k.l}}.j_{q_{k.l}}$ are the maximal subgroups of $k.l$ and $f(m_1.n_1), \ldots, f(m_{q_{k.l}}.n_{q_{k.l}})$ are the maximal subgroups of $f(k.l)$. Then $(**')$ easily implies $(**)$ for $k.l \in S$. For, $i.j$ is a maximal subgroup of $k.l$

implies that $i.j \in \{i_1.j_1, \ldots, i_{q_{k.l}}.j_{q_{k.l}}\}$. Then, $(**')$ implies that $i.j = m_t.n_t \in \{m_1.n_1, \ldots, m_{q_{k.l}}.n_{q_{k.l}}\}$. Hence, $f(i.j) = f(m_t.n_t) \in \{f(m_1.n_1), \ldots, f(m_{q_{k.l}}.n_{q_{k.l}})\}$, the set of maximal subgroups of $f(k.l)$. That is, $f(i.j)$ is a maximal subgroup of $f(k.l)$. Conversely, if $f(i.j)$ is a maximal subgroup of $f(k.l)$, then $f(i.j) \in \{f(m_1.n_1), \ldots, f(m_{q_{k.l}}.n_{q_{k.l}})\}$, and so $f(i.j) = f(m_t.n_t)$ for some $m_t.n_t$ in the set $\{m_1.n_1, \ldots, m_{q_{k.l}}.n_{q_{k.l}}\}$. Since f is injective, $i.j = m_t.n_t$. By $(**'), i.j = m_t.n_t \in \{i_1.j_1, \ldots, i_{q_{k.l}}.j_{q_{k.l}}\}$, the set of maximal subgroups of $k.l$. That is, $i.j$ is a maximal subgroup of $k.l$. Thus, $(**)$ holds for $k.l \in S$, and so (1) holds for $k.l \in S$.

We now start the fourth part, which is to show that (1) holds for $k.l \notin S$. Suppose that $k.l \notin S$. Then, $f(k.l) = k'.l$ by definition of S. Suppose $i.j$ is a maximal subgroup of $k.l$. By definition, S contains all subgroups $m.n$ such that either $f(m.n) \neq m'.n$ or $m.n$ is a minimal overgroup of some $a.b$ such that $f(a.b) \neq a'.b$. If $f(i.j) \neq i'.j$, then $k.l \in S$ since $k.l$ is a minimal overgroup of $i.j$. This contradicts the assumption; therefore, $f(i.j) = i'.j$. We saw when we tested if $\widetilde{h}$ was an order isomorphism that $i.j \leq k.l$ if and only if $i'.j \leq k'.l$, except for if both $i = 3, i' = 3'$ and $k = 12, k' = 12'$. Since $k.l \notin S$, we have that $k \neq 12$. Hence, $f(i.j) = i'.j$ is a maximal subgroup of $f(k.l) = k'.l$. Conversely, suppose that $f(i.j)$ is a maximal subgroup of $f(k.l)$. Again, $k.l \notin S$ implies that $f(k.l) = k'.l$ by definition of S. If $f(i.j) \neq i'.j$, then by definition of f, $i' = 12', 24', 35'$, or $39'$ (these are the only subgroup classes of P_2 containing subgroups on which $\widetilde{h}$ was changed). Since $f(i.j)$ is a maximal subgroup of $k'.l$, we have $k' = 24', 35', 38', 39'$, or $49'$ (these are the subgroup classes of which $i' = 12', 24', 35'$, or $39'$ are maximal subclasses). But then, $k = 24, 35, 38, 39,49 \in S$, which is a contradiction. Thus, $f(i.j) = i'.j$. We saw above that the condition $k \notin S$ implies that if $i'.j \leq k'.l$, then $i.j \leq k.l$. Since $f(i.j) = i'.j$ and $f(k.l) = k'.l$, we have $i.j \leq k.l$. This covers the two possible cases.

Hence (1) holds. Then, (1) implies (2), so that f is an order-isomorphism. Propositionr̃eforderiso gives us that f is a lattice isomorphism.

5.3 Comparing Examples Two and Three

In a few places so far, we have noted parallels and contrasts among the results obtained for Examples Two and Three. We divide these patterns into three types. The first type of similarity pertains to group cohomology. The D_4-actions on each abelian subgroup of greatest order are similar. The resulting second cohomology groups have the same structure, and the extension groups have the same Frattini-quotient ranks. A contrast can be observed in the groups' subgroup lattices. While the subgroup posets of $C_{2,1}$ and $C_{2,2}$ are not isomorphic, their cardinalities differ only by two. In Example Three, the candidates' posets of conjugacy classes of subgroups are order-isomorphic, and the candidates' subgroup lattices are lattice isomorphic. A second comparison can be made in the generation of the 4 candidates with the p-group generation algorithm: all groups are the same through the second step of their generation. In other words, it is not until the third iteration of the p-group generation algorithm that we can detect a difference between the four candidates. Let C denote one of the the four groups $C_{2,1}, C_{2,2}, C_{3,1}, C_{3,2}$. We observe that $C/P_2(C)$ has order 16 and has standard presentation

$$< x_1, x_2, x_3, x_4 | x_1^2 = x_4, [x_2, x_1] = x_2 x_3 > .$$

Starting at the third iteration, the four pair off and the elements of each pair of candidates are indistinguishable until the fourth (and final) iteration of the algorithm. The picture is given in Figure 5.1.

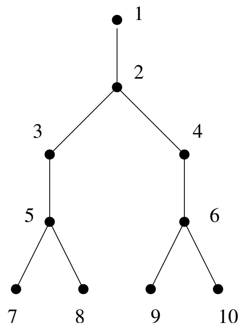

Figure 5.1: The generation of the candidates in Examples Two and Three is given above. Vertex 1 is the maximal exponent-2 class 1 quotient of each candidate, vertex 2 is the maximal exponent-2 class 2 quotient of each candidate, etc. Verticies 7 and 8 represent $C_{2,1}$ and $C_{2,2}$; verticies 9 and 10 represent $C_{3,1}$ and $C_{3,2}$.

These parallels warrant a more thorough study of the extension groups giving rise to the D_4-actions from Examples Two and Three. Interestingly, we find that they are members of an infinite class of group extensions. The groups among this class share properties that the groups in examples two and three have in common.

5.4 A Class of Group Extensions

We begin by considering the D_4-action in each example. Let D_4 be defined by the presentation

$$< r, s | r^4 = 1, s^2 = 1, rsrs^{-1} = 1 > .$$

Fix $n \geq 3$. Let $a_{n,1}, a_{n,2}, a_{n,3} \in C_2 \times C_2 \times C_{2^n}$ be of orders 2, 2, and 2^n, respectively, such that

$$C_2 \times C_2 \times C_{2^n} \cong < a_{n,1} > \times < a_{n,2} > \times < a_{n,3} > .$$

Let D_4 act on $C_2 \times C_2 \times C_{2^n}$ with action $\circ_n$ given by:

$$\begin{aligned}
r \circ_n a_{n,1} &= a_{n,1} + a_{n,2} + 2^{n-1} a_{n,3} \\
r \circ_n a_{n,2} &= a_{n,2} + 2^{n-1} a_{n,3} \\
r \circ_n a_{n,3} &= a_{n,1} + a_{n,2} + a_{n,3} \\
s \circ_n a_{n,1} &= a_{n,1} + 2^{n-1} a_{n,3} \\
s \circ_n a_{n,2} &= a_{n,2} + 2^{n-1} a_{n,3} \\
s \circ_n a_{n,3} &= a_{n,1} + a_{n,2} + a_{n,3}
\end{aligned}$$

Taking $n = 3$ yields the D_4-action on $C_2 \times C_2 \times C_8$ in Example Two. Taking $n = 4$ yields the D_4-action on $C_2 \times C_2 \times C_{16}$ in Example Three. This action gives rise to $H^2(D_4, C_2 \times C_2 \times C_{2^n})$. Let $\mathcal{E}_n$ denote the corresponding extension groups. For example, $\mathcal{E}_3$ contains $C_{2,1}$ and $C_{2,2}$. The set $\mathcal{E}_4$ contains $C_{3,1}$ and $C_{3,2}$.

