2015-06-01

Octahedral Extensions and Proofs of Two Conjectures of Wong

Kevin Ronald Childers
Brigham Young University - Provo

Octahedral Extensions and Proofs of Two Conjectures of Wong

Kevin Ronald Childers

A thesis submitted to the faculty of
Brigham Young University
in partial fulfillment of the requirements for the degree of

Master of Science

Darrin Doud, Chair
Pace Nielsen
David Cardon

Department of Mathematics

Brigham Young University

June 2015

ABSTRACT

Octahedral Extensions and Proofs of Two Conjectures of Wong

Kevin Ronald Childers
Department of Mathematics, BYU
Master of Science

Consider a non-Galois cubic extension $K/\mathbb{Q}$ ramified at a single prime $p > 3$. We show that if K is a subfield of an S_4-extension $L/\mathbb{Q}$ ramified only at p, we can determine the Artin conductor of the projective representation associated to $L/\mathbb{Q}$, which is based on whether or not $K/\mathbb{Q}$ is totally real. We also show that the number of S_4-extensions of this type with K as a subfield is of the form $2^n - 1$ for some $n \geq 0$. If $K/\mathbb{Q}$ is totally real, $n > 1$. This proves two conjectures of Siman Wong.

Keywords: octahedral, Galois representations, number fields

Contents

List of Tables

List of Figures

Chapter 1. Introduction

This thesis is mostly concerned with **octahedral extensions**, which are Galois extensions of number fields with Galois group isomorphic to S_4, the group of symmetries of the octahedron. We will develop relationships between the S_4-extensions and their cubic subfields. Our main goal will be to prove the following two conjectures made by Siman Wong in [27].

Conjecture 1.1. *Let $K/\mathbb{Q}$ be a quartic number field with S_4-Galois closure ramified at a single prime $p > 3$. Let $K_3/\mathbb{Q}$ be a cubic subfield of the Galois closure of $K/\mathbb{Q}$. Let $\tilde{\rho}$ be the projective 2-dimensional Artin representation associated to $K/\mathbb{Q}$.*

(i) Suppose $K_3/\mathbb{Q}$ is totally real. If $\tilde{\rho}$ has conductor p^2, then $v_p(\mathrm{disc}(K)) = 1$.

(ii) Suppose $K_3/\mathbb{Q}$ is not totally real. If $\tilde{\rho}$ has conductor p^2 then $v_p(\mathrm{disc}(K)) = 3$, otherwise $v_p(\mathrm{disc}(K)) = 1$.

Conjecture 1.2. *Let $K/\mathbb{Q}$ be a non-Galois cubic extension such that $|\mathrm{disc}(K)|$ is a prime power. Then the number of S_4-extensions $L/\mathbb{Q}$ containing K with $|\mathrm{disc}(L)|$ a prime power is $2^n - 1$ for some integer n. Furthermore, if $K/\mathbb{Q}$ is totally real, then $n > 0$.*

In Chapter 2, we will give necessary background definitions and results in the subjects of number fields, Galois representations, and group cohomology. In Section 2.1 we will discuss number rings, factorization of primes, basic class field theory, some Galois theory of number fields, and Dirichlet's Unit Theorem. Section 2.2 contains necessary definitions for Galois representations, such as the conductor, and we also discuss ramification groups. In Section 2.3 we define cohomology of groups, give basic results, and discuss the Hochschild-Serre spectral sequence.

Chapter 3 is devoted to the proof of Conjecture 1.1, which is restated as Theorem 3.1. Our treatment relies heavily on results of Serre's 1977 paper [21]. We have published these results separately as [4].

In Chapter 4 we will prove Conjecture 1.2, restated as Theorem 4.5, and several related results. For instance, we will prove a generalization to the first part of Conjecture 1.2 which

holds for ramification at more primes and for an arbitrary base number field as Theorem 4.6. The proof relies on showing that the S_4-extensions are the non-identity elements of an elementary abelian 2-group, C_2^n (here we are using the notation C_m to denote the cyclic group of order m). We also give examples of various values of n occurring (in the context of Conjecture 1.2 or Theorem 4.6), as well as explicit examples of the group operation.

Chapter 2. Background

2.1 Number Fields

Our main results all consider extensions of number fields. This section briefly states the important definitions and results that we will need throughout.

2.1.1 Number fields. By a **number field**, we mean a subfield of $\mathbb{C}$ which is a finite extension of the rational numbers $\mathbb{Q}$. For two number fields K and F, K/F means that K is an extension of F. We will denote the degree of K as an F-vector space by $[K : F]$. If $[K : F] = n$, then there are n embeddings $K \to \mathbb{C}$ which restrict to the identity on F, see [17, pg 259].

An **algebraic integer** is a number $\alpha \in \mathbb{C}$ which is a root of a monic polynomial in $\mathbb{Z}[x]$. The set of algebraic integers in a number field K forms a ring [17, pg 16], called the **ring of integers of** K. We denote this ring by $\mathfrak{O}_K$. Notice that $\mathbb{Z} \subset \mathfrak{O}_K$, and $\mathfrak{O}_K \cap \mathbb{Q} = \mathbb{Z}$.

Definition 2.1. ([17, pg 55]) A **Dedekind domain** is an integral domain R which satisfies

(i) Every ideal is finitely generated (R is Noetherian),

(ii) Every nonzero prime ideal is maximal (R has Krull dimension 1),

(iii) R is integrally closed in its field of fractions K.

Condition (iii) means that that for a root α of a monic polynomial in $R[X]$, $\alpha \in K$ implies $\alpha \in R$. The ring $\mathfrak{O}_K$ is a Dedekind domain for any number field K, see [17, pg 56]. In general, a Dedekind domain is not a unique factorization domain. However, Dedekind domains always have unique factorization *of ideals*.

2.1.2 Factorization of ideals.

Theorem 2.2 ([17, pg 59])**.** *Let R be a Dedekind domain, and $\mathfrak{a}$ an ideal of R. Then $\mathfrak{a}$ can be written uniquely as a product of prime ideals of R,*

$$\mathfrak{a} = \mathfrak{p}_1^{v_{\mathfrak{p}_1}(\mathfrak{a})} \cdots \mathfrak{p}_r^{v_{\mathfrak{p}_r}(\mathfrak{a})}$$

This implies that for a prime ideal $\mathfrak{p}$, we have a well defined function $v_\mathfrak{p}$ defined on ideals of R. It takes in an ideal and returns the exponent of $\mathfrak{p}$ in the factorization (0 if $\mathfrak{p}$ does not appear in the factorization). We can also define $v_\mathfrak{p}$ on elements, by allowing $v_\mathfrak{p}(\alpha)$ to equal $v_\mathfrak{p}(\mathfrak{a})$ where $\mathfrak{a} = \alpha R$.

Factorization of ideals is especially interesting for extensions of number fields. Let K/F be an extension of number fields, and $\mathfrak{p}$ a prime ideal of F (this means "$\mathfrak{p}$ is a non-zero prime of $\mathfrak{O}_F$"). Then $\mathfrak{p}\mathfrak{O}_K$ is an ideal of $\mathfrak{O}_K$, so it has a unique factorization into prime ideals of $\mathfrak{O}_K$,

$$\mathfrak{p}\mathfrak{O}_K = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}.$$

We call the $\mathfrak{P}_i$'s **primes lying over** $\mathfrak{p}$, and $\mathfrak{p}$ the **prime lying below** $\mathfrak{P}_i$. We call e_i the **ramification index** of $\mathfrak{P}_i \mid \mathfrak{p}$, see [17, pg 64]. We say that $\mathfrak{p}$ **ramifies in** K if any of the e_i's are greater than 1.

For any prime $\mathfrak{P}$ of K, $\mathfrak{O}_K/\mathfrak{P}$ is a finite field of characteristic p (where (p) is the prime ideal of $\mathbb{Z}$ lying below $\mathfrak{P}$), see [17, pg 56]. Therefore we have a field extension $(\mathfrak{O}_K/\mathfrak{P})/(\mathbb{Z}/p)$. More generally, if K/F is an extension of number fields, and $\mathfrak{P}$ is a prime of K lying over a prime $\mathfrak{p}$ of F, then $(\mathfrak{O}_K/\mathfrak{P})/(\mathfrak{O}_F/\mathfrak{p})$ is an extension of finite fields, see [17, pg 64]. We call the degree of this extension the **inertial degree** of $\mathfrak{P} \mid \mathfrak{p}$.

Theorem 2.3 ([17, pg 65])**.** *Let K/F be an extension of number fields, and let $\mathfrak{p}$ be a prime of F. Suppose that $\mathfrak{p}\mathfrak{O}_K$ has prime factorization*

$$\mathfrak{p}\mathfrak{O}_K = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$$

in K. Let f_i denote the inertial degree of $\mathfrak{P}_i \mid \mathfrak{p}$. Then

$$\sum_{i=1}^{r} e_i f_i = [K : F].$$

Suppose that K/F is a Galois extension of number fields and $\mathfrak{p}$ is a prime of F. If $\mathfrak{P}, \mathfrak{P}'$ are both primes of K lying over $\mathfrak{p}$, then $\mathfrak{P}$ and $\mathfrak{P}'$ have the same ramification indexes e and inertial degrees f by [17, pg 71]. If r is the number of distinct primes of K lying over $\mathfrak{p}$, then Theorem 2.3 reduces to

$$efr = [K : F].$$

in this case. Three special cases are:

(i) $e = [K : F]$ and $f = r = 1$. In this case we say that $\mathfrak{p}$ is **totally ramified** in K/F.

(ii) $f = [K : F]$ and $e = r = 1$. In this case we say that $\mathfrak{p}$ is **inert** in K/F.

(iii) $r = [K : F]$ and $e = f = 1$. In this case we say that $\mathfrak{p}$ **splits completely** in K/F.

2.1.3 The discriminant. An important invariant of a number field is the discriminant, which we now define.

Definition 2.4. ([17, pg 24]) Let K be a number field of degree n. Let $\sigma_1, \cdots, \sigma_n$ denote the n embeddings of $K \to \mathbb{C}$. Let $\alpha_1, \ldots, \alpha_n \in K$. Then the **discriminant of the n-tuple** $(\alpha_1, \ldots, \alpha_n)$ is defined as

$$\operatorname{disc}(\alpha_1, \ldots, \alpha_n) = \det([\sigma_i(\alpha_j)])^2.$$

The ring $\mathfrak{O}_K$ is always a free abelian group of rank n by [17, pg 30]. In other words, there exist algebraic integers $\alpha_1, \ldots, \alpha_n \in K$ called an **integral basis for $\mathfrak{O}_K$** (see [17, pg 30]) so that every $\alpha \in \mathfrak{O}_K$ is uniquely representable in the form

$$\alpha = m_1\alpha_1 + \cdots + m_n\alpha_n \qquad \text{with } m_i \in \mathbb{Z}.$$

It is also a fact that the discriminant of an integral basis for $\mathfrak{O}_K$ is an invariant of $\mathfrak{O}_K$.

Theorem 2.5 ([17, pg 32])**.** *Let K be a number field of degree n over $\mathbb{Q}$. If $\alpha_1 \ldots, \alpha_n$ and $\beta_1, \ldots, \beta_n$ are two integral bases for $\mathfrak{O}_K$, then*

$$\operatorname{disc}(\alpha_1, \ldots, \alpha_n) = \operatorname{disc}(\beta_1, \ldots, \beta_n).$$

Therefore we define the **discriminant of** K to be the discriminant of any integral basis for $\mathfrak{O}_K$, denoted $\operatorname{disc}(K)$. Notice that $\operatorname{disc}(K) \in \mathbb{Q}$, since it is fixed by any embedding of $K \to \mathbb{C}$. In fact, $\operatorname{disc}(K) \in \mathbb{Z}$, since all entries of the matrix are algebraic integers. A remarkable and useful fact about $\operatorname{disc}(K)$ is the following theorem.

Theorem 2.6 ([19, pg 202])**.** *Let K be a number field. Then a prime $p \in \mathbb{Z}$ ramifies in K if and only if $p \mid \operatorname{disc}(K)$.*

One consequence of this theorem is that only a finite number of primes can ramify in a given number field. A useful theorem for determining factorizations of primes is the following.