Do the trends apparent in $\mathcal{E}_3$ and $\mathcal{E}_4$ continue to hold for $n \geq 5$? Fix $n \geq 5$. We ask three questions:

1. Is $H^2(D_4, C_2 \times C_2 \times C_{2^n}) \cong C_2 \times C_2 \times C_2$? Is the cardinality of $\mathcal{E}_n$ equal to eight? Do the extension groups share the same properties of Frattini rank as the extension groups in $\mathcal{E}_3$ and $\mathcal{E}_4$?

2. Are there pairs of extension groups that have isomorphic subgroup lattices with corresponding proper subgroups and quotients isomorphic?

3. In the p-group generation algorithm, are the extension groups identical up to a certain point in their generation? At what point can you begin to distinguish them?

To investigate these questions, we look at the groups in $\mathcal{E}_n$ when $n = 3, 4, 5, 6, 7, 8$. For what follows, we fix $n \in \{3, 4, \dots, 8\}$.

We start by addressing the questions in group cohomology. We found that the patterns present in $\mathcal{E}_3$ and $\mathcal{E}_4$ continue to hold in $\mathcal{E}_n$. Specifically,

$$H^2(D_4, C_2 \times C_2 \times C_{2^n}) \cong C_2 \times C_2 \times C_2.$$

By comparing standard presentations of the extension groups, we find that $\mathcal{E}_n$ contains eight groups distinct up to isomorphism. Four groups have Frattini-quotient rank two, and four have Frattini-quotient rank three, and these latter four include the semi-direct product.

To answer 2., we use Example Three as a prototype when attempting to construct a subgroup lattice isomorphism among a pair of groups in $\mathcal{E}_n$. We note that in order for there to exist a lattice isomorphism between the subgroup lattices of the groups in the pair, the two groups must have the same Frattini-quotient rank. For, the Frattini-quotient rank determines the number of maximal subgroups, and these are easily identified in the lattice.

Recall that in Example Three, we began by constructing an order-isomorphism between subgroup posets of the pair of candidates before constructing a lattice isomorphism. Hence, among the groups having the same Frattini-quotient rank, we compute cardinalities of each group's poset of conjugacy classes of subgroups. If one group's poset has the same cardinality as the other's, we pair them together. We notice that Frattini-quotient-rank-two groups tend to have considerably fewer conjugacy classes of subgroups. Also, the groups in Bush's examples have Frattini-quotient rank two, so we restrict ourselves to Frattini-quotient rank two.

From here, we examine subgroup posets of each group in a pair. Let the notation for subgroup classes be as above. It turns out that given any pair of Frattini-quotient-rank-two groups in E_n whose subgroup posets have the same cardinality, the map

$$i \mapsto i'$$

is an order-isomorphism. We then use the order-isomorphism to construct a lattice isomorphism that preserves the isomorphism classes of proper subgroups and proper quotients. By using a similar procedure to that applied in Example Three, we obtain lattice isomorphisms for each pair of groups in $\mathcal{E}_4, \mathcal{E}_5, \ldots, \mathcal{E}_8$ having subgroup posets with the same cardinality. The maps are given at the end of the chapter.

Question 3 examines how the groups compare in their generation in the p-group generation algorithm. We revisit in more detail the observations made with the generations of $C_{2,1}, C_{2,2}, C_{3,1}$, and $C_{3,2}$. Recall that:

$$C_{2,1}/P_1(C_{2,1}) \cong C_{2,2}/P_1(C_{2,2}) \cong C_{3,1}/P_1(C_{3,1}) \cong C_{3,2}/P_1(C_{3,2})$$
$$\text{and} \quad C_{2,1}/P_2(C_{2,1}) \cong C_{2,2}/P_2(C_{2,2}) \cong C_{3,1}/P_2(C_{3,1}) \cong C_{3,2}/P_2(C_{3,2}).$$

But the same is not true for P_3 and beyond:

$$C_{2,1}/P_3(C_{2,1}) \ncong C_{3,1}/P_3(C_{3,1}),$$

$$C_{2,1}/P_4(C_{2,1}) \ncong C_{3,1}/P_4(C_{3,1}),$$

$$C_{2,1}/P_5(C_{2,1}) \ncong C_{3,1}/P_5(C_{3,1}).$$

Fix $n \in \{3, 4, 5, 6, 7, 8\}$. Let $\mathcal{E}_{n,1}$, $\mathcal{E}'_{n,1}$ denote a pair of groups in E_n having isomorphic subgroup lattices. Let $E_{n,2}$ and $E'_{n,2}$ be the other pair. We compute the 2-central series of each of $\mathcal{E}_{n,1}, \mathcal{E}'_{n,1}, \mathcal{E}_{n,2}$, and $\mathcal{E}'_{n,2}$ and form quotients. This gives the groups appearing at each step in the p-group generation algorithm. Four types of patterns are present.

The first pattern pertains to the number of descendants of the extensions. We first find that for $n \geq 4$, the 2-class of each of $\mathcal{E}_{n,1}, \mathcal{E}'_{n,1}, \mathcal{E}_{n,2}$, and $\mathcal{E}'_{n,2}$ is $n+1$. For example, we saw that $C_{3,1}$, and $C_{3,2}$ each has 2-class five. Note that this is not the case with $n = 3$ since $C_{2,1}$ and $C_{2,2}$ each has 2-class 5. Recall that a finite p-group is terminal if it has no immediate descendants. Evidently, for $3 \leq n \leq 8$, the four Frattini-quotient rank two groups are terminal.

The second trend pertains to the exponent-2 class two quotients. By comparing the Standard Presentations, we find that the all groups have the same maximal exponent-2 class 2 quotient. This group E has order 16 and standard presentation

$$< x_1, x_2, x_3, x_4 | x_1^2 = x_4, [x_2, x_1] = x_3 > .$$

We saw that

$$C_{2,j}/P_2(C_{2,j}) \cong C_{3,j}/P_2(C_{3,j}) \cong E$$

for $j = 1, 2$, and similarly for $C_{3,1}$ and $C_{3,2}$.

The third pattern pertains to the generation of a pair of groups having isomorphic subgroup lattices. Fix $n \geq 4$ and consider $\mathcal{E}_{n,1}$ and $\mathcal{E}'_{n,1}$. These groups are indistinguishable through p-class n. The same is true for $\mathcal{E}_{n,2}$ and $\mathcal{E}'_{n,2}$:

$$\mathcal{E}_{n,1}/P_n(\mathcal{E}_{n,1}) \cong \mathcal{E}'_{n,1}/P_n(\mathcal{E}'_{n,1}) \quad \text{and} \quad \mathcal{E}_{n,2}/P_n(\mathcal{E}_{n,2}) \cong \mathcal{E}'_{n,2}/P_n(\mathcal{E}'_{n,2})$$

but

$$\mathcal{E}_{n,1}/P_{n+1}(\mathcal{E}_{n,1}) \ncong \mathcal{E}'_{n,1}/P_{n+1}(\mathcal{E}'_{n,1}) \quad \text{and} \quad \mathcal{E}_{n,2}/P_{n+1}(\mathcal{E}_{n,2}) \ncong \mathcal{E}'_{n,2}/P_{n+1}(\mathcal{E}'_{n,2}).$$

We saw this for $C_{2,1}$, $C_{2,2}$, $C_{3,1}$, and $C_{3,2}$. Note that

$$E_{n,1}/P_j(E_{n,1}) \ncong E_{n,2}/P_j(E_{n,2})$$

for $j \geq 3$. For example,

$$C_{3,1}/P_4(C_{3,1}) \cong C_{3,2}/P_4(C_{3,2}) \text{but} C_{3,1}/P_5(C_{3,1}) \ncong C_{3,2}/P_5(C_{3,2})$$

as noted above. Also, $C_{3,1}/P_3(C_{3,1}) \ncong E_{4,2}/P_3(E_{4,2})$, so that it must also be $C_{3,2}/P_3(C_{3,2}) \ncong E'_{4,2}/P_3(E'_{4,2})$ by the above remarks.