Theorem 2.7 ([6, pg 99])**.** *Let K/F be an extension of number fields of degree n. Choose $\alpha \in K$ of degree n, so that $K = F(\alpha)$. Let $g(x) \in \mathfrak{O}_F[x]$ be the minimal polynomial of α. Fix a prime $\mathfrak{p}$ of F, and let p be the prime of $\mathbb{Z}$ lying below $\mathfrak{p}$. Assume that $p \nmid [\mathfrak{O}_K : \mathfrak{O}_F[\alpha]]$. Assume that $g(x)$ factors as*

$$g(x) \equiv g_1(x)^{e_1} \cdots g_r(x)^{e_r} \pmod{\mathfrak{p}}.$$

Let $f_i = \deg g_i(x)$. Then the prime factorization of $\mathfrak{p}\mathfrak{O}_K$ is given by

$$\mathfrak{p}\mathfrak{O}_K = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r},$$

where $\mathfrak{P}_i = (\mathfrak{p}, g_i(\alpha))$, and $\mathfrak{P}_i \mid \mathfrak{p}$ has inertial degree f_i.

2.1.4 Infinite primes. Thus far the primes we have discussed are the *finite* primes of K. We can also talk about the *infinite* primes of K, which are the embeddings $K \to \mathbb{C}$, see

[7, pg 94]. Let K/F be an extension of number fields. Let τ be an embedding of $K \to \mathbb{C}$. Then $\sigma = \tau|_F$ is an embedding of $F \to \mathbb{C}$, and we say τ **lies over** σ, or σ **lies below** τ.

An embedding $\sigma : K \to \mathbb{C}$ is a **real embedding** if $\sigma(K) \subset \mathbb{R}$, and is non-real otherwise. If σ is a non-real embedding, then the composition of σ with complex conjugation is also a non-real embedding. We consider a non-real embedding to be "the same" as its complex conjugate. If all embeddings of K are real, then we say that K is a **totally real** number field. If τ lies above σ, with σ real and τ non-real, then we say that σ **ramifies**, with ramification index 2, see [7, pg 94]. In any other case, the ramification index of τ over σ is 1. There is no analogue of inertial degree for infinite primes.

Suppose that σ is an infinite prime of F. Let $\sigma_1, \ldots, \sigma_{r_1}$ be the real embeddings of K over σ and $\tau_1, \overline{\tau}_1, \cdots, \tau_{r_2}, \overline{\tau}_{r_2}$ be the non-real embeddings of K over σ. Then $r_1 + 2r_2 = [K : F]$, which is an analogue of Theorem 2.3.

2.1.5 Hilbert and narrow class fields. For an extension to be unramified, it must not ramify at any primes, finite or infinite. The only unramified extension of $\mathbb{Q}$ is itself by [6, pg 198]. It is a fact that the composite of all *abelian* unramified extensions of K is a number field (see [7, pg 148]), called the **Hilbert class field of** K. Its degree over K is called the **class number**. The Galois group of this extension can be identified by class field theory (see [19, Ch VI]) as the group of equivalence classes of ideals of $\mathfrak{O}_K$ modulo principal ideals of $\mathfrak{O}_K$. The group operation is multiplication of ideals, see [19, pg 22].

The **narrow class field of** K is the composite of all abelian extensions which are unramified at all finite primes, and the **narrow class number of** K is the degree of this extension. The Galois group of this extension is identified by class field theory with the group of ideals modulo **totally positive** principal ideals. A totally positive principal ideal is an ideal that has a generator α for which $\sigma(\alpha) > 0$ for all real embeddings $\sigma : K \to \mathbb{R}$, see [8, pg 180].

2.1.6 Galois theory of number fields. Let K/F be a Galois extension of number fields, and G the Galois group. We will make use of the following subgroups of G.

Definition 2.8. ([17, pg 98]) Let $\mathfrak{p}$ be a prime of F and $\mathfrak{P}$ a prime of K lying over $\mathfrak{p}$.

(i) The **decomposition group** of $\mathfrak{P} \mid \mathfrak{p}$ is defined as

$$D = \{\sigma \in G : \sigma(\mathfrak{P}) = \mathfrak{P}\}.$$

(ii) The **inertia group** of $\mathfrak{P} \mid \mathfrak{p}$ is defined as

$$I = \{\sigma \in G : \sigma(\alpha) \equiv \alpha \bmod \mathfrak{P} \text{ for all } \alpha \in \mathfrak{O}_K\}.$$

By reducing mod $\mathfrak{P}$, the elements of D induce automorphisms of $\mathfrak{O}_K/\mathfrak{P}$ fixing $\mathfrak{O}_F/\mathfrak{p}$, and we obtain a homomorphism $D \to \mathrm{Gal}((\mathfrak{O}_K/\mathfrak{P})/(\mathfrak{O}_F/\mathfrak{p}))$. This map is surjective and has kernel I by [17, pg 99], therefore

$$D/I \cong \mathrm{Gal}((\mathfrak{O}_K/\mathfrak{P})/(\mathfrak{O}_F/\mathfrak{p})) \cong C_f,$$

where f is the inertial degree of $\mathfrak{P} \mid \mathfrak{p}$. We have that $|I| = e$ by [17, pg 100], where e is the ramification index of $\mathfrak{P} \mid \mathfrak{p}$, so $|D| = ef$. The fixed field of D is called the **decomposition field**, and the fixed field of I is called the **inertia field**, see [17, pg 99]. These fields have the following properties.

Theorem 2.9 ([17, pg 104])**.** *Let K/F be a Galois extension of number fields, $\mathfrak{P}$ a prime of K, and $\mathfrak{p}$ the prime of F lying below $\mathfrak{P}$. Let F' be a subextension of K/F, and $\mathfrak{p}'$ the prime of F' lying below $\mathfrak{P}$.*

(i) The decomposition field is the largest F' such that both the inertial degree and the ramification index of $\mathfrak{p}' \mid \mathfrak{p}$ are equal to 1.

(ii) The decomposition field is the smallest F' such that $\mathfrak{P}$ is the only prime lying over $\mathfrak{p}'$.

(iii) The inertia field is the largest F' such that the ramification index of $\mathfrak{p}' \mid \mathfrak{p}$ is 1.

(iv) The inertia field is the smallest F' such that $\mathfrak{P}$ is totally ramified over $\mathfrak{p}'$.

When $\mathfrak{P} \mid \mathfrak{p}$ is unramified, I is trivial, therefore $D \cong \mathrm{Gal}((\mathfrak{O}_K/\mathfrak{P})/(\mathfrak{O}_F/\mathfrak{p}))$, where the right side is generated by the Frobenius automorphism $\alpha \mapsto \alpha^p$, see [10, pg 288]. We call the corresponding generator of D the **Frobenius automorphism of $\mathfrak{P} \mid \mathfrak{p}$** (see [17, pg 109]), and denote this element of D by φ. It satisfies

$$\varphi(\alpha) \equiv \alpha^{|\mathfrak{O}_F/\mathfrak{p}|} \pmod{\mathfrak{P}} \text{ for all } \alpha \in \mathfrak{O}_K, \text{ see [17, pg 108].}$$

By [17, pg 109], all Frobenius automorphisms for primes over $\mathfrak{p}$ of F are conjugate. We will define a Frobenius automorphism φ of $\mathfrak{p}$ to be any Frobenius automorphism of a prime over $\mathfrak{p}$, which is well defined up to conjugacy.

2.1.7 Dirichlet's Unit Theorem. We will also need a basic understanding of the units of $\mathfrak{O}_K$ for a number field K.

Theorem 2.10 (Dirichlet's Unit Theorem, see [17, pg 142])**.** *Let K be a number field. Let r_1 denote the number of real embeddings of K and r_2 the number of pairs of non-real embeddings of K. Then*

$$\mathfrak{O}_K^\times \cong \mathbb{Z}^{r_1+r_2-1} \times V,$$

where V is the finite cyclic group consisting of the roots of unity in K.

2.2 Galois representations

The main theorem of Chapter 3 is a result about certain Galois representations. This section develops the basic theory that we need. Let $\overline{\mathbb{Q}}$ denote an algebraic closure of $\mathbb{Q}$, and let $G_\mathbb{Q} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. The group $G_\mathbb{Q}$ is a profinite group, which means that it is a compact,

Hausdorff topological space under the Krull topology, see [18, pg 2]. Thus by [18, pg 4] we can write $G_{\mathbb{Q}}$ as a limit over its normal subgroups of finite index:

$$G_{\mathbb{Q}} = \varprojlim G_{\mathbb{Q}}/N = \varprojlim \mathrm{Gal}(K/\mathbb{Q}),$$

where K runs through finite Galois extensions of $\mathbb{Q}$.

2.2.1 Galois representations. Let V be an $\mathbb{F}$-vector space. When $\mathbb{F}$ has a topology, we can think of $\mathrm{GL}(V)$ as a subspace of $\mathbb{F}^{n^2}$.

Definition 2.11. A **Galois representation** is a continuous homomorphism

$$\rho : G_{\mathbb{Q}} \to \mathrm{GL}(V).$$

The **dimension** of ρ is just the dimension of V. All Galois representations we consider will have dimension 2, meaning that the codomain is $\mathrm{GL}(V)$ where $V \cong \mathbb{F}^2$. Sometimes we talk about V as the representation, instead of ρ. By this we mean to consider V as an $\mathbb{F}G_{\mathbb{Q}}$-module, where the $G_{\mathbb{Q}}$ action is achieved via ρ.

Let $\tau \in G_{\mathbb{Q}}$ denote the automorphism of complex conjugation. We say a Galois representation $\rho : G_{\mathbb{Q}} \to \mathrm{GL}(V)$ is **odd** if $\rho(\tau)$ is a nonscalar matrix, see [21, Sec 1]. We say ρ is **even** otherwise.

2.2.2 Ramification groups.

Definition 2.12. ([19, pg 168]) Let K/F be a Galois extension of number fields, and let $\mathfrak{P}$ be a prime of $\mathfrak{O}_K$. Let $\mathfrak{p}$ be the prime of F lying below $\mathfrak{P}$. For $i \geq 0$, define the i**th ramification group of** $\mathfrak{P} \mid \mathfrak{p}$ to be

$$G_i = \{\sigma \in \mathrm{Gal}(K/F) : \sigma(\alpha) \equiv \alpha \bmod \mathfrak{P}^{i+1} \text{ for all } \alpha \in \mathfrak{O}_K\}.$$

The ramification groups G_i form a decreasing chain of normal subgroups of D, with

$G_0 = I$, the inertia group. Only finitely many G_i are non-trivial by [22, pg 62]. If G_1 is trivial, we say that $\mathfrak{P} \mid \mathfrak{p}$ is **tamely ramified**. Otherwise, we say that $\mathfrak{P} \mid \mathfrak{p}$ is **wildly ramified**, see [8, pg 145].

The following results about ramification groups are proved in [19] in terms of valuations and in [22] for local fields. For number fields, they are left as exercises in [17], so we provide proofs of them here. We follow the exercises given in [17, pg 122–123]. For the remainder of the subsection, let K/F be a Galois extension of number fields, $\mathfrak{P}$ a prime of K, $\mathfrak{p}$ the prime of F lying below $\mathfrak{P}$, and p the prime of $\mathbb{Z}$ lying below $\mathfrak{P}$. Let G_i denote the ramification groups of $\mathfrak{P} \mid \mathfrak{p}$. Fix $\pi \in \mathfrak{O}_K$ with $v_{\mathfrak{P}}(\pi) = 1$.

Proposition 2.13. *For $\sigma \in G_{i-1}$, $\sigma \in G_i$ if and only if $\sigma(\pi) \equiv \pi \pmod{\mathfrak{P}^{i+1}}$.*

Proof. The forwards implication is trivial. We will prove the reverse implication in three stages. Assume that $\sigma \in G_{i-1}$ for some $i \geq 1$ and also assume $\sigma(\pi) \equiv \pi \pmod{\mathfrak{P}^{i+1}}$.

Case 1. Suppose $\alpha \in \pi\mathfrak{O}_K$. Write $\alpha = \pi\beta$ with $\beta \in \mathfrak{O}_K$. Since $\sigma \in G_{i-1}$,

$$\sigma(\beta) \equiv \beta \pmod{\mathfrak{P}^i},$$

and we can write $\sigma(\beta) = \beta + \pi'$ with $\pi' \in \mathfrak{P}^i$. We have

$$\sigma(\alpha) \equiv \sigma(\beta\pi) \equiv \sigma(\beta)\sigma(\pi) \equiv (\beta + \pi')\pi \equiv \beta\pi + \pi'\pi \equiv \alpha + 0 \pmod{\mathfrak{P}^{i+1}}.$$

Case 2. Suppose $\alpha \in \mathfrak{P}$. Since $v_{\mathfrak{P}}(\pi) = 1$, we can write $\pi\mathfrak{O}_K = \mathfrak{P}J$ with $\mathfrak{P}$ and J coprime. Using the Chinese Remainder Theorem (see [17, pg 253]) we can choose $\beta \in \mathfrak{O}_K$ such that

$$\beta \equiv 1 \pmod{\mathfrak{P}} \qquad \text{and} \qquad \beta \equiv 0 \pmod{J}.$$

So $\beta \in J$, and $\alpha\beta \in \pi\mathfrak{O}_K$. Again, we can write $\sigma(\beta) = \beta + \pi'$ for some $\pi' \in \mathfrak{P}^i$. I

claim that $\sigma(\alpha) \in \mathfrak{P}$. To see this, note that $\sigma \in G_0$ and $\alpha \in \mathfrak{P}$, so

$$\sigma(\alpha) \equiv \alpha \equiv 0 \pmod{\mathfrak{P}}.$$

In particular,

$$\sigma(\alpha\beta) = \sigma(\alpha)\sigma(\beta) = \sigma(\alpha)(\beta + \pi') \equiv \sigma(\alpha)\beta \pmod{\mathfrak{P}^{i+1}}.$$

On the other hand,

$$\sigma(\alpha\beta) \equiv \alpha\beta \pmod{\mathfrak{P}^{i+1}}$$

by Case 1. Thus we have

$$\sigma(\alpha)\beta \equiv \alpha\beta \pmod{\mathfrak{P}^{i+1}}.$$

Since $\beta \equiv 1 \pmod{\mathfrak{P}}$, we have that β is invertible modulo any power of $\mathfrak{P}$. We cancel to obtain

$$\sigma(\alpha) \equiv \alpha \pmod{\mathfrak{P}^{i+1}}.$$

Case 3. Suppose $\alpha \in \mathfrak{O}_K$. First, I claim that $\mathfrak{O}_K = \mathfrak{O}_K^{G_0} + \mathfrak{P}$, where $\mathfrak{O}_K^{G_0}$ denotes the elements of $\mathfrak{O}_K$ fixed by the inertia group G_0. It is clear that $\mathfrak{O}_K \supseteq \mathfrak{O}_K^{G_0} + \mathfrak{P}$. Let $\mathfrak{p}'$ be the prime of $\mathfrak{O}_K^{G_0}$ lying below $\mathfrak{P}$. By Theorem 2.9, K/K^{G_0} is totally ramified at $\mathfrak{p}'$, so $\mathfrak{P} \mid \mathfrak{p}'$ has inertial degree 1. Therefore $\mathfrak{O}_K^{G_0}/\mathfrak{p}'$ is naturally isomorphic to $\mathfrak{O}_K/\mathfrak{P}$. In particular, the composition of injection and projection

$$\mathfrak{O}_K^{G_0} \to \mathfrak{O}_K \to \mathfrak{O}_K/\mathfrak{P}$$

is surjective. Let $\alpha \in \mathfrak{O}_K$. Let $\beta \in \mathfrak{O}_K^{G_0}$ such that $\beta \mapsto \alpha + \mathfrak{P}$ in the above composition. Then $\alpha - \beta \mapsto \mathfrak{P}$ in the projection, so $\alpha = \beta + \pi'$ for some $\pi' \in \mathfrak{P}$. Thus $\mathfrak{O}_K = \mathfrak{O}_K^{G_0} + \mathfrak{P}$,

as desired. We now can use the fact that σ fixes β together with Case 2 to obtain

$$\sigma(\alpha) = \sigma(\beta + \pi') = \sigma(\beta) + \sigma(\pi') \equiv \beta + \pi' = \alpha \pmod{\mathfrak{P}^{i+1}}.$$

□

Proposition 2.14. *For $\sigma \in G_0$, $\sigma \in G_i$ if and only if $\sigma(\pi) \equiv \pi \pmod{\mathfrak{P}^{i+1}}$.*

Proof. Let $\sigma \in G_0$. The forward implication is obvious. Suppose that $\sigma \in G_j - G_{j+1}$. I claim that $\sigma(\pi) \equiv \pi \pmod{\mathfrak{P}^{i+1}}$ if and only if $i \leq j$. It is clear that if $i \leq j$, $\sigma(\pi) \equiv \pi \pmod{\mathfrak{P}^{i+1}}$. On the other hand, if $i > j$, then we cannot have $\sigma(\pi) \equiv \pi \pmod{\mathfrak{P}^{i+1}}$ by Proposition 2.13, else $\sigma \in G_i \subset G_{j+1}$. This proves the claim.

Now suppose that $\sigma(\pi) \equiv \pi \pmod{\mathfrak{P}^{i+1}}$. Then $i \leq j$, so $\sigma \in G_j \subseteq G_i$. □

Theorem 2.15. *There is a homomorphism $G_0 \to (\mathfrak{O}_K/\mathfrak{P})^\times$ with kernel G_1.*

In particular, G_0/G_1 is cyclic of order dividing $|\mathfrak{O}_K/\mathfrak{P}| - 1$. Thus if G_0 is non-cyclic, G_1 must be nontrivial. In other words, $\mathfrak{P} \mid \mathfrak{p}$ is wildly ramified. We will prove Theorem 2.15 using two lemmas.

Lemma 2.16. *For each $\sigma \in I = G_0$, there exists an α_σ such that*

$$\sigma(\pi) \equiv \alpha_\sigma \pi \pmod{\mathfrak{P}^2}.$$

Further, α_σ is determined mod $\mathfrak{P}$.

Proof. We can choose τ so that $v_{\mathfrak{P}}(\tau) \geq 3$, and $\mathfrak{P} = \pi\mathfrak{O}_K + \tau\mathfrak{O}_K$ (see [17, pg 61]). Let $\sigma \in G_0$. Since $\mathfrak{P} \mid \pi\mathfrak{O}_K$, $\pi\mathfrak{O}_K = \mathfrak{P}J$ for some ideal J of $\mathfrak{O}_K$ which is relatively prime to $\mathfrak{P}$. By the Chinese Remainder Theorem (see [17, pg 253]) we can choose $x \in \mathfrak{O}_K$ such that

$$x \equiv \sigma(\pi) \pmod{\mathfrak{P}^2} \qquad \text{and} \qquad x \equiv 0 \pmod{J}.$$

We have that $x \in \mathfrak{P}$, since $\sigma \in G_0 = I$ implies that

$$x \equiv \sigma(\pi) \equiv \pi \equiv 0 \pmod{\mathfrak{P}}.$$

Thus we can write $x = \alpha\pi + \beta\rho$ for some $\alpha, \beta \in \mathfrak{O}_K$. We have

$$\sigma(\pi) \equiv x \equiv \alpha\pi \pmod{\mathfrak{P}^2}.$$

To see that α is determined mod $\mathfrak{P}$, suppose that

$$\sigma(\pi) \equiv \alpha\pi \equiv \gamma\pi \pmod{\mathfrak{P}^2}.$$

Then we have that $\pi(\alpha - \gamma) \in \mathfrak{P}^2$, so $(\alpha - \gamma) \in \mathfrak{P}$, since $v_{\mathfrak{P}}(\pi) = 1$. Thus α is the desired element α_σ. □

Lemma 2.17. *For each $\sigma \in G_0$, let α_σ be as in the previous lemma. Then*

$$\alpha_{\sigma\tau} \equiv \alpha_\sigma \alpha_\tau \pmod{\mathfrak{P}}.$$

Proof. Since $\sigma \in G_0$, $\sigma(\alpha_\tau) \equiv \alpha_\tau \pmod{\mathfrak{P}}$. Write $\sigma(\alpha_\tau) = \alpha_\tau + \pi'$ with $\pi' \in \mathfrak{P}$. We show that

$$\alpha_{\sigma\tau}\pi \equiv \alpha_\sigma \alpha_\tau \pi \pmod{\mathfrak{P}^2}.$$

First, we have that $\tau(\pi) \equiv \alpha_\tau \pi \pmod{\mathfrak{P}^2}$. Applying σ, we obtain the following.

$$\alpha_{\sigma\tau}\pi \equiv \sigma\tau(\pi) \equiv \sigma(\alpha_\tau\pi) \equiv \sigma(\alpha_\tau)\sigma(\pi) \equiv (\alpha_\tau + \pi')\alpha_\sigma\pi \equiv \alpha_\sigma\alpha_\tau\pi + 0 \pmod{\mathfrak{P}^2}.$$

Therefore $\pi(\alpha_{\sigma\tau} - \alpha_\sigma\alpha_\tau) \in \mathfrak{P}^2$, and $\alpha_{\sigma\tau} - \alpha_\sigma\alpha_\tau \in \mathfrak{P}$. □

Proof of Theorem 2.15. Define a map $\varphi : G_0 \to (\mathfrak{O}_K/\mathfrak{P})^\times$ by $\varphi(\sigma) = \alpha_\sigma$, which is well

defined by Lemma 2.16. This map is a homomorphism by Lemma 2.17. If $\sigma \in G_1$, then

$$\alpha_\sigma \pi \equiv \sigma(\pi) \equiv \pi \pmod{\mathfrak{P}^2},$$

so $\alpha \equiv 1 \pmod{\mathfrak{P}}$. Therefore $\sigma \in \ker \varphi$. Conversely, if $\varphi(\sigma) = 1 + \mathfrak{p}$, then $a_\sigma \equiv 1 \pmod{\mathfrak{p}}$, so $\sigma(\pi) \equiv \pi \pmod{\mathfrak{P}}^2$. By Proposition 2.14, $\sigma \in G_1$. Therefore $\ker \varphi = G_1$. □

Our next goal will be to prove the following:

Theorem 2.18. *Fix $i \geq 2$. There is an additive homomorphism $G_{i-1} \to \mathfrak{O}_K/\mathfrak{P}$ with kernel G_i.*

We will prove Theorem 2.18 using two lemmas.

Lemma 2.19. *For each $\sigma \in G_{i-1}$, there exists $\alpha_\sigma \in \mathfrak{O}_K$ such that*

$$\sigma(\pi) \equiv \pi + \alpha_\sigma \pi^i \pmod{\mathfrak{P}^{i+1}}.$$

Further, α_σ is unique modulo $\mathfrak{P}$.

Proof. Fix $\sigma \in G_{i-1}$. Then $\sigma(\pi) \equiv \pi \pmod{\mathfrak{P}^i}$. We have that $v_\mathfrak{P}(\pi^i) = i$, so $\pi^i \in \mathfrak{P}^i - \mathfrak{P}^{i+1}$. Write $\mathfrak{P}^i = (\pi^i, \tau)$ where $v_\mathfrak{P}(\tau) \geq i + 1$. Then there exists $\alpha, \beta \in \mathfrak{O}_K$ such that

$$\sigma(\pi) = \pi + \alpha\pi^i + \beta\tau.$$

Mod $\mathfrak{P}^{i+1}$ we have

$$\sigma(\pi) \equiv \pi + \alpha\pi^i \pmod{\mathfrak{P}^{i+1}}.$$

Suppose that there exists $\beta \in \mathfrak{O}_K$ such that

$$\sigma(\pi) \equiv \pi + \beta\pi^i \pmod{\mathfrak{P}^{i+1}}.$$

Then we have that $(\alpha - \beta)\pi^i \in \mathfrak{P}^{i+1}$. Since $\mathfrak{P}^i \mid (\pi^i)$ but $\mathfrak{P}^{i+1} \nmid (\pi^i)$, we must have $\mathfrak{P} \mid (\alpha - \beta)$. Therefore $\alpha \equiv \beta \pmod{\mathfrak{P}}$. Thus α is the desired element α_σ. □

Lemma 2.20. *Let α_σ denote the element constructed in Lemma 2.19. Then for $\sigma, \tau \in G_{i-1}$,*

$$\alpha_{\sigma\tau} \equiv \alpha_\sigma + \alpha_\tau \pmod{\mathfrak{P}}.$$

Proof. We have that $\tau(\pi) \equiv \pi + \alpha_\tau \pi^i \pmod{\mathfrak{P}^{i+1}}$. Applying σ we have

$$\begin{aligned} \sigma\tau(\pi) &\equiv \sigma(\pi + \alpha_\tau \pi^i) \\ &\equiv \sigma(\pi) + \sigma(\alpha_\tau)\sigma(\pi)^i \\ &\equiv \pi + \alpha_\sigma \pi^i + \sigma(\alpha_\tau)(\pi + \alpha_\sigma \pi^i)^i \qquad \pmod{\mathfrak{P}^{i+1}}. \end{aligned}$$

Since $\sigma(\alpha_\tau) \equiv \alpha_\tau \pmod{\mathfrak{P}^i}$, we can write $\sigma(\alpha_\tau) = \alpha_\tau + \pi'$ with $\pi' \in \mathfrak{P}^i$. Then

$$\begin{aligned} \sigma\tau(\pi) &\equiv \pi + \alpha_\sigma \pi^i + (\alpha_\tau + \pi')\pi^i (1 + \alpha_\sigma \pi^{i-1})^i \\ &\equiv \pi + (\alpha_\sigma + \alpha_\tau)\pi^i \qquad \pmod{\mathfrak{P}^{i+1}}. \end{aligned}$$

Since $\alpha_\sigma \tau$ is determined mod $\mathfrak{P}$, we have that

$$\alpha_\sigma \tau \equiv \alpha_\sigma + \alpha_\tau \pmod{\mathfrak{P}}.$$

□

Proof of Theorem 2.18. Define a map $G_{i-1} \to \mathfrak{O}_K/\mathfrak{P}$ by $\sigma \mapsto \alpha_\sigma$. This map is well defined by Lemma 2.19. The map is an additive homomorphism by Lemma 2.20. If σ is in the kernel, then $\alpha_\sigma \equiv 0 \pmod{\mathfrak{P}}$. This means that

$$\sigma(\pi) \equiv \pi \pmod{\mathfrak{P}^{i+1}},$$

which implies that $\sigma \in G_i$ by Lemma 2.14. Conversely, if $\sigma \in G_i$, then

$$\sigma(\pi) \equiv \pi \pmod{\mathfrak{P}^{i+1}},$$

so we can choose $\alpha_\sigma = 0$, thus σ is in the kernel. □

Theorem 2.18 shows us that each G_{i-1}/G_i for $i \geq 2$ is an elementary abelian p-group (a direct sum of copies of $\mathbb{Z}/p$). Since the G_i's are all trivial for sufficiently large i, we can conclude that each G_i is a p-group for $i \geq 1$.