Lastly, we look at similarities between E_m and E_n, where $m \neq n$. We see that for $4 \leq n \leq 8$:

$$E_{n,1}/P_{n-1}(E_{n,1}) \cong E_{n+1,1}/P_{n-1}(E_{n+1,1}),$$
$$E'_{n,1}/P_{n-1}(E'_{n,1}) \cong E'_{n+1,1}/P_{n-1}(E'_{n+1,1}),$$
$$E_{n,2}/P_{n-1}(E_{n,2}) \cong E_{n+1,2}/P_{n-1}(E_{n+1,2}),$$
$$E'_{n,2}/P_{n-1}(E'_{n,2}) \cong E'_{n+1,2}/P_{n-1}(E'_{n+1,2}).$$

However,

$$E_{n,1}/P_n(E_{n,1}) \ncong E_{n+1,1}/P_n(E_{n+1,1}), \text{etc.}$$

For example, take $n = 4$:

$$C_{3,1}/P_3(C_{3,1}) \cong E_{5,1}/P_3(E_{5,1}), \text{but} C_{3,1}/P_4(C_{3,1}) \ncong E_{5,1}/P_4(E_{5,1}).$$

In other words, $C_{3,1}$ and $E_{5,1}$ are identical through the third iteration of the p-group generation algorithm, but differ after the fourth iteration. The picture for the pairs $E_{n,1}$ and $E'_{n,1}, n = 3, 4, \ldots, 7$ is given in Figure 5.2. The pairs $E_{n,2}$ and $E'_{n,2}, n = 3, 4 \ldots, 7$ have a similar picture.

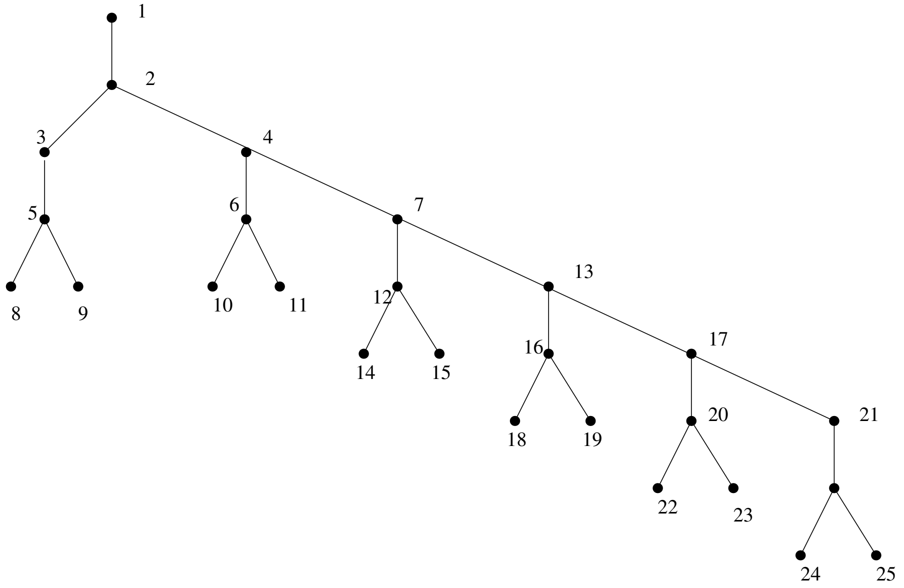

Figure 5.2: The generation of $E_{3,1}, E'_{3,1}, E_{3,2}, E'_{3,2}$, etc.

Verticies 8 and 9 represent $C_{2,1}$ and $C_{2,2}$; verticies 10 and 11 represent $C_{3,1}$ and $C_{3,2}$; verticies 14 and 15 represent $E_{5,1}$ and $E'_{5,1}$, etc. Verticies on the same level have the same exponent-2 class. For example, $C_{2,1}, C_{2,2}, C_{3,1}$, and $C_{3,2}$ have 2-class 5. Verticies 25 and 26 represent $E_{8,1}$ and $E_{8,2}$, which have 2-class 9. Note that all extensions are descendants of E (Vertex 2). Also, the picture shows that $E_{7,1}$ and $E_{8,1}$ have the same maximal 2-class 6 quotients (Vertex 17), and similarly for other groups branching off from the same node.

We conjecture that all the above patterns hold for all $n \geq 3$.

Conjecture 1. *Let the action by D_4 on $C_2 \times C_2 \times C_{2^n}$ be as above. For $n \geq 3$, $H^2(D_4, C_2 \times C_2 \times C_{2^n}) \cong C_2 \times C_2 \times C_2$. Four of the corresponding group extensions have Frattini-quotient rank two and four have Frattini-quotient rank three, including the semi-direct product. For $n \geq 4$, the Frattini-quotient-rank-two groups form two pairs such that the groups in each pair have isomorphic posets of conjugacy classes of subgroups and isomorphic subgroup lattices.*

Conjecture 2. *Let the notation be as in Conjecture 1. Given $n \geq 3$ and a pair of Frattini-quotient rank 2 groups or a Frattini-quotient rank 3 group in $H^2(D_4, C_2 \times C_2 \times C_{2^n})$, the steps of the p-group generation algorithm of each follow the specific pattern described above.*

Lastly, we conjecture presentations for the 3 index 2 subgroups of a Frattini-quotient-rank-two group in $\mathcal{E}_n$. Let $n \geq 4$ and consider a pair of Frattini-quotient rank 2 groups in $\mathcal{E}_n$ having isomorphic subgroup lattices. Let $M_{n,1,1}, M_{n,1,2}$, and $M_{n,1,3}$ denote the three maximal subgroups of $E_{n,1}$. Recall that the maximal subgroups of $E_{n,1}$ and $E'_{n,1}$ are the same by the nature of the subgroup lattice isomorphism above. We find that the Frattini-quotient ranks of $M_{n,1,1}$ and $M_{n,1,2}$ are two, and the Frattini-quotient rank of $M_{n,1,3}$ is three.

Using MAGMA to compute standard presentations of subgroups of $E_{n,1}$ and $E'_{n,1}$, we find that $M_{n,1,1}$ is a quotient of the free group $F(n+4)$ on $n+4$ generators for $4 \leq n \leq 8$. Specifically, $M_{n,1,1}$ is defined by $F_{n+4}/R_{n,1,1}$, where $R_{n,1,1}$ is the normal subgroup generated by the words

$$\begin{array}{ll}
x_1^2x_4^{-1}, & [x_2,x_1]x_3^{-1} \\
x_2^2x_5^{-1}, & [x_3,x_1]x_5^{-1} \\
x_4^2x_6^{-1}, & [x_3,x_2]x_{n+4}^{-1} \\
x_6^2x_7^{-1}, & [x_4,x_2]x_5 \\
x_7^2x_8^{-1}, & [x_4,x_3]x_{n+4} \\
\vdots & [x_5,x_1]x_{n+4}^{-1} \\
x_{n+3}x_{n+4}^{-1}. &
\end{array}$$

The second maximal subgroup $M_{n,1,2}$ of $E_{n,1}$ and $E'_{n,1}$ is defined by $F_{n+4}/R_{n,1,2}$ where $R_{n,1,2}$ is the normal subgroup generated by the words

$$\begin{array}{ll}
x_1^2x_4^{-1}, & [x_2,x_1]x_3^{-1} \\
x_2^2x_5^{-1}, & [x_3,x_1]x_5^{-1} \\
x_3^2x_{n+4}^{-1}, & [x_3,x_2]x_{n+4}^{-1} \\
x_4^2x_6^{-1}, & [x_4,x_2](x_5x_{n+4})^{-1} \\
x_6^2x_7^{-1}, & \\
x_7^2x_8^{-1} & \\
\vdots & \\
x_{n+3}x_{n+4}^{-1}. &
\end{array}$$

The Frattini-rank-3 maximal subgroup is defined by $F_{n+4}/R_{n,1,3}$ where $R_{n,1,3}$

is the normal subgroup generated by the words

$$\begin{array}{ll}
x_1^2x_6^{-1}, & [x_2,x_1]x_4^{-1} \\
x_2^2x_4^{-1}, & [x_3,x_1]x_5^{-1} \\
x_3^2x_5^{-1}, & [x_3,x_2]x_{n+3}^{-1} \\
x_6^2x_7^{-1}, & [x_4,x_3]x_{n+4}^{-1} \\
x_7^2x_8^{-1}, & [x_5,x_2]x_{n+4}^{-1} \\
\vdots & \\
x_{n+3}x_{n+4}^{-1}. &
\end{array}$$

Note that the maximal subgroups of $C_{2,1}$ and $C_{2,2}$ do not follow this pattern.