Theorem 2.21. *G_1 is the unique Sylow p-subgroup of G_0.*

Proof. Since G_1 is normal in G_0, uniqueness follows by showing that G_1 is a Sylow p-subgroup of G_0. By Theorem 2.15, $|G_0/G_1| \mid (|(\mathfrak{O}_K/\mathfrak{P})^\times| - 1)$, which is relatively prime to p. Therefore it suffices to know that G_1 is a p-subgroup of G_0. This follows from Theorem 2.18. □

Corollary 2.22. *Let e denote the ramification index of $\mathfrak{P} \mid \mathfrak{p}$. Then $\mathfrak{P} \mid \mathfrak{p}$ is tamely ramified if and only if $(e, p) = 1$.*

Proof. Since $G_0 = I$ is the inertia group, $|G_0| = e$ is the ramification index. By Theorem 2.21, $\mathfrak{P} \mid \mathfrak{p}$ is tamely ramified if and only if the Sylow p-subgroup of G_0 is trivial, if and only if $(e, p) = 1$. □

Remark. Often the definition of tame ramification is given as: $\mathfrak{P} \mid \mathfrak{p}$ is tamely ramified if $(e, p) = 1$, and wildly ramified otherwise.

2.2.3 The conductor of a Galois representation.

Definition 2.23. ([19, pg 527]) Let K be a number field which is Galois over $\mathbb{Q}$, $p \in \mathbb{Z}$ a prime. Let $\rho : G_{\mathbb{Q}} \to \mathrm{GL}(V)$ be a Galois representation which factors through the projection $G_{\mathbb{Q}} \to \mathrm{Gal}(K/\mathbb{Q})$. We define the **conductor of** ρ to be

$$N = \prod_p p^{n_p},$$

where

$$n_p = \sum_{i=1}^{\infty} \frac{1}{|G_0 : G_i|} \dim V/V_i$$

with $V_i = V^{G_i}$, the fixed space of the ith ramification group of a prime $\mathfrak{p} \mid p$.

When $K/\mathbb{Q}$ is unramified at p, G_i is trivial for all i, $V = V_i$, and thus $n_p = 0$. Therefore the conductor is a finite integer. When $\mathfrak{p} \mid p$ is tamely ramified, meaning that G_1 is trivial, $n_p = \dim V/V_0$.

One significance of the conductor is Serre's modularity conjecture, stated in [23] and proven recently by Khare and Wintenberger in [14] and [13].

Theorem 2.24. *Let p be a prime number and let $\overline{\mathbb{F}}_p$ an algebraic closure of $\mathbb{F}_p$, the field of p elements. Let V be a 2-dimensional $\overline{\mathbb{F}}_p$-vector space, and suppose that*

$$\rho : G_{\mathbb{Q}} \to \mathrm{GL}(V)$$

is a continuous, irreducible, odd representation. Let N denote the conductor of ρ. Then ρ is attached to a newform of level N.

Having ρ attached to a newform (see [1]) means that there exists a newform f with Fourier expansion

$$f = \sum_{n=1}^{\infty} a_n q^n$$

such that

$$\mathrm{tr}(\rho(\varphi_\ell)) \equiv a_\ell \pmod{p}$$

for almost all primes ℓ. Here φ_ℓ denotes a Frobenius automorphism of ℓ for the number field $K/\mathbb{Q}$ with Galois group $G_{\mathbb{Q}}/\ker\rho$, and tr denotes the trace. See [23] for more details.

2.3 Group cohomology

We use this section to summarize the required group cohomology theory that we will use.

2.3.1 Definitions. Let G be a group, and A a $\mathbb{Z}G$-module. Consider an **injective resolution** of A (see [20, pg 179]), which is an exact sequence

$$0 \to A \to I^0 \to I^1 \to I^2 \to \cdots$$

where each I^n is an injective $\mathbb{Z}G$-module, see [20, pg 167].

Applying the "invariant functor" $(-)^G$ (see [26, pg 160]) to the **complex** (meaning the composition of two adjacent maps is 0) $\cdots \to 0 \to I^0 \to I^1 \to \cdots$, we obtain a complex

$$\cdots \to 0 \to 0 \xrightarrow{d^{-1}} (I^0)^G \xrightarrow{d^0} (I^1)^G \xrightarrow{d^1} (I^2)^G \to \cdots .$$

We define for $n \geq 0$ the nth **cohomology group of** G **with coefficients in** A (see [26, pg 161]) as

$$H^n(G, A) = \ker d^n / \operatorname{im} d^{n-1}.$$

Homology groups are defined dually using the "coinvariant functor" $(-)_G$ (see [26, pg 160]), where

$$A_G = A/\langle g \cdot a - a : a \in A, g \in G \rangle.$$

The functor $(-)^G$ turns out to be isomorphic to $\operatorname{Hom}_{\mathbb{Z}G}(\mathbb{Z}, -)$ (see [26, pg 161]), which means that

$$H^n(G, A) = \operatorname{Ext}^n_{\mathbb{Z}G}(\mathbb{Z}, A), \text{ see [20, pg 45].}$$

This means that we can also compute $H^n(G, A)$ by using **projective resolution** of $\mathbb{Z}$ (see [20, pg 179] and [26, pg 63]), that is, an exact sequence

$$\cdots \to P_2 \to P_1 \to P_0 \to \mathbb{Z} \to 0,$$

where each P_n is a projective $\mathbb{Z}G$-module, see [20, pg 167]. In this case, we apply the

contravariant functor $\mathrm{Hom}_{\mathbb{Z}G}(-, A)$ (see [20, pg 13]) to obtain the complex

$$\cdots \to 0 \to 0 \to \mathrm{Hom}_{\mathbb{Z}G}(P_0, A) \xrightarrow{d^0} \mathrm{Hom}_{\mathbb{Z}G}(P_1, A) \xrightarrow{d^1} \mathrm{Hom}_{\mathbb{Z}G}(P_2, A) \to \cdots,$$

and we have

$$H^n(G, A) = \ker d^n / d^{n-1}(I^{n-1}).$$

2.3.2 Group extensions. An important application of group cohomology is group extensions. A **group extension** is an exact sequence of groups

$$0 \to A \to E \to G \to 0$$

with A abelian, and we say E **is an extension of** G **by** A, see [26, pg 182]. Two extensions of G by A are **equivalent** if there exists a map $E \to E'$ making the following diagram commute (see [26, pg 183]).

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \longrightarrow & E & \longrightarrow & G & \longrightarrow & 0 \\ & & \| & & \downarrow & & \| & & \\ 0 & \longrightarrow & A & \longrightarrow & E' & \longrightarrow & G & \longrightarrow & 0. \end{array}$$

This is an equivalence relation, since the map $E \to E'$ is an isomorphism by the 5-lemma, see [20, pg 191].

Theorem 2.25 ([26, pg 183])**.** *There is a one-to-one correspondence between equivalence classes of group extensions of G by A with a given G-action on A, and elements of $H^2(G, A)$.*

In particular, if $H^2(G, A) = 0$, then the only extension of G by A is the semi-direct product (see [11, pg 367])

$$0 \to A \to A \rtimes G \to G \to 0.$$

One instance where the semi-direct product is the only extension of G by A is if the orders of A and G are relatively prime. This follows from the more general theorem given below.

Theorem 2.26 ([11, pg 362])**.** *Suppose that the orders of A and G are relatively prime. Then*

$H^n(G, A) = 0$ *for all* $n \geq 1$.

2.3.3 Spectral sequences. For our purposes, we define a spectral sequence as follows.

Definition 2.27. ([26, pg 123]) A **spectral sequence** consists of:

(i) a family $\{E_r^{pq}\}$ of objects for $r \geq a$ (where a is a fixed integer) and $p, q \in \mathbb{Z}$,

(ii) for all $p, q \in \mathbb{Z}$ and $r \geq a$, there is a map

$$d_r^{pq} : E_r^{pq} \to E_r^{p+r,q-r+1},$$

which satisfy the differential rule $d_r^{pq} d_r^{p+r,q-r+1} = 0$, and

(iii) for all $p, q \in \mathbb{Z}$ and $r \geq a$, an isomorphism between E_{r+1}^{pq} and the cohomology of E_r^{pq} computed using the differentials of part (ii).

For our purposes, $E_r^{pq} = 0$ wherever p or q is negative. We think of p and q as coordinates on a first quadrant grid, and r as indexing the "pages" of the sequence. For instance, pages 0–3 of a spectral sequence have form as shown in Figure 2.1.

If for some $r_0 \geq 0$, $E_r^{pq} = E_{r_0}^{pq}$ for all $r \geq r_0$, we write E_∞^{pq} for this stable value. Let $\{H^n\}$ denote a family of objects for $n \geq a$. Following [26, pg 123], we say that E_r^{pq} **converges** to $H^\bullet$ if each H^n has a finite filtration

$$0 = F^t H^n \subset \cdots \subset F^s H^n = H^n$$

such that

$$E_\infty^{pq} \cong F^p H^{p+q} / F^{p+1} H^{p+q}.$$

We denote this by

$$E_a^{pq} \implies H^{p+q}.$$

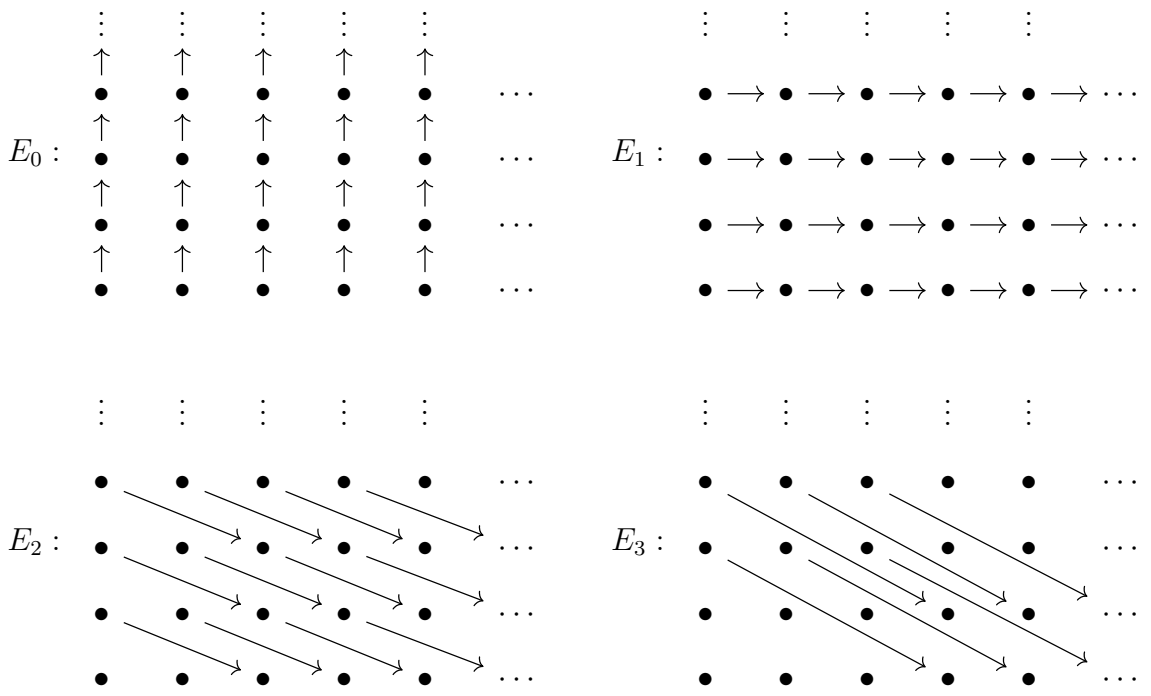

Figure 2.1: Pages 0–3 of a spectral sequence

2.3.4 The Hochschild-Serre spectral sequence. The spectral sequence that we will use is the Hochschild-Serre spectral sequence, given by Theorem 2.28.

Theorem 2.28 ([26, pg 195])**.** *For a normal subgroup H of a group G, there is a convergent spectral sequence for any $\mathbb{Z}G$-module A:*

$$E_2^{pq} = H^p(G/H, H^q(H, A)) \implies H^{p+q}(G, A).$$

Chapter 3. Octahedral representations with prime conductor

The goal of this section is to prove the following result, which was originally conjectured by Siman Wong in [27, Conj 2]. These results were published in [4], and are joint with Darrin Doud.

Theorem 3.1. *Let $K/\mathbb{Q}$ be a number field with S_4-Galois closure ramified at a single prime $p > 3$. Let $K_3/\mathbb{Q}$ be a cubic subfield of the Galois closure of $K/\mathbb{Q}$. Let $\tilde{\rho}$ be the projective 2-dimensional Artin representation associated to $K/\mathbb{Q}$.*

(i) Suppose $K_3/\mathbb{Q}$ is totally real. If $\tilde{\rho}$ has conductor p^2, then $v_p(\mathrm{disc}(K)) = 1$.

(ii) Suppose $K_3/\mathbb{Q}$ is not totally real. If $\tilde{\rho}$ has conductor p^2 then $v_p(\mathrm{disc}(K)) = 3$, otherwise $v_p(\mathrm{disc}(K)) = 1$.

We will prove Theorem 3.1 using the techniques of Serre found in [21].

3.1 Results of Serre

A continuous representation $\rho : G_{\mathbb{Q}} \to \mathrm{GL}(2, \mathbb{C})$ always has finite image, see [5, pg 45]. Let $\tilde{\rho} : G_{\mathbb{Q}} \to \mathrm{PGL}(2, \mathbb{C})$ be the **projective representation** obtained by composing ρ with the projection $\pi : \mathrm{GL}(2, \mathbb{C}) \to \mathrm{PGL}(2, \mathbb{C})$. Then the image of $\tilde{\rho}$ is a finite subgroup of $\mathrm{PGL}(2, \mathbb{C})$. The following Theorem is due to Klein, and lists all possible images for $\tilde{\rho}$.

Theorem 3.2 ([15])**.** *A finite subgroup of $\mathrm{PGL}(2, \mathbb{C})$ is isomorphic to one of the following polyhedral groups:*

(i) a cyclic group C_n;

(ii) a dihedral group D_{2n} of order $2n$, $n \geq 2$;

(iii) the tetrahedral group A_4 or order 12;

(iv) the octahedral group S_4 of order 24;

(v) the icosahedral group A_5 of order 60.

Up to conjugation, all of these groups occur as subgroups of $\mathrm{PGL}(2,\mathbb{C})$ *exactly once.*

Given a projective representation $\tilde{\rho} : G_{\mathbb{Q}} \to \mathrm{PGL}(2,\mathbb{C})$, we define a **lift** of $\tilde{\rho}$ to be a representation $\rho : G_{\mathbb{Q}} \to \mathrm{GL}(2,\mathbb{C})$ such that $\tilde{\rho} = \pi \circ \rho$, see [21, Sec 6.1].

3.1.1 Conductor for a projective representation. Let $\tilde{\rho} : G_{\mathbb{Q}} \to \mathrm{PGL}(2,\mathbb{C})$ be a projective representation. Let p be a prime, and D_p a decomposition group of a prime of $\overline{\mathbb{Q}}$ above p. Define $m(p)$ as the smallest integer such that the restriction $\tilde{\rho}|_{D_p}$ has a lifting with conductor $p^{m(p)}$. Then we define the **conductor** of $\tilde{\rho}$ (see [21, Sec 6.2]) to be the integer

$$N = \prod_p p^{m(p)}.$$

If $\tilde{\rho}$ is unramified at p, then we necessarily have $m(p) = 0$. If $\tilde{\rho}$ is tamely ramified at p, then we have $m(p) = 1$ if $\tilde{\rho}(D_p)$ is cyclic, and $m(p) = 2$ if $\tilde{\rho}(D_p)$ is dihedral by [21, Sec 6.3].

For our purposes we will only be considering $\tilde{\rho}$ ramified (tamely) at a single prime p. Thus the only possible values for the conductor are p and p^2. Serre has classified all odd projective representations with prime conductor in [21], and Vignéras has classified all even projective representations of prime conductor in [25]. One useful result in determining the conductor of $\tilde{\rho}$ is the following.

Lemma 3.3 ([21, Sec 8.1])**.** *Let $\tilde{\rho}$ be any 2-dimensional projective representation of $G_{\mathbb{Q}}$, and p any prime number. Let $i_p = |\tilde{\rho}(I_p)|$, where I_p denotes the inertia group at p. Assume that i_p is prime to p and $i_p \geq 3$. Then the conductor of $\tilde{\rho}$ is exactly divisible by p if and only if $i_p \mid (p-1)$.*

This lemma will be essential to proving part (i) of Theorem 3.1. Part (ii) of Theorem 3.1 depends on Serre's classification of odd representations.

3.1.2 Classification of odd projective representations. Let p be a prime number, and $E/\mathbb{Q}$ a Galois extension. After classifying projective representations with cyclic and dihedral image, Serre considers three cases in [21, Sec 8.1]:

(a) $\mathrm{Gal}(E/\mathbb{Q}) = S_4$ and $p \equiv 5 \pmod 8$;

(b) $\mathrm{Gal}(E/\mathbb{Q}) = S_4$ and $p \equiv 3 \pmod 4$;

(c) $\mathrm{Gal}(E/\mathbb{Q}) = A_5$ and $p \equiv 3 \pmod 4$.

By Theorem 3.2, there is a unique subgroup (up to conjugation) of $\mathrm{PGL}(2,\mathbb{C})$ isomorphic to each of S_4 and A_5. By projecting $G_{\mathbb{Q}} \to \mathrm{Gal}(E/\mathbb{Q})$ and then embedding $\mathrm{Gal}(E/\mathbb{Q}) \to \mathrm{PGL}(2,\mathbb{C})$, we obtain a projective representation $\tilde{\rho}$. We call $\tilde{\rho}$ the **projective Artin representation** associated to $E/\mathbb{Q}$. We then have the following.

Theorem 3.4 ([21, Sec 8.1])**.** *The representation $\tilde{\rho}$ has an odd lifting with conductor p if and only if:*

Case (a): *E is the Galois closure of a non-real quartic field $E_4/\mathbb{Q}$ with discriminant p^3;*

Case (b): *E is the Galois closure of a non-real quartic field $E_4/\mathbb{Q}$ with discriminant $-p$;*

Case (c): *E is the Galois closure of a non-real quintic field $E_5/\mathbb{Q}$ with discriminant p^2.*

When these conditions are satisfied, in each case $\tilde{\rho}$ has precisely two non-isomorphic odd liftings with conductor p; if one of these is ρ, the other is $\rho' = \rho \otimes \epsilon$, where $\epsilon = \det(\rho)$.

Specifically, we will make use of case (b) of Theorem 3.4 in proving Theorem 3.1.

3.2 Octahedral representations

In this section we will prove Theorem 3.1 using the results of Serre from the previous section, along with some additional lemmas. A result that is surprisingly useful for us is the following.

Theorem 3.5 (Stickelberger's Criterion [16, pg 67])**.** *Let $K/\mathbb{Q}$ be a number field, and $\alpha_1, \ldots, \alpha_n \in \mathfrak{O}_K$. Then*

$$\operatorname{disc}(\alpha_1, \ldots, \alpha_n) \equiv 0 \text{ or } 1 \pmod 4.$$

Proof. Let $\sigma_1, \ldots, \sigma_n$ denote the n embeddings $K \to \mathbb{C}$. Then

$$\begin{aligned} d = \operatorname{disc}(\alpha_1, \ldots, \alpha_n) &= \det([\sigma_i(\alpha_j)])^2 \\ &= \left(\sum_{\tau \in S_n} \operatorname{sgn}(\tau) \sigma_{\tau(1)}(\alpha_1) \cdots \sigma_{\tau(n)}(\alpha_n) \right)^2 \\ &= (P - N)^2 = (P + N)^2 - 4PN \end{aligned}$$

where

$$P = \sum_{\tau \in A_n} \sigma_{\tau(1)}(\alpha_1) \cdots \sigma_{\tau(n)}(\alpha_n)$$

and

$$N = \sum_{\tau \in S_n - A_n} \sigma_{\tau(1)}(\alpha_1) \cdots \sigma_{\tau(n)}(\alpha_n).$$

It is clear that P and N are algebraic integers, since they are sums of products of algebraic integers. Therefore $P + N$ and PN are algebraic integers as well. Let L denote the Galois closure of $K/\mathbb{Q}$. I claim that $P + N, PN \in \mathbb{Z}$, which will follow by showing that they are fixed by $\operatorname{Gal}(L/\mathbb{Q})$.

Let $\tau \in \operatorname{Gal}(L/\mathbb{Q})$, and note that $\tau \circ \sigma_i$ is an embedding $K \to \mathbb{C}$. Further, if $\tau \circ \sigma_i = \tau \circ \sigma_j$, then $\sigma_i = \sigma_j$. We have that τ permutes the set $\{\sigma_1, \ldots, \sigma_n\}$. Thus $\operatorname{Gal}(L/\mathbb{Q})$ acts on this set. We can think of $\operatorname{Gal}(L/\mathbb{Q})$ as a subset of S_n, in which case we have $\tau(\sigma_i) = \sigma_{\tau(i)}$. Therefore we can rewrite P and N as

$$P = \sum_{\tau \in A_n} \tau(\beta) \qquad \text{and} \qquad \sum_{\tau \in S_n - A_n} \tau(\beta),$$

where $\beta = \sigma_1(\alpha_1) \cdots \sigma_n(\alpha_n)$.

Suppose that $\chi \in \mathrm{Gal}(L/\mathbb{Q})$. If χ is even, then $\chi\tau$ will have the same parity as τ. In this case, P and N are fixed by χ. If χ is odd, then $\chi\tau$ will have the opposite parity as τ. In this case P and N are swapped by χ. In either case, $P + N$ and PN are fixed by χ. Since χ was arbitrary, $P + N$ and PN are fixed by $\mathrm{Gal}(L/\mathbb{Q})$, as desired.

Since $d = (P + N)^2 - 4PN$ with $P + N, PN \in \mathbb{Z}$, d is a square mod 4. Therefore $d \equiv 0$ or $1 \pmod 4$. □

In particular, Stickelberger's Criterion implies that $\mathrm{disc}(K) \equiv 0$ or $1 \pmod 4$.

3.2.1 Preliminary lemmas. Let $K/\mathbb{Q}$ be a quartic extension with S_4-Galois closure. Assume further that $K/\mathbb{Q}$ is ramified at only one prime $p > 3$. Then $\mathrm{disc}(K) = \pm p^k$ for some $k \geq 1$. Theorem 3.1 is stated in terms of $k = v_p(\mathrm{disc}(K))$. We will show that $v_p(\mathrm{disc}(K))$ is always either 1 or 3.