As with the first pair, $\mathcal{E}_{n,2}$ and $\mathcal{E}'_{n,2}$, $n \geq 4$, each has two Frattini-quotient-rank-2 subgroups and a Frattini-quotient-rank-3 subgroup. Let $M_{n,2,1}, M_{n,2,2}, M_{n,2,3}$ denote these subgroups, respectively. By using MAGMA to compare standard presentations, we see that

$$M_{n,1,1} \cong M_{n,2,1} \quad \text{and} \quad M_{n,1,2} \cong M_{n,2,2}.$$

However, the Frattini-rank-3 groups are not isomorphic. There is one relation in the standard presentation of $M_{n,1,3}$ that is different from $M_{n,2,3}$. This relation is in boldface below. Specifically, $M_{n,2,3}$ is defined by $F(n+4)/R_{n,2,3}$ where $R_{n,2,3}$ is the normal subgroup generated by the words

$$\begin{array}{ll}
x_1^2 x_6^{-1}, & [x_2, x_1] x_4^{-1} \\
\mathbf{x_2^2 (x_4 x_6)^{-1}}, & [x_3, x_1] x_5^{-1} \\
x_3^2 x_5^{-1}, & [x_3, x_2] x_{n+3}^{-1} \\
x_6^2 x_7^{-1}, & [x_4, x_3] x_{n+4}^{-1} \\
x_7^2 x_8^{-1}, & [x_5, x_2] x_{n+4}^{-1} \\
\vdots & \\
x_{n+3} x_{n+4}^{-1}. &
\end{array}$$

Again, the maximal subgroups in the second pair of groups, $E_{3,2}$ and $E'_{3,2}$, do not follow this pattern.

Conjecture 3. *Given $n \geq 4$, the maximal subgroups of $E_{n,1}$, $E'_{n,1}$, $E_{n,2}$, and $E'_{n,2}$ have the standard presentations given above.*

5.5 Subgroup Lattice Isomorphisms for $E_{4,2}, E'_{4,2}, \ldots, E_{8,2}, E'_{8,2}$

The rest of this chapter gives the subgroup lattice isomorphisms for the groups in $\mathcal{E}_n$ for $4 \leq n \leq 8$. Recall that the map for $C_{3,1}$ and $C_{3,2}$ (i.e. $E_{4,1} \to E_{4,2}$) was given in Section 5.2.

For $n = 4$, the map, $f_{4,2} : E_{4,2} \to E'_{4,2}$ is given by

$$f_{4,2}(i.j) \quad = \quad \begin{cases} i.j & if\ i \notin \{16, 30, 42, 43\} \\ 16'.4 & if \quad i.j = 16.1, \\ 16'.7 & if \quad i.j = 16.2, \\ 16'.8 & if \quad i.j = 16.3, \\ 16'.1 & if \quad i.j = 16.4, \\ 16'.6 & if \quad i.j = 16.5, \\ 16'.5 & if \quad i.j = 16.6, \\ 16'.2 & if \quad i.j = 16.7, \\ 16'.3 & if \quad i.j = 16.8, \\ 30'.3 & if \quad i.j = 30.1, \\ 30'.4 & if \quad i.j = 30.2, \\ 30'.1 & if \quad i.j = 30.3, \\ 30'.2 & if \quad i.j = 30.4, \\ 42'.2 & if \quad i.j = 42.1, \\ 42'.1 & if \quad i.j = 42.2, \\ 43'.2 & if \quad i.j = 43.1, \\ 43'.1 & if \quad i.j = 43.2. \end{cases}$$

For $n = 5$, the first map $f_{5,1} : E_{5,1} \to E'_{5,1}$ is given by

$$f_{5,1}(i.j) = \left\{ \begin{array}{llllll} i'.j & if\ i \notin \{4, 11, 14, 15, 16, 26, 44, 46\} & & & & \\ 4'.3 & if \quad i.j = 4.1, & & & & \\ 4'.2 & if \quad i.j = 4.2, & & & & \\ 4'.1 & if \quad i.j = 4.3, & & 16'.j & if & i.j = 15.j, \\ 4'.1 & if \quad i.j = 4.4, & & 15'.j & if & i.j = 16.j, \\ 11'.3 & if \quad i.j = 11.1, & & 26'.3 & if & i.j = 26.1, \\ 11'.4 & if \quad i.j = 11.2, & & 26'.4 & if & i.j = 26.2, \\ 11'.1 & if \quad i.j = 11.3, & & 26'.1 & if & i.j = 26.3, \\ 11'.2 & if \quad i.j = 11.4, & & 26'.2 & if & i.j = 26.4, \\ 14'.4 & if \quad i.j = 14.1, & & 44'.2 & if & i.j = 44.1, \\ 14'.7 & if \quad i.j = 14.2, & & 44'.1 & if & i.j = 44.2, \\ 14'.8 & if \quad i.j = 14.3, & & 46'.2 & if & i.j = 46.1, \\ 14'.1 & if \quad i.j = 14.4, & & 46'.1 & if & i.j = 46.2. \\ 14'. & if \quad i.j = 14.5, & & & & \\ 14'.5 & if \quad i.j = 14.6, & & & & \\ 14'.2 & if \quad i.j = 14.7, & & & & \\ 14'.3 & if \quad i.j = 14.8, & & & & \end{array} \right.$$

For $n = 5$, the second map $f_{5,2} : E_{5,2} \longrightarrow E'_{5,2}$ is given by

$$f_{5,2}(i.j) \quad = \quad \begin{cases} i.j & if\ i \notin \{12, 26, 40, 43\} \\ 12'.4 & if \quad i.j = 12.1, \\ 12'.7 & if \quad i.j = 12.2, \\ 12'.8 & if \quad i.j = 12.3, \\ 12'.1 & if \quad i.j = 12.4, \\ 12'.6 & if \quad i.j = 12.5, \\ 12'.5 & if \quad i.j = 12.6, \\ 12'.2 & if \quad i.j = 12.7, \\ 12'.3 & if \quad i.j = 12.8, \\ 26'.3 & if \quad i.j = 26.1, \\ 26'.4 & if \quad i.j = 26.2, \\ 26'.1 & if \quad i.j = 26.3, \\ 26'.2 & if \quad i.j = 26.4, \\ 40'.2 & if \quad i.j = 40.1, \\ 40'.1 & if \quad i.j = 40.2, \\ 43'.2 & if \quad i.j = 43.1, \\ 43'.1 & if \quad i.j = 43.2. \end{cases}$$