Lemma 3.6. *Let $K/\mathbb{Q}$ be as above. Let e denote the ramification index of any prime lying over p in the splitting field of $K/\mathbb{Q}$. Then $v_p(\mathrm{disc}(K))$ is either 1 (when $e = 2$) or 3 (when $e = 4$). If $v_p(\mathrm{disc}(K)) = 3$, then the ramification index of any prime lying over p in the splitting field of $K/\mathbb{Q}$ is $e = 4$.*

Proof. Suppose that there are r primes above p in of $K/\mathbb{Q}$, and each has ramification index e_i and inertial degree f_i. Then we have by Theorem 2.3 that

$$e_1 f_1 + \cdots + e_r f_r = [K : \mathbb{Q}] = 4$$

Since $K/\mathbb{Q}$ is tamely ramified,

$$v_p(\mathrm{disc}(K)) = (e_1 - 1)f_1 + \cdots + (e_r - 1)f_r$$

by [22, pg 58]. Table 3.1 shows all possible splitting of $p\mathfrak{O}_K$ with ramification, and the corresponding discriminants. In the table we take $f_i = 1$ unless otherwise noted. Since p

Factorizations of $p\mathfrak{O}_K$	$v_p(\text{disc}(K))$
$e_1 = 2,\ e_2 = e_3 = 1$	1
$e_1 = 2,\ f_1 = 2$	2
$e_1 = 3,\ e_2 = 1$	2
$e_1 = e_2 = 2$	2
$e_1 = 4$	3

Table 3.1: Possible factorizations of $p\mathfrak{O}_K$ in the notation of Lemma 3.6

is odd, we have that $p^2 \equiv 1 \pmod 4$. Therefore if $v_p(\text{disc}(K)) = 2$, then $\text{disc}(K) = p^2$ by Stickelberger's Criterion. Since the discriminant would be a square, $\text{Gal}(K/\mathbb{Q})$ would be a subgroup of A_4 by [10, pg 258], which is not permitted. Thus we must have that $v_p(\text{disc}(K))$ is 1 or 3.

Let L denote the Galois closure of $K/\mathbb{Q}$. Since p is tamely ramified, the inertia group I is cyclic by Theorem 2.15. Since I has order e and $\text{Gal}(L/\mathbb{Q}) \cong S_4$ has no elements of order > 4, we have $e \leq 4$.

Suppose that $v_p(\text{disc}(K)) = 3$. Then $p\mathfrak{O}_K$ factors as $p\mathfrak{O}_K = \mathfrak{p}^4$. Therefore $e \geq 4$, thus $e = 4$.

Suppose that $v_p(\text{disc}(K)) = 1$. Then $p\mathfrak{O}_K = \mathfrak{p}^2\mathfrak{p}'\mathfrak{p}''$ We see that $2 \mid e$, so e is either 2 or 4. If it were 4, then $\mathfrak{p}'$ and $\mathfrak{p}''$ would have to factor as 4th powers in L. However, $4 \nmid [L : K] = 6$, so this cannot happen. Thus $e = 2$. □

Let $K_3/\mathbb{Q}$ be a cubic subfield of the splitting field of $K/\mathbb{Q}$. Theorem 3.1 is stated in terms of whether $K_3/\mathbb{Q}$ is totally real, or non-real. We can interpret this information in terms of p mod 4.

Lemma 3.7. *Let $K_3/\mathbb{Q}$ be a cubic field extension with Galois group S_3 ramified only at a prime $p > 3$. Then K_3 is totally real if and only if $p \equiv 1 \pmod 4$.*

Proof. Let $p^* = (-1)^{(p-1)/2}p$, so that $p^* \equiv 1 \pmod 4$. Let L be the splitting field of $K_3/\mathbb{Q}$, and K_2 the unique quadratic subfield of L. We have that $K_2 = \mathbb{Q}(\sqrt{p^*})$, since this is the only

quadratic extension with ramification only at p. (The discriminant of $\mathbb{Q}(\sqrt{-p^*})$ is divisible by 2, see [17, pg 33].) Then K_2 is real if $p \equiv 1 \pmod 4$ (i.e. $p^* > 0$), and non-real if $p \equiv 3 \pmod 4$ (i.e. $p^* < 0$). The extension L/K_2 has odd degree, thus no infinite primes can ramify. Therefore L, and hence K_3, is totally real if and only if K_2 is. □

3.2.2 Proof of the main Theorem. With these lemmas in hand, we are prepared to prove Theorem 3.1.

Proof of Theorem 3.1. Assume that $K/\mathbb{Q}$ is is a quartic extension with S_4-Galois closure $L/\mathbb{Q}$. Suppose $K/\mathbb{Q}$ is ramified at only one prime $p > 3$. Let $K_3/\mathbb{Q}$ be a cubic subfield of $L/\mathbb{Q}$. Let $\tilde{\rho}$ be the projective representation associated to $L/\mathbb{Q}$.

Suppose that $K_3/\mathbb{Q}$ is totally real. Then by Lemma 3.7, $p \equiv 1 \pmod 4$. We wish to show that if $\tilde{\rho}$ has conductor p^2, then $v_p(\text{disc}(K)) = 1$. Suppose that $\tilde{\rho}$ does not have $v_p(\text{disc}(K)) = 1$. Then by Lemma 3.6, $v_p(\text{disc}(K)) = 3$, and $e = 4$. But we have that $i_p := |\tilde{\rho}(I_p)| = e$, since $\tilde{\rho}$ is an isomorphism after projecting onto $\text{Gal}(L/\mathbb{Q})$. Since $i_p = 4$, we have that $i_p \geq 3$, and i_p is prime to p (since p is odd). Since $p \equiv 1 \pmod 4$, $i_p \mid (p-1)$ and thus the conductor of $\tilde{\rho}$ is p by Lemma 3.3. This completes the proof of part (i).

Suppose that $K_3/\mathbb{Q}$ is not totally real. Then Lemma 3.7 implies that $p \equiv 3 \pmod 4$. In light of our discussion and Lemma 3.6, Theorem 3.1 (ii) can be restated as

$$\tilde{\rho} \text{ has conductor } p^2 \text{ if and only if } v_p(\text{disc}(K)) = 3.$$

Equivalently, $\tilde{\rho}$ has conductor p if and only if $v_p(\text{disc}(K)) = 1$. Since $p \equiv 3 \pmod 4$, Stickelberger's Criterion shows that the latter condition is equivalent to $\text{disc}(K) = -p$. So we wish to show that $\tilde{\rho}$ has conductor p if and only if $\text{disc}(K) = -p$. This is exactly Theorem 3.4(b) when $\tilde{\rho}$ is odd.

Suppose that $\tilde{\rho}$ is even. This would imply that $\tilde{\rho}$ maps complex conjugation to the identity in $\text{PGL}(2, \mathbb{C})$. But K_3 is not real, thus complex conjugation is not a trivial automorphism of $L/\mathbb{Q}$, therefore $\tilde{\rho}$ must be odd, and (ii) is proved. □

Chapter 4. Counting extensions

In the last chapter we discussed a cubic subfield of an S_4-extension. In this chapter we explore how often a fixed cubic extension is contained in S_4-extensions with given properties. These results were published separately in [3], and are joint with Darrin Doud.

4.1 Counting S_4-extensions

Let F be a number field, and let K/F be a cubic extension, with S_3-Galois closure. Let $\mathcal{P}$ be a finite set of primes of F containing the primes which ramify in K. Then there are only finitely many extensions of a given degree with ramification only in $\mathcal{P}$ by [16, pg 122], thus finitely many S_4-extensions of $\mathbb{Q}$ containing K and unramified outside of $\mathcal{P}$. How many S_4 extensions L/F exist which contain K and are unramified outside of $\mathcal{P}$?

4.1.1 Motivating examples. The following examples were computed using GP/PARI (see [24]) and John Jones' number field database (see [12]).

Example 4.1. Let α be a root of $f(x)$, $K = \mathbb{Q}(\alpha)$, and $\mathcal{P} = \{p, \infty\}$. In each of the three examples below, $K/\mathbb{Q}$ is unramified outside of $\mathcal{P}$, but there are no S_4-extensions of $\mathbb{Q}$ which are unramified outside of $\mathcal{P}$.

(i) $f(x) = x^3 - 3$ and $p = 3$.

(ii) $f(x) = x^3 - x^2 + 1$ and $p = 23$.

(iii) $f(x) = x^3 + x - 1$ and $p = 31$.

Example 4.2. Let $K = \mathbb{Q}(\alpha)$ with α a root of $f(x)$, and $\mathcal{P} = \{p, \infty\}$. In the examples below, $K/\mathbb{Q}$ is unramified outside of $\mathcal{P}$ and there is a unique S_4-extension $L/\mathbb{Q}$ containing K and unramified outside of $\mathcal{P}$. The field L can be found as the splitting field of $g(x)$.

(i) $f(x) = x^3 - 2x + 1$, $p = 59$, and $g(x) = x^4 - x^3 - 7x^2 + 11x + 3$.

(ii) $f(x) = x^3 - x^2 + 3x - 2$, $p = 107$, and $g(x) = x^4 - x^3 - 13x^2 + 20x - 28$.

(iii) $f(x) = x^3 - x^2 + x + 2$, $p = 139$, and $g(x) = x^4 - x^3 - 17x^2 + 26x + 120$.

Example 4.3. Let $K = \mathbb{Q}(\alpha)$ with α a root of $f(x)$, and $\mathcal{P} = \{p, \infty\}$. In the following examples, $K/\mathbb{Q}$ is unramified outside of $\mathcal{P}$ and there are exactly three S_4-extensions $L/\mathbb{Q}$ containing K and unramified outside of $\mathcal{P}$. Values for $g(x)$ defining the three S_4-extensions are listed.

(i) $f(x) = x^3 - 4x - 1$, $p = 229$, and

$$g(x) \in \{x^4 - x + 1,\ x^4 - x^3 + 29x^2 - 43x + 17,\ x^4 - x^3 + 29x^2 - 43x + 246\}.$$

(ii) $f(x) = x^3 + 4x - 1$, $p = 283$, and

$$g(x) \in \{x^4 - x - 1,\ x^4 - x^3 - 35x^2 + 53x - 21,\ x^4 - x^3 - 35x^2 + 53x + 262\}.$$

(iii) $f(x) = x^3 - x^2 + 3x - 4$, $p = 331$, and

$$g(x) \in \{x^4 - x^3 + x^2 + x - 1,\ x^4 - x^3 - 41x^2 + 62x - 128,\ x^4 - x^3 - 41x^2 + 393x - 459\}.$$

Example 4.4. Let $K = \mathbb{Q}(\alpha)$ with α a root of $x^3 - x^2 - 9x - 16$. The $K/\mathbb{Q}$ is unramified outside of $\mathcal{P} = \{6571, \infty\}$. There are seven S_4-extensions $L/\mathbb{Q}$ containing K and unramified outside of $\mathcal{P}$, which are the splitting fields of the following polynomials:

$$x^4 - 2x^2 - 3x + 2, \qquad x^4 - x^3 - 2x^2 + 4x + 1,$$
$$x^4 + 4x^2 - 5x + 1, \qquad x^4 - 6571x - 45997,$$
$$x^4 - x^3 - 821x^2 + 20945x - 85500, \qquad x^4 - x^3 - 821x^2 - 11910x - 59216,$$
$$x^4 - x^3 - 821x^2 + 7803x - 26361$$

4.1.2 Statement of theorems. The previous examples show that when $F = \mathbb{Q}$ and $\mathcal{P}$ consists of a single finite prime, we can get values

$$0 = 2^0 - 1, \qquad 1 = 2^1 - 1, \qquad 3 = 2^2 - 1, \qquad 7 = 2^4 - 1$$

for the number of S_4-extensions with the desired properties. Based on extensive computations, Wong conjectured the following in [27], which we will prove.

Theorem 4.5. *Let $K/\mathbb{Q}$ be a non-Galois cubic extensions such that $|\operatorname{disc}(K)|$ is a prime power. Then the number of S_4-extensions $L/\mathbb{Q}$ containing K with $|\operatorname{disc}(L)|$ a prime power is $2^n - 1$ for some integer n. Furthermore, if $K/\mathbb{Q}$ is totally real, then $n > 0$.*

Remark. Example 4.1 is not a counterexample to the last statement, since none of the extensions $K/\mathbb{Q}$ are totally real. In Section 4.3 we will prove the final statement of Theorem 4.5. The remainder will follow from the more general theorem.

Theorem 4.6. *Let F be a number field, and let $\mathcal{P}$ be a set of primes of F. Let K/F be a non-Galois cubic extension, unramified outside of $\mathcal{P}$. Then the number of S_4-extensions L/F containing K and unramified outside of $\mathcal{P}$ is $2^n - 1$ for some nonnegative integer n.*

4.1.3 More examples.

Example 4.7. Let $F = \mathbb{Q}$ and $\mathcal{P} = \{2, 3, \infty\}$. Table 4.1 lists *all* cubic extensions $K/\mathbb{Q}$ unramified outside of $\mathcal{P}$ and the S_4-extensions of $\mathbb{Q}$ unramified outside of $\mathcal{P}$ containing the various K's.

Example 4.8. Let $F = \mathbb{Q}$ and $\mathcal{P} = \{2, 3, 5, \infty\}$. Let $K = \mathbb{Q}(\alpha)$ with α a root of $x^3 - 18x - 12$. There are 15 S_4-extensions of $\mathbb{Q}$ containing K and unramified outside of $\mathcal{P}$. They can be

$f(x)$ **defining** K	$g(x)$ **defining** S_4**-extensions**
$x^3 - 2$	$x^4 - 4x - 6$
$x^3 - 3$	$x^4 - 2x^3 - 4x + 2$
	$x^4 - 2x^3 - 3x^2 - 2x + 7$
	$x^4 - 6x^2 - 4x + 6$
$x^3 - 3x - 4$	$x^4 - 2x^3 + 3x^2 + 2x - 1$
	$x^4 - 16x - 24$
	$x^4 - 6x^2 - 8x + 15$
$x^3 + 3x - 2$	$x^4 - 4x - 3$
	$x^4 - 12x^2 - 16x + 12$
	$x^4 - 8x + 6$
$x^3 - 12$	$x^4 - 6x^2 - 4x + 15$
$x^3 - 6$	$x^4 - 2x^3 - 6x + 3$
$x^3 - 3x - 10$	$x^4 - 6x^2 - 8x + 6$
	$x^4 - 12x^2 - 8x + 18$
	$x^4 - 8x - 6$
$x^3 - 9x - 6$	$x^4 + 3x^2 - 2x + 6$
	$x^4 + 12x^2 - 16x + 24$
	$x^4 + 12x^2 - 4x + 69$
	$x^4 - 24x^2 - 56x - 30$
	$x^4 + 12x^2 - 16x + 60$
	$x^4 + 12x^2 - 8x + 42$
	$x^4 + 12x^2 - 16x + 6$

Table 4.1: Extensions unramified outside of $\mathcal{P} = \{2, 3, \infty\}$

computed as the splitting fields of the following polynomials.

$$
\begin{aligned}
&x^4 - 2x^3 - 4x + 20, && x^4 - 2x^3 + 9x^2 - 4x + 2,\\
&x^4 - 2x^3 + 9x^2 - 6x + 3, && x^4 - x^3 - 9x^2 + 4x + 26,\\
&x^4 - 15x^2 - 10x + 15, && x^4 - 24x^2 - 16x + 24,\\
&x^4 - 6x^2 - 8x + 159, && x^4 + 12x^2 - 32x + 60,\\
&x^4 - 6x^2 - 32x + 87, && x^4 - 60x + 135,\\
&x^4 - 2x^3 + 9x^2 + 32x + 56, && x^4 - 60x^2 - 160x + 60,\\
&x^4 + 90x^2 - 120x + 1215, && x^4 - 60x^2 - 160x + 1860,\\
&x^4 + 30x^2 - 40x + 15
\end{aligned}
$$

Example 4.9. Let $\mathcal{P} = \{2, 3, 5, 7\}$. Let $K = \mathbb{Q}(\alpha)$ with α a root of $x^3 + 9x - 30$. Then there are 31 S_4-extensions containing K and unramified outside of $\mathcal{P}$.

4.2 A group operation on fields

Let F be a number field and let $\mathcal{P}$ be a set of primes of F. Let K/F a non-Galois cubic extension unramified outside of $\mathcal{P}$. Let I denote the Galois closure of K/F. The idea behind the proof of Theorem 4.6 is the following. We will describe an abelian group with exponent 2, where the non-identity elements are the S_4-extensions L/F containing K unramified outside of $\mathcal{P}$, and I acts as the identity. By the fundamental theorem of finitely generated abelian groups (see [10, pg 195]), this group must in fact be isomorphic to C_2^n for some integer n. Such a group has order 2^n.

4.2.1 Composites of S_4-extensions. Defining the group operation depends on uniqueness of certain group extensions of S_3. First, note that S_4 is an extension of S_3 by the Klein 4-group V, via the short exact sequence induced by canonical projection, namely

$$1 \to V \to S_4 \to S_4/V \cong S_3 \to 1.$$

The map $V \to S_4$ is embedding the copy of V which is normal inside S_4. In fact, V is an S_3-module where the action is given by letting elements of S_3 permute the non-identity elements of V.

Lemma 4.10. *S_4 is the only extension of S_3 by V with this action.*

Proof. We apply the Hochschild-Serre spectral sequence (Theorem 2.28) to the group extension

$$1 \to A_3 \to S_3 \to C_2 \to 1$$

and S_3-module V (with the action as above). Then $H^q(A_3, V) = 0$ for all $q \geq 1$ by Theorem 2.26, since the order of V and A_3 are relatively prime, and $H^0(A_3, V) = V^{A_3} = 0$ since A_3 permutes the non-identity elements. Therefore

$$E_2^{pq} := H^p(C_2, H^q(A_3, V)) = H^p(C_2, 0) = 0$$

for all p and q. Therefore E_2 is a page of 0's. Nothing can change on later pages, thus E_∞ is also a page of 0's, and $H^n(S_3, V) = 0$ for all n. In particular, $H^2(S_3, V) = 0$, so there is a unique extension of S_3 by V with the given action by Theorem 2.25. Since S_4 is such an extension, it is the only one. □

Let L/F and L'/F be two distinct S_4-extensions containing K which are both unramified outside of $\mathcal{P}$. Then $L \cap L'$ must be a Galois extension of F containing K, so $L \cap L' \supseteq I$, where I denotes the Galois closure of K/F. Note that $L \cap L'$ must be an intermediate field of L/I, and we have $\mathrm{Gal}(L/I) \cong V$. First, $L \cap L' \neq L$, since L and L' are distinct. If $[L \cap L' : I] = 2$, then $L \cap L'$ is a Galois extension of F of degree 12. Then $L \cap L'$ is fixed by a normal subgroup of S_4 of order 2, which does not exist. Therefore $L \cap L' = I$. Combining this with the fact that $\mathrm{Gal}(L/I) \cong V \cong \mathrm{Gal}(L/I)$, we have $\mathrm{Gal}(LL'/I) = V \oplus V$. Therefore $\mathrm{Gal}(LL'/F)$ is an extension of S_3 by $V \oplus V$. The direct sum is not only of abelian groups, but also a direct sum as S_3-modules. Since cohomology commutes with finite direct sums

(see [26, pg 74]), Lemma 4.10 implies that

$$H^2(S_3, V \oplus V) = H^2(S_3, V) \oplus H^2(S_3, V) = 0 \oplus 0 = 0.$$

Thus we obtain the following corollary.

Corollary 4.11. *Let S_3 act on V by permuting the non-identity elements. Let $V \oplus V$ denote the direct sum as S_3-modules. Then there is a unique extension of S_3 by $V \oplus V$.* □

Therefore $\mathrm{Gal}(LL'/F)$ will always be the same group of order 96. For the rest of the chapter let G denote this group. The group G can be identified in Magma (see [2]) as `SmallGroup(96,227)`.

4.2.2 Structure of the group G. Using Magma we can understand the structure of G. The group G has very few normal subgroups. Besides the trivial ones, there is a normal subgroup of index 2, a normal subgroup of index 6 which we call N, and three normal subgroups of index 24 which we call H_1, H_2, and H_3. Further, we verify in Magma that G/N is isomorphic to S_3, and G/H_i is isomorphic to S_4 for $i = 1, 2, 3$.

If we think of G as $\mathrm{Gal}(LL'/F)$, then the unique subgroup of index 2 fixes the unique quadratic extension F'/F contained in LL'/F. The subgroup N must have fixed field I, and two of H_1, H_2, H_3, say H_1 and H_2, must respectively have L and L' as fixed fields. Let $L * L'$ denote the fixed field of H_3. See Figure 4.1.

Let A be the subgroup of G fixing K, which has order 32. We restrict our attention from G to A. Since A/H_i is a subgroup of $G/H_i \cong S_4$ of order 8, $A/H_i \cong D_8$. Therefore A/H_i has exactly three subgroups of order 4. One of these is cyclic, and the other two are isomorphic to V. One of the latter two subgroups is normal in G/H_i. Using Magma we verify that the normal subgroup is N/H_i for each i. We call this copy of V the even Klein 4-group. The other copy of V is not normal in S_4, and we call this copy of V the odd Klein 4-group. Let N_i be the subgroup of A corresponding to the odd Klein 4-group of A/H_i. Given an

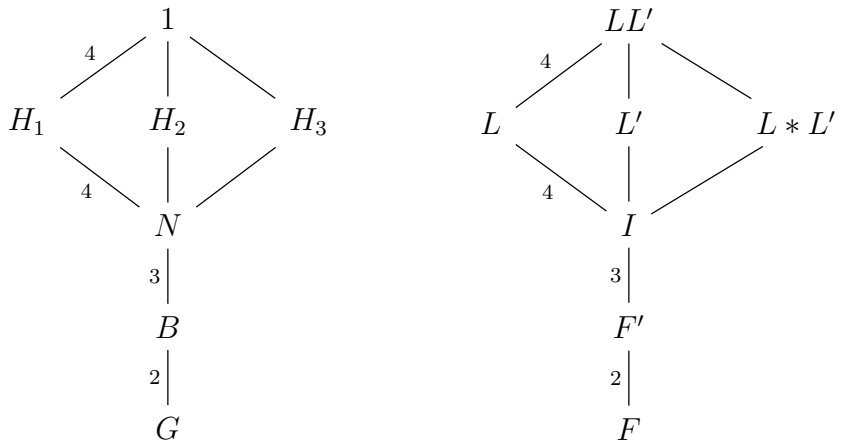

Figure 4.1: The normal sugbroups of G

S_4-extension L/F containing K, let $W_K(L)$ denote the fixed field of the odd Klein 4-group in $\mathrm{Gal}(L/K)$.

The subgroups N and N_i for $i = 1, 2, 3$ fix quadratic extensions of K. Call these fields $L_6 := W_K(L)$, $L_6' := W_K(L')$, and $L_6 * L_6' := W_K(L' * L)$ respectively. Note that $L_6 L_6'/K$ is a Klein 4-extension, and therefore has three intermediary quadratic extensions. Two of these are, of course, L_6 and L_6'. Using Magma we verify that the third is $L_6 * L_6'$. This can be summed up by the lattices in Figure 4.2, which correspond under the Galois correspondence.

4.2.3 Definition of the group operation. We can now describe the group operations alluded to earlier. Let

$$\mathcal{S} = \{S_4\text{-extensions containing } K/F \text{ unramified outside of } \mathcal{P}\} \cup \{I\}.$$

Definition 4.12. Define $* : \mathcal{S} \times \mathcal{S} \to \mathcal{S}$ as follows.

(i) I acts trivially:

$$I * L = L = L * I \qquad \text{for all } L \in \mathcal{S}.$$

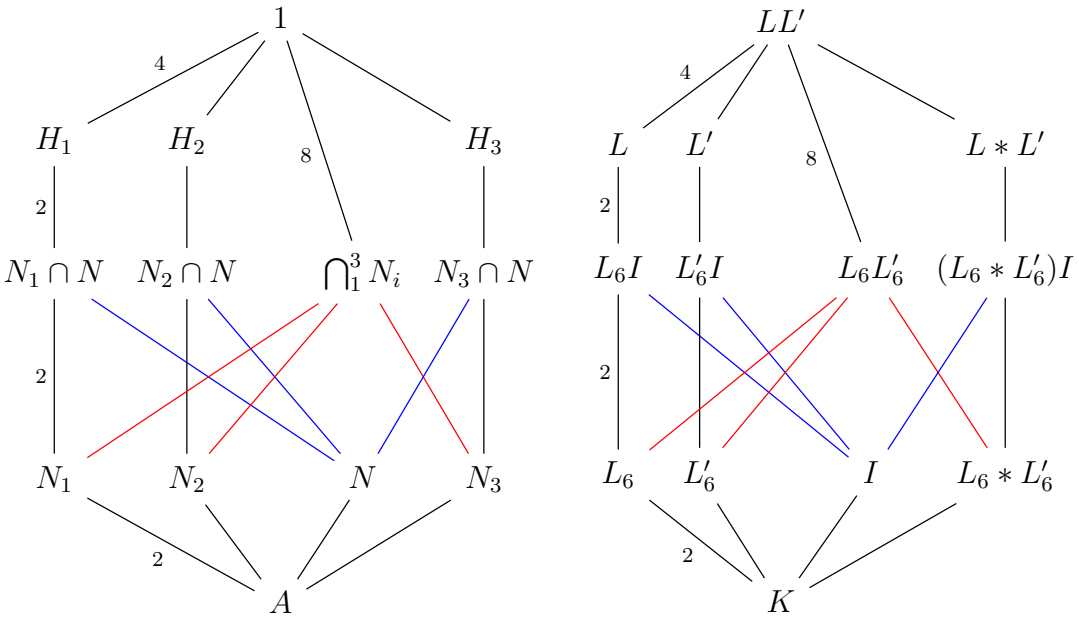

Figure 4.2: The Galois correspondence for several subgroups of G

(ii) Composing an extension with itself gives I:

$$L * L = I \qquad \text{for all } L \in \mathcal{S}.$$

(iii) If L and L' are distinct S_4-extensions, then $L * L'$ is defined as the third S_4-extension contained in LL', as described above.