For $n = 6$, the first map $f_{6,1} : E_{6,1} \longrightarrow E'_{6,1}$ is given by

$$f_{6,1}(i.j) = \begin{cases} i'.j & if\ i \notin \{4, 11, 13, 14, 16, 29, 48, 51\} \\ 4'.3 & if \quad i.j = 4.1, \\ 4'.2 & if \quad i.j = 4.2, \\ 4'.1 & if \quad i.j = 4.3, \\ 4'.1 & if \quad i.j = 4.4, \\ 11'.3 & if \quad i.j = 11.1, \\ 11'.4 & if \quad i.j = 11.2, \\ 11'.1 & if \quad i.j = 11.3, \\ 11'.2 & if \quad i.j = 11.4, \\ 16'.4 & if \quad i.j = 16.1, \\ 16'.7 & if \quad i.j = 16.2, \\ 16'.8 & if \quad i.j = 16.3, \\ 16'.1 & if \quad i.j = 16.4, \\ 16'.6 & if \quad i.j = 16.5, \\ 16'.5 & if \quad i.j = 16.6, \\ 16'.2 & if \quad i.j = 16.7, \\ 16'.3 & if \quad i.j = 16.8, \end{cases} \qquad \begin{array}{lll} 14'.j & if & i.j = 13.j, \\ 13'.j & if & i.j = 14.j, \\ 29'.3 & if & i.j = 29.1, \\ 29'.4 & if & i.j = 29.2, \\ 29'.1 & if & i.j = 29.3, \\ 29'.2 & if & i.j = 29.4, \\ 48'.2 & if & i.j = 48.1, \\ 48'.1 & if & i.j = 48.2, \\ 51'.2 & if & i.j = 51.1, \\ 51'.1 & if & i.j = 51.2. \end{array}$$

For $n = 6$, the second map $f_{6,2} : E_{6,2} \to E'_{6,2}$ is given by

$$f_{6,2}(i.j) \quad = \quad \begin{cases} i.j & if\ i \notin \{12, 25, 34, 43\} \\ 12'.4 & if \quad i.j = 12.1, \\ 12'.7 & if \quad i.j = 12.2, \\ 12'.8 & if \quad i.j = 12.3, \\ 12'.1 & if \quad i.j = 12.4, \\ 12'.6 & if \quad i.j = 12.5, \\ 12'.5 & if \quad i.j = 12.6, \\ 12'.2 & if \quad i.j = 12.7, \\ 12'.3 & if \quad i.j = 12.8, \\ 25'.3 & if \quad i.j = 25.1, \\ 25'.4 & if \quad i.j = 25.2, \\ 25'.1 & if \quad i.j = 25.3, \\ 25'.2 & if \quad i.j = 25.4, \\ 34'.2 & if \quad i.j = 34.1, \\ 34'.1 & if \quad i.j = 34.2, \\ 43'.2 & if \quad i.j = 43.1, \\ 43'.1 & if \quad i.j = 43.2. \end{cases} .$$

For $n = 7$, the first map $f_{7,1} : E_{7,1} \to E'_{7,1}$ is given by

$$f_{7,1}(i.j) = \begin{cases} i'.j & if\ i \notin \{4, 11, 13, 14, 16, 29, 48, 51\} \\ 4'.3 & if \quad i.j = 4.1, \\ 4'.2 & if \quad i.j = 4.2, \\ 4'.1 & if \quad i.j = 4.3, \\ 4'.1 & if \quad i.j = 4.4, \\ 11'.3 & if \quad i.j = 11.1, \\ 11'.4 & if \quad i.j = 11.2, \\ 11'.1 & if \quad i.j = 11.3, \\ 11'.2 & if \quad i.j = 11.4, \\ 16'.4 & if \quad i.j = 16.1, \\ 16'.7 & if \quad i.j = 16.2, \\ 16'.8 & if \quad i.j = 16.3, \\ 16'.1 & if \quad i.j = 16.4, \\ 16'.6 & if \quad i.j = 16.5, \\ 16'.5 & if \quad i.j = 16.6, \\ 16'.2 & if \quad i.j = 16.7, \\ 16'.3 & if \quad i.j = 16.8, \\ 14'.j & if \quad i.j = 13.j, \\ 13'.j & if \quad i.j = 14.j, \\ 29'.3 & if \quad i.j = 29.1, \\ 29'.4 & if \quad i.j = 29.2, \\ 29'.1 & if \quad i.j = 29.3, \\ 29'.2 & if \quad i.j = 29.4, \\ 48'.2 & if \quad i.j = 48.1, \\ 48'.1 & if \quad i.j = 48.2, \\ 51'.2 & if \quad i.j = 51.1, \\ 51'.1 & if \quad i.j = 51.2. \end{cases} .$$

For $n = 7$, the second map $f_{7,2} : E_{7,2} \to E'_{7,2}$ is given by

$$f_{7,2}(i.j) \quad = \quad \begin{cases} i.j & if\ i \notin \{12, 25, 38, 43\} \\ 12'.4 & if \quad i.j = 12.1, \\ 12'.7 & if \quad i.j = 12.2, \\ 12'.8 & if \quad i.j = 12.3, \\ 12'.1 & if \quad i.j = 12.4, \\ 12'.6 & if \quad i.j = 12.5, \\ 12'.5 & if \quad i.j = 12.6, \\ 12'.2 & if \quad i.j = 12.7, \\ 12'.3 & if \quad i.j = 12.8, \\ 25'.3 & if \quad i.j = 25.1, \\ 25'.4 & if \quad i.j = 25.2, \\ 25'.1 & if \quad i.j = 25.3, \\ 25'.2 & if \quad i.j = 25.4, \\ 38'.2 & if \quad i.j = 38.1, \\ 38'.1 & if \quad i.j = 38.2, \\ 43'.2 & if \quad i.j = 43.1, \\ 43'.1 & if \quad i.j = 43.2. \end{cases} \qquad .$$

For $n = 8$, the first map $f_{8,1} : E_{8,1} \to E'_{8,1}$ is given by

$$f_{8,1}(i.j) = \begin{cases} i'.j & if\ i \notin \{4, 11, 13, 14, 16, 29, 48, 51\} \\ 4'.3 & if \quad i.j = 4.1, \\ 4'.2 & if \quad i.j = 4.2, \\ 4'.1 & if \quad i.j = 4.3, \\ 4'.1 & if \quad i.j = 4.4, \\ 11'.3 & if \quad i.j = 11.1, \\ 11'.4 & if \quad i.j = 11.2, \\ 11'.1 & if \quad i.j = 11.3, \\ 11'.2 & if \quad i.j = 11.4, \\ 16'.4 & if \quad i.j = 16.1, \\ 16'.7 & if \quad i.j = 16.2, \\ 16'.8 & if \quad i.j = 16.3, \\ 16'.1 & if \quad i.j = 16.4, \\ 16'.6 & if \quad i.j = 16.5, \\ 16'.5 & if \quad i.j = 16.6, \\ 16'.2 & if \quad i.j = 16.7, \\ 16'.3 & if \quad i.j = 16.8, \\ 14'.j & if \quad i.j = 13.j, \\ 13'.j & if \quad i.j = 14.j, \\ 29'.3 & if \quad i.j = 29.1, \\ 29'.4 & if \quad i.j = 29.2, \\ 29'.1 & if \quad i.j = 29.3, \\ 29'.2 & if \quad i.j = 29.4, \\ 48'.2 & if \quad i.j = 48.1, \\ 48'.1 & if \quad i.j = 48.2, \\ 51'.2 & if \quad i.j = 51.1, \\ 51'.1 & if \quad i.j = 51.2. \end{cases} \qquad .$$

We have yet to investigate why the numbering is the same for $E_{6,1}, E_{7,1}$, and $E_{8,1}$. Note that MAGMA shows that the numbering of the minimal overgroups is not the same. Also, the cardinality of subgroup lattices of each are different. For

$n = 8$, the second map $f_{8,2} : E_{8,2} \to E'_{8,2}$ is given by

$$f_{8,2}(i.j) \quad = \quad \begin{cases} i.j & if\ i \notin \{12, 25, 36, 38\} \\ 12'.4 & if \quad i.j = 12.1, \\ 12'.7 & if \quad i.j = 12.2, \\ 12'.8 & if \quad i.j = 12.3, \\ 12'.1 & if \quad i.j = 12.4, \\ 12'.6 & if \quad i.j = 12.5, \\ 12'.5 & if \quad i.j = 12.6, \\ 12'.2 & if \quad i.j = 12.7, \\ 12'.3 & if \quad i.j = 12.8, \\ 25'.3 & if \quad i.j = 25.1, \\ 25'.4 & if \quad i.j = 25.2, \\ 25'.1 & if \quad i.j = 25.3, \\ 25'.2 & if \quad i.j = 25.4, \\ 36'.2 & if \quad i.j = 36.1, \\ 36'.1 & if \quad i.j = 36.2, \\ 38'.2 & if \quad i.j = 38.1, \\ 38'.1 & if \quad i.j = 38.2. \end{cases}$$

Appendix A

MAGMA code

We present the MAGMA code and PARI code used to carry out the computations for the results in Chapters 3, 4, and 5. We use MAGMA [3] version 2.11-9 and PARI [1] version 2.1.4.

A.1 Example One

Recall that in Chapter 3 we discussed a method that reduces the number of candidates for $G = Gal(k^{nr,2}/k)$ from 8 to 4. Whenever we demonstrate computations performed on a possibility for G, we use the candidate $C_{1,000}$ from Chapter 3. The computations for the other 7 candidates for G are similar.

The first step in the method was to show that G is an extension of D_4 by $C_2 \times C_8 \times C_{16}$. We first need to show that G contains the subgroup $C_2 \times C_8 \times C_{16}$. The following loop accomplishes this:

```
for i := 1 to 272 do
H:=Group(S_000!i);
    if (Index(C_000,H) le 8 and Length(Group(S_000!i)) eq 1 and IsAbelian(H)) then
        print ”K_”, i, “has abelianization”, AbelianQuotientInvariants(H);
    end if;
end for;.
```

The output is :

```
K_235 has abelianization [ 2, 8, 16].
```

Since MAGMA does not permit the use of commas in identifiers, “C000” throughout refers to $C_{1,000}$, and similarly for $C_{1,100}, C_{1,010}, \ldots$, etc. Note that S_{000} denotes the poset of conjugacy classes of subgroups of $C_{1,000}$. The output indicates that $C_{1,000}$ contains the subgroup $C_2 \times C_8 \times C_{16}$, and it is in the 235th subgroup class. In Chapter 3, we referred to this subgroup as K_{235}.

The next function gives the standard presentation of $C_{1,000}/K_{235}$:

```
StandardPresentation(C_000/Group(S_000!235));.
```

MAGMA outputs:

```
GrpPC of order 8
PC-Relations:
[x2, x1] = x2 * x3.
```

Recall that the standard presentation of a finite p-group is unique. We saw in Section 2.1 that this is the standard presentation of D_4, so that $C_{000}/K_{235} \cong D_4$. Similar results occur with the 7 other candidates. Therefore, G is an extension of D_4 by $C_2 \times C_8 \times C_{16}$.

Let $H \leq G$ denote the subgroup $C_2 \times C_8 \times C_{16}$. The next step is to compute a generating polynomial for the fixed field F^H of H. Recall from Chapter 3 that J denotes the subgroup fixing $E = \mathbb{Q}(\sqrt{-3}, \sqrt{13}, \sqrt{61})$, and that J is the unique normal subgroup of index 4 that has abelianization $C_4 \times C_4 \times C_8$. First, we show that H is a maximal subgroup of J by identifying in each candidate the subgroup that fixes E.

```
for i:=1 to 272 do
J:=Group(S_000!i);
   if (IsNormal(C_000,J) and Index(C_000,J) eq 4 and
      AbelianQuotientInvariants(J ) eq [4,4,8]) then
         print ”J is in subgroup class”, i;
   end if;
end for;.
```

The output is:

```
J is in subgroup class 260.
```

Let $J_{260} \leq C_{1,000}$ denote this subgroup. Next, we check if $K_{235} \leq J_{260}$:

```
S_000!235 le S_000!260;.
```

MAGMA outputs the Boolean:

```
true.
```

The next step is to compute a generating polynomial for F^H. Recall that we do this by computing the generating polynomials over $\mathbb{Q}$ of all quadratic subfields of $E^{(2)}/E$ (equivalently, all fields fixed by an index 2 subgroup of $Cl_E^{(2)}$). First, we compute the 2-class group of E, denoted below by g:

```
Q:=RationalField();
P<x>:=PolynomialRing(Q);
E:=NumberField([x^2 + 3, x^2 − 13, x^2 − 61]);
E:=AbsoluteField(E);
g,m:=ClassGroup(E);
g;.
```

The output is:

```
Abelian Group isomorphic to Z/4 + Z/4 + Z/8
Defined on 3 generators
Relations:
4*g.1 = 0
4*g.2 = 0
8*g.3 = 0.
```

This tells us that $Cl_E \cong C_4 \times C_4 \times C_8$ and is generated by $g.1, g.2, g.3$, of orders 4,4, and 8, respectively. Note that $Cl_E = Cl_E^{(2)}$.

Next, we compute the generating polynomial over $\mathbb{Q}$ of the fields fixed by an index 2 subgroup of $Cl_E^{(2)}$. For example, consider the subgroup $< g.1, g.2, 2 * g.3 >$

and let F denote its fixed field:

```
aE:=AbelianExtension(m);
q,mq:=quo<g|g.1,g.2,2*g.3>;
m2:=Inverse(mq)*m;
F:=AbelianpExtension(m2,2);
F:=NumberField(F);
F:=AbsoluteField(F);.
```

We apply this to each of the 7 index 2 subgroups of Cl_E.

Next, we compute the class groups of the fixed fields computed above. Recall from Chapter 3 that the field with 2-class group $C_2 \times C_8 \times C_{16}$ is F^H. The sequence of commands in PARI that computes a generating polynomial for F_2, for example, is:

```
p_2=y^16 + 338y^14 + 105445y^12 + 2973386y^10 + 77308156y^8
+ 2973386y^6 + 105445y^4 + 338y^2 + 1;
f=bnfinit(p_2);
f.clgp.
```

Recall that p_2 actually generates F^H.

Next, we compute the action of $Gal(F^H/k)$ on $Cl_{F^H}^{(2)}$. We begin by computing in PARI the automorphisms of F^H (not necessarily fixing k). Recall that $Gal(F^H/\mathbb{Q})$ has order 16. The command ”nfgaloisconj(f);” outputs the 16 automorphisms as a sequence of the Galois conjugates of a root α of p_2. The first step is to identify generators for $Gal(F^H/k)$. First, we check that an automorphism fixes k. The computation for the first automorphism is:

```
k=nfroots(f,x^2+2379);
a1:=nfgaloisconj[1];
nfgaloisapply(f,a1,k[1]).
```

We perform this for all 16 automorphisms.

Recall from Chapter 3 that the next step is to find $\sigma, \tau \in Gal(F^H/\mathbb{Q})$ of orders 4 and 2, respectively, such that $\sigma^2 \neq \tau$. For example, to see if $a1$ above is σ, we can check if $a1^2$ is the identity on the 3rd element ”f.nf.zk[3]” of the integral basis:

```
a1=nfgaloisconj[1];
nfgaloisapply(f, a1, nfgaloisapply(f,a1,f.nf.zk[3])).
```

Once we identify the 2 automorphisms of order 2, we only need to check that $\sigma^2 \neq \tau$. This is verified similarly to the above.

The last computation in PARI is to compute the action of $Gal(F^H/k)$ on Cl_{F^H}. Let $a1$ as above, and let $a4$ denote the fourth automorphism, “nfgaloisconj[4]”. To compute the image under $a1$ of the ideal class $g1$ of order 2, we use the sequence of commands:

```
g1=bnf.clgp.gen[1];
a1g1=nfgaloisapply(f,a1,g1);
bnfisprincipal(f,a1g1,0).
```

The next step is to compute the extensions resulting from the Galois action on Cl_{F^H}. The following program computes the extensions of D_4 by $C_2 \times C_8 \times C_{16}$ giving rise to the action δ in Example One.

```
D4 := PermutationGroup< 4|(1,2,3,4),(2,4)>;
M := [2,8,16];
T1 := Matrix(Integers(),3,3,[1,4,0,0,3,4,0,6,7]);
T2 := Matrix(Integers(),3,3,[1,4,8,0,3,4,0,0,1]);
CMP := CohomologyModule(D4,M,[T1,T2]);
H2 := CohomologyGroup(CMP,2);
print ”H2=”, H2;
dext:=DistinctExtensions(CM);
print ”# of Distinct Extensions=”, #dext;
end for;.
```

The output is:

```
H2=
Full Quotient RSpace of degree 3 over Integer Ring
Column moduli:
[ 2, 2, 2 ]
# of Distinct Extensions= 8.
```

Next, we identify which of the extension groups are candidates. To do so, we form the standard presentation of the ith extension, and compare it to each of the candidates.

```
for i:=1 to #dext do
E:=pQuotient(dext[i],2,0);
st:=StandardPresentation(E);
    if IsIdenticalPresentation(C_000,st) then
        print i, ”is C_000”;
    end if;
    if IsIdenticalPresentation(C_100,st) then
        print i, ”is C_100”;
    end if;
    if IsIdenticalPresentation(C_010,st) then
        print i, ”is C_010”;
    end if;
    if IsIdenticalPresentation(C_001,st) then
        print i, ”is C_001”;
    end if;
    if IsIdenticalPresentation(C_110,st) then
        print i, ”is C_110”;
    end if;
    if IsIdenticalPresentation(C_101,st) then
        print i, ”is C_101”;
    end if;
    if IsIdenticalPresentation(C_011,st) then
        print i, ”is C_011”;
    end if;
    if IsIdenticalPresentation(C_111,st) then
        print i, ”is C_111”;
    end if;
end for;
```

The output in MAGMA is:

```
2 is C_111
```

```
3 is C_011
6 is C_000
7 is C_100.
```

This tells us that extension 2 is $C_{1,111}$, extension 3 is $C_{1,011}$ etc. Therefore, the four candidates in $\mathcal{E}_0$ are $C_{1,000}, C_{1,100}, C_{1,011}$, and $C_{1,111}$.

To show that G is an extension of a group of order 32 by $C_8 \times C_{16}$, we proceed as we did with D_4 and $C_2 \times C_8 \times C_{16}$. We find in all candidates that $C_8 \times C_{16}$ is in subgroup class 201. Let $K_{201} \leq C_{1,000}$ denote this subgroup and Q denote $C_{1,000}/K_{201}$. We compute the action of Q on K_{201}:

```
g:=AbelianGroup(GrpPC,[8,16]);
flag,phi:=IsIsomorphic(g,K_201);
A:=sub<g—g.1,g.4>; Q,q :=quo<C_000—K_201>;
for i:= 1 to 2 do
    print ”The action of Q.1 on a_ ”, i, ”is”,
    X!((((Q.1@@q)*(phi(a.i))*(Q.1@@q)^(-1)))@@phi);
end for;
for i:=1 to 2 do
    print ”The action of Q.2 on X.”, i, ”is”,
    X!((((Q.2@@q)*(phi(a.i))*(Q.2@@q)^(-1)))@@phi);
end for;.
```

To compute the resulting set of extension groups, we proceed as we did above with the action of $Gal(F^H/k)$ on $Cl^{(2)}_{F^H}$.

A.2 Example Two

Recall that $C_{2,1}$ and $C_{2,2}$ denote the two possibilities for $G = Gal(k^{nr,2}/k)$. In the computations below, we denote these by “C_21” and “C_22”. We proceed as we did in Example One to show that $Gal(k^{nr,2}/k)$ is an extension of D_4 by $C_2 \times C_2 \times C_8$. Fix $i = 1, 2$. Recall that A_i denotes the subgroup of $C_{1,i}$ isomorphic to $C_2 \times C_2 \times C_8$, and that $Q_i = C_{1,i}/A_i \cong D_4$ for $i = 1, 2$. To compute the action of D_4 on A_i, we apply to $C_{2,i}$ the sequence of commands used with $C_8 \times C_{16}$ and Q in Section A.1. The loop used in Example One also computes $H^2(D_4, C_2 \times C_2 \times C_8)$ and corresponding extension groups. Recall that the set extension groups $\mathcal{E}_1$ and $\mathcal{E}_2$ are the same.

Recall that Chapter 4 also discusses differences between the subgroup posets and the number of elements of order 8 of $C_{2,1}$ and $C_{2,2}$. Computing the posets P_1 and P_2 of $C_{2,1}$ and $C_{2,2}$ requires the function ”SubgroupLattice”, which actually computes the poset of conjugacy classes of subgroups:

```
P_1:=SubgroupLattice(C_21);
P_2:=SubgroupLattice(C_22);.
```

The command “#P_i” indicates the number of elements in the poset of conjugacy classes of subgroups of P_i for $i = 1, 2$.

MAGMA represents the poset of conjugacy classes as a table, where the ith row of the table represents the ith conjugacy class. For example, recall from Chapter 4 that $C_{2,1}$ has 85 subgroup classes. Subgroup classes 82 through 84 contain the 3 maximal subgroups of $C_{2,1}$ (which each have order 128). Hence, for example, row 82 represents the 82nd conjugacy class. MAGMA further represents subgroup class 82 in the following way:

```
[82]   Order 128         Length 1   Maximal Subgroups: 76  78
```

The portion “Length 1” indicates that there is a single subgroup in subgroup class 82. Recall from Chapter 5 that 82.1 is our notation for this subgroup. Hence, 82.1 is one of the 3 maximal subgroups of $C_{2,1}$ referred to above, and the 2 are 83.1 and

84.1. The portion “Maximal Subgroups: 76 78” indicates that the subgroups in classes 76 and 78 are the maximal subgroups of 82.1.

To find the the number of elements of order 8 in $C_{2,1}$, we use the loop:

```
S:=[];
for x in C_21 do
      if Order(x) eq 8 then
         Append( S,x);
      end if;
end for;
print #S;.
```

We apply this loop to $C_{2,2}$ to see that the 2 groups have different numbers of elements of order 8.

A.3 Example Three

Recall that $C_{3,1}$ and $C_{3,2}$ denote the candidates for $G = Gal(k^{nr,2}/k)$. To show that G is an extension of D_4 by $C_2 \times C_2 \times C_{16}$, we use the loops presented in Section A.1. To compute the resulting second cohomology group and sets $\mathcal{E}_1$ and $\mathcal{E}_2$ of extension groups, we also use the loops given in Section A.1.

Next, we test if the subgroup posets P_1 and P_2 of $C_{3,1}$ and $C_{3,2}$ are order-isomorphic. First, we easily check that $\#P_1 = \#P_2$ (recall that computing each of these numbers were explained in Section A.2). Next, we verify that P_1 and P_2 are order-isomorphic:for i:= 1 to P_1 do

```
    for j:= 1 to P_1 do
      if (P_1!i le P_1!j) ne (P_2!i le P_2!j) then
          print i,j, ”fails”;
      end if;
    end for;
end for;.
```

When we run this loop, there is no output. Therefore, $i \leq j$ in P_1 if and only if $i' \leq j'$ in P_2. Recall from Chapter 5 that this shows that the map $\tilde{h} : P_1 \to P_2$ given by $i \mapsto i'$ is an order-isomorphism.

The next 4 loops enable us to construct a lattice isomorphism $f : L_1 \to L_2$, where L_i denote the subgroup lattice of $C_{3,i}$ for $i = 1, 2$. Recall from Section 5.2 that $\#P_1 = \#P_2 = 95$. Also recall that for all $1 \leq i \leq 94$, subgroup class i in P_1 contains the same number of subgroups as class i' in L_2 and that the subgroups in class i are of the same isomorphism type as those in class i'. The first loop compares the lengths of conjugacy classes:

```
for i:= 1 to #P_1 do
    if Length(P_1!i) ne Length(P_2!i) then
      print i, ”fails”;
    end if;
end for;.
```

Recall that f is such that corresponding proper subgroups and quotients are isomorphic. The loop that tests if subgroups in corresponding conjugacy classes are isomorphic is given by:

```
for i:= 2 to #P_1 do
    stpr1:=StandardPresentation(Group(P_1!i));
    stpr2:=StandardPresentation(Group(P_2!i));
        if IsIdenticalPresentation(stpr1,stpr2) eq false then
            print i, ”fails”;
        end if;
end for;.
```

The loop that tests if corresponding quotients are isomorphic is given by:

```
for i:= 2 to #P_1 do
     if Length(P_1!i) eq 1 then
         stpr1:=StandardPresentation(C_21/Group(P_1!i));
         stpr2:=StandardPresentation(C_22/Group(P_2!i));
               if IsIdenticalPresentation(stpr1,stpr2) eq false then
                    print i, ”fails”;
               end if;
     end if;
end for;.
```

When either one of the above 3 loops is run, there is no output thereby indicating that f has the properties we claim.

The last of the 4 loops is as followed. Recall that $i.j$ represents the jth subgroup in the ith conjugacy class of $C_{3,1}$ and $i'.j$ represents the jth subgroup in the ith conjugacy class of $C_{3,2}$. We test whether or not

$$\tilde{h} : i.j \mapsto i'.j$$

is an order-isomorphism:

```
for i:=1 to #P_1 do
    for j:=1 to #P_2 do
        if P_1!i le P_1!j then
           C:=SetToIndexedSet(Class(C_21,Group(P_1!i)));
           D:=SetToIndexedSet(Class(C_22,Group(P_2!i)));
           E:=SetToIndexedSet(Class(C_21,Group(P_1!j)));
           F:=SetToIndexedSet(Class(C_22,Group(P_2!j)));
               for k:=1 to #C do
               for l:=1 to #E do
               if (C[k] subset E[l]) ne (D[k] subset F[l]) then
                  print i,k,j,l, ”fails”;
               end if;
               end for;
           end for;
        end if;
    end for;
end for;.
```

Recall from Section 5.2 that $\tilde{h}$ fails to be an order-isomorphism only on subgroup classes $3, 3', 12$, and $12'$. Also recall that class 3 contains 2 subgroups and class 12 contains 8 subgroups. The output indicates the failure of $\tilde{h}$ on these classes:

```
3 1 12 1 fails
3 1 12 2 fails
3 1 12 3 fails
3 1 12 4 fails
3 1 12 5 fails
3 1 12 6 fails
3 1 12 7 fails
3 1 12 8 fails
3 2 12 1 fails
3 2 12 2 fails
3 2 12 3 fails
3 2 12 4 fails
3 2 12 5 fails
3 2 12 6 fails
3 2 12 7 fails
3 2 12 8 fails
```

The first line, for example, indicates that either $3.1 \leq 12.1$ in $C_{3,1}$ and $3'.1 \not\leq 12'.1$ in $C_{3,2}$ or vice versa. The actual containments for the subgroups in classes $3, 12$ and $3', 12'$ are given in Section 5.2.

From there, we construct the lattice isomorphism f. Recall that we utilized maximal subgroup information in order to do so. To compute maximal subclasses of subgroup class i, we type "MaximalSubgroups(i)"; to compute the subgroup classes containing the minimal overgroups of i, we type "MinimalOvergroups(i)". To determine specific containment among the subgroups in class i and j, we use the loop below. For example, in $E_{7,2}$ we find that class 12 is a maximal subclass of 25. Let P_{72} denote the subgroup poset of $E_{7,2}$. The loop determining containment for subgroup classes 12, 25 is given by:

```
S:={12, 25};
for i in S do
C:=SetToIndexedSet(Class(E_72,Group(P_72!i)));
    for j in [1..#P72] do
         if P_72!j in MaximalSubgroups(P_72!i) then
              D:=SetToIndexedSet(Class(E_72,Group(P_72!j)));
              for k in [1..#C] do
                   for l in [1..#D] do
                        if D[l] subset C[k] then
                             print j “.” l, “is maxl subg of”, i,”.” k, ”;
                        end if;
                   end for;
              end for;
         end if;
    end for;
end for;
```

The output is:

```
12.1 is maxl subg of 25.1
12.5 is maxl subg of 25.1
12.2 is maxl subg of 25.2
12.3 is maxl subg of 25.2
12.4 is maxl subg of 25.3
12.6 is maxl subg of 25.3
12.7 is maxl subg of 25.4
12.8 is maxl subg of 25.4.
```

This indicates the following containment in $E_{7,2}$:

$$12.1, 12.5 \leq 25.1, \quad 12.2, 12.3 \leq 25.2, \quad 12.4, 12.6 \leq 25.3, \quad 12.7, 12.8 \leq 25.4.$$

Recall in Sections 5.3 and 5.4 that we investigate various properties of the set $\mathcal{E}_n$ of extension groups giving rise to the action $\circ_n$. We compute group cohomology and extension groups as we did in Section A.1. To show that a pair of groups have isomorphic subgroup lattices such that corresponding proper subgroups and proper quotients are isomorphic, we use the same sequence of loops used above for $C_{3,1}$ and $C_{3,2}$.

For the results pertaining to the generation of the extension groups, we compute the exponent-2 central series of the Frattini-quotient rank 2 groups. For example, to show that $E_{6,1}$ and $E_{7,1}$ are identical through the fourth iteration of the p-group generation algorithm we use:

```
pcs61:=pCentralSeries(E_61,2);
pcs71:=pCentralSeries(E_71,2);
    for i:=1 to #pcs61 do
       g:=StandardPresentation(E_61/pcs61[i]);
       h:=StandardPresentation(E_71/pcs71[i]);
            if IsIdentical(g,h) eq false then
              print i;
            end if;
    end for;.
```

The other results relating to the generation of the extensions are obtained similarly.

At the end of Chapter 5, we predict the presentations of the index 2 subgroups of a Frattini-quotient-rank-2 group. For this, we use the sequence of commands located below. Consider $E_{5,1}$, for example. Let $P_{5,1}$ denote the poset of conjugacy classes of subgroups of $E_{5,1}$. We find that the maximal subgroups of $E_{5,1}$ are the groups in subgroup classes 92,93, and 94. We compute the standard presentations of each to reveal the patterns described in Chapter 5:

```
M511:=StandardPresentation(Group(P_51!92));
M512:=StandardPresentation(Group(P_51!93));
M513:=StandardPresentation(Group(P_51!94));.
```

BIBLIOGRAPHY

[1] C. Batut, K. Belabas, D. Bernardi, H. Cohen, M. Olivier, *User's Guide to PARI GP*, Université Bordeaux, Cedex, France, 1999.

[2] E. Benjamin, F. Lemmermeyer, C. Snyder, *Imaginary quadratic fields with* $Cl_2(k) \cong (2,2,2)$, J. Number Theory, **103**, no.1 (2003), 38-70.

[3] W. Bosma, J.J. Cannon, *Handbook of MAGMA Functions*, School of Mathematics and Statistics, University of Sydney, Sydney, 1995.

[4] N. Boston, C. Leedham-Green, *Explicit Computation of Galois p-groups unramified at p*, J. Algebra, **256** no.2, (2002), 402-413.

[5] M. Bush, *Computation of Galois groups associated to the 2-class towers of some quadratic fields*, J. Number Theory, **100**, no. 2 (2003), 313-325.

[6] Gerth, F. *A density result for some imaginary quadratic fields with infinite Hilbert* 2*-class field towers*, Arch. Math. (Basel), **82**, no.1 (2004) /23-27.

[7] F. Hajir, *On a Theorem of Koch*, Pacific J. Math., **176**, no. 1 (1996), 15-18.

[8] B.A. Davey, H.A. Priestly, *Introduction to Lattices and Order*, Cambridge University Press, Cambridge, 2002.

[9] M.F. Newman, "Determination of groups of prime-power order", *Group Theory* (Canberra 1975), 73-84, Lecture Notes in Math., **573**, Springer-Verlag, Berlin, Heidelberg, New York.

[10] E.A. O'Brien, *The p-group generation algorithm*, J. Symbolic Comput., **9**, no.5-6 (1990), 677-698.

[11] E.A. O'Brien *Isomorphism Testing for p-Groups*, J. Symbolic Comput., **16** (1993), no.3, 305-320.

[12] P. Roquette, *On class field towers*, 231-249, in: Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965), J. Cassels and A. Fröhlich (Eds), Academic Press, San Diego, 1980.