It is clear that $*$ is well defined, has an identity, has inverses, and is commutative. It remains to show that $*$ is associative. Proving associativity directly would require using a larger composite field. There is a better way.

We describe a similar group operation, which we also call $*$, on the set

$$\mathcal{T} = \{W_K(L) : L \in \mathcal{S} - \{I\}\} \cup \{I\}.$$

Definition 4.13. Define $* : \mathcal{T} \times \mathcal{T} \to \mathcal{T}$ as follows.

(i) I acts trivially:

$$I * W_K(L) = W_K(L) = W_K(L) * I \qquad \text{for all } L \in \mathcal{S} - \{I\}.$$

(ii) Composing an extension with itself gives I:

$$I * I = I \qquad \text{and} \qquad W_K(L) * W_K(L) = I \qquad \text{for all } L \in \mathcal{S} - \{I\}.$$

(iii) If $L, L' \in \mathcal{S} - \{I\}$ are distinct S_4-extensions, then $W_K(L) * W_K(L')$ is defined as the third intermediate subfield of the Klein 4-extension $W_K(L)W_K(L')/K$.

Again, the operation is well defined, has an identity, has inverse, and is commutative. Define $\mathcal{T} \to \mathcal{S}$ by mapping an extensions to its Galois closure over F. Define $W_K : \mathcal{S} \to \mathcal{T}$ by sending $L \mapsto W_K(L)$ as defined above, and $W_K(I) \mapsto I$. It is clear that these maps are inverses, thus $\mathcal{T}$ and $\mathcal{S}$ are in one-to-one correspondence. Further, these maps preserve $*$, since $W_K(L) * W_K(L') = W_K(L * L')$ by the above discussion. Therefore proving associativity for the operation on $\mathcal{T}$ will also prove associativity of the operation on $\mathcal{S}$.

Proposition 4.14. *The binary operation $*$ makes $\mathcal{T}$ and $\mathcal{S}$ into abelian groups.*

Proof of associativity. We will prove associativity for $(\mathcal{T}, *)$ in 4 cases.

Case 1 At least one of the fields is I. We have

$$(I * L_6) * L_6' = L_6 * L_6' = I * (L_6 * L_6'),$$

and

$$(L_6 * I) * L_6' = L_6 * L_6' = L_6 * (I * L_6').$$

Combining these equalities with commutativity we obtain associativity in this case.

Case 2 A field is repeated. We have

$$(L_6 * L_6) * L_6' = I * L_6' = L_6' = L_6 * (L_6 * L_6'),$$

$$(L_6 * L_6') * L_6' = L_6 = L_6 * I = L_6 * (L_6' * L_6'),$$

and

$$\begin{aligned}(L_6 * L_6') * L_6 = (L_6' * L_6) * L_6 = L_6' * (L_6 * L_6) \\ = (L_6' * L_6) * L_6 = L_6 * (L_6' * L_6).\end{aligned}$$

These equations and commutativity implies associativity in this case.

Case 3 The three fields are distinct non-identity, but lie in the same degree 96 extension. In this case,

$$((L_6 * L_6') * L_6) * L_6' = L_6' * L_6' = I = (L_6 * L_6') * (L_6 * L_6').$$

This is symmetric in L_6, L_6', and $L_6 * L_6'$.

Case 4 The three fields are distinct, non-identity, and do not lie in a single degree 96 extension. Each is a quadratic extension, so we can represent each field as $K(\sqrt{\alpha})$ for some element $\alpha \in K$. Then the operation for distinct fields is given by

$$K(\sqrt{\alpha}) * K(\sqrt{\beta}) = K(\sqrt{\alpha\beta}).$$

It is now easy to see that

$$\begin{aligned}(K(\sqrt{\alpha}) * K(\sqrt{\beta})) * K(\sqrt{\gamma}) = K(\sqrt{\alpha\beta\gamma}) \\ = K(\sqrt{\alpha}) * (K(\sqrt{\beta}) * K(\sqrt{\gamma})).\end{aligned}$$

□

4.2.4 Application to Theorem 4.6. We can now prove Theorem 4.6.

Proof of Theorem 4.6. By Proposition 4.14 and the definition of the operation $*$ on $\mathcal{S}$, the pair $(\mathcal{S}, *)$ is an abelian group with exponent 2. Having $\mathcal{P}$ finite forces $\mathcal{S}$ to be finite by [16, pg 122]. Therefore $\mathcal{S} \cong C_2^n$ for some integer n. We have $|C_2^n| = 2^n$, so there are $2^n - 1$ non-identity elements of $\mathcal{S}$. But the non-identity elements of $\mathcal{S}$ are precisely the objects we wished to count. □

4.2.5 Examples of the operation. We close this section with explicit examples of the group operation.

Example 4.15. In Example 4.7, we listed all non-Galois cubic extensions $K/\mathbb{Q}$ unramified outside of $\mathcal{P} = \{2, 3, \infty\}$, along with quartic polynomials defining all S_4-extensions of $\mathbb{Q}$ containing K which are unramified outside of $\mathcal{P}$. Using Jones' number field database and the following PARI code,

```
for(k=1,length(A),
    print("---------------");
    print(k,"  ",A[k]);
    for(j=1,length(B),
        if(nfisincl(A[k],B[j]),
            print("  ",j,"  ",B[j])
        )
    )
)
```

we sort the $W_K(L)$'s for the S_4-extensions by their cubic subfields, which we list in Table 4.2. In the code, `A` is an array containing the polynomials defining the cubic extensions and

`B` is an array containing the polynomials defining the degree six extensions.

For the choices of K where $|\mathcal{S}| = |\mathcal{T}| \leq 4$, the group operation is obvious. Consider $K = \mathbb{Q}(\alpha)$ with α a root of $x^3 - 9x - 6$. Then there are 7 non-identity elements in $\mathcal{T}$, which are given as $\mathbb{Q}(\beta)$ where β is a root of a $g(x)$ listed in Table 4.2. Call these fields $L_1, \ldots, L_7$ respectively. The following PARI code computes the group operation for non-identity elements.

```
composite(f,g) =
    h = polcompositum(f,g)[1];
    SF = nfsubfields(h);
    for(k=1,length(SF),
        p = SF[k][1];
        if(poldegree(p)==6 && nfisisom(f,p)==0 && nfisisom(g,p)==0,
            q = polredabs(p)
        )
    );
    q
```

We can use this to create a multiplication table for the group, given in Figure 4.3.

Example 4.16. We will give an example where Jones' number field database is incomplete, and use the group operation to fill in missing data. Let $K = \mathbb{Q}(\alpha)$ with α a root of $x^3 - 9x - 3$. $K/\mathbb{Q}$ is unramified outside of $\mathcal{P} = \{3, 5, 7, 11, \infty\}$. Jones' database list 61 degree 6 polynomials defining $W_{K'}(L)$ for some S_4-extension L unramified outside of $\mathcal{P}$ above some non-Galois cubic $K'/\mathbb{Q}$. Using the sort algorithm from the previous example,

$f(x)$ **defining** K	$g(x)$ **defining** $W_K(L)$
$x^3 - 2$	$x^6 + 3x^4 + 3x^2 - 1$
$x^3 - 3$	$x^6 - 3x^4 - 6x^2 - 4$
	$x^6 - 3x^4 + 3x^2 - 4$
	$x^6 - 3x^4 + 12x^2 - 4$
$x^3 - 3x - 4$	$x^6 - 3x^2 - 4$
	$x^6 + 6x^2 - 4$
	$x^6 - 6x^4 + 18x^2 - 16$
$x^3 + 3x - 2$	$x^6 - 3x^4 - 4$
	$x^6 - 6x^4 + 18x^2 - 4$
	$x^6 - 6x^4 + 6x^2 - 4$
$x^3 - 12$	$x^6 + 6x^4 + 12x^2 - 4$
$x^3 - 6$	$x^6 - 3x^4 - 6x^3 + 3x^2 - 1$
$x^3 - 3x - 10$	$x^6 + 3x^4 + 9x^2 - 1$
	$x^6 + 24x^2 - 64$
	$x^6 - 30x^2 - 64$
$x^3 - 9x - 6$	$x^6 + 6x^4 - 15x^2 - 4$
	$x^6 - 12x^4 + 30x^2 - 16$
	$x^6 + 6x^4 + 3x^2 - 4$
	$x^6 + 6x^4 + 3x^2 - 16$
	$x^6 + 6x^4 - 42x^2 - 4$
	$x^6 + 6x^4 - 96x^2 - 64$
	$x^6 + 6x^4 - 6x^2 - 4$

Table 4.2: $W_K(L)$ for various K's with $\mathcal{P} = \{2, 3, \infty\}$

	I	L_1	L_2	L_3	L_4	L_5	L_6	L_7
I	I	L_1	L_2	L_3	L_4	L_5	L_6	L_7
L_1	L_1	I	L_5	L_4	L_3	L_2	L_7	L_6
L_2	L_2	L_5	I	L_7	L_6	L_1	L_4	L_3
L_3	L_3	L_4	L_7	I	L_1	L_6	L_5	L_2
L_4	L_4	L_3	L_6	L_1	I	L_7	L_2	L_5
L_5	L_5	L_2	L_1	L_6	L_7	I	L_3	L_4
L_6	L_6	L_7	L_4	L_5	L_2	L_3	I	L_1
L_7	L_7	L_6	L_3	L_2	L_5	L_4	L_4	I

Table 4.3: Multiplication table of $\mathcal{T}$ for K defined by $x^3 - 9x - 6$

we find that only five of these 61 extensions contain K. They are defined by polynomials

$$x^6 - 3x^5 + 3x^4 - x^3 - 9x^2 + 9x - 3$$
$$x^6 + 6x^4 - 15x^2 - 25$$
$$x^6 + 6x^4 - 30x^3 + 21x^2 + 18x - 7$$
$$x^6 - 3x^5 - 42x^4 + 65x^3 + 324x^2 + 198x + 33$$
$$x^6 - 3x^5 + 15x^4 + 143x^3 - 3x^2 - 1245x - 2603$$

Call the number fields defined by these polynomials $L_1, \ldots, L_5$ respectively. Since 5 is not of the form $2^n - 1$, we know that the database is incomplete. Staying within $I, L_1, \ldots, L_5$, the multiplication table is

	I	L_1	L_2	L_3	L_4	L_5
I	I	L_1	L_2	L_3	L_4	L_5
L_1	L_1	I	L_3	L_2	L_5	L_4
L_2	L_2	L_3	I	L_1		
L_3	L_3	L_2	L_1	I		
L_4	L_4	L_5			I	L_1
L_5	L_5	L_4			L_1	I.

However, if we compose L_2 with L_4, we get a polynomial

$$x^6 - 3x^5 - 84x^4 - 187x^3 - 1884x^2 + 11922x - 48869.$$

Let L_6 be the number field defined by this polynomial. Adding this field to our multiplication table, we obtain

	I	L_1	L_2	L_3	L_4	L_5	L_6
I	I	L_1	L_2	L_3	L_4	L_5	L_6
L_1	L_1	I	L_3	L_2	L_5	L_4	
L_2	L_2	L_3	I	L_1	L_6		L_4
L_3	L_3	L_2	L_1	I		L_6	L_5
L_4	L_4	L_5	L_6		I	L_1	L_2
L_5	L_5	L_4		L_6	L_1	I	L_3
L_6	L_6		L_4	L_5	L_2	L_3	I.

Composing L_3 with L_4 yields the polynomial

$$x^6 + 168x^4 - 630x^3 + 5835x^2 - 37080x + 57821.$$

Let L_7 be the number field defined by this polynomial. When we add this into our multipli-

cation table, we get the full multiplication table.

	I	L_1	L_2	L_3	L_4	L_5	L_6	L_7
I	I	L_1	L_2	L_3	L_4	L_5	L_6	L_7
L_1	L_1	I	L_3	L_2	L_5	L_4	L_7	L_6
L_2	L_2	L_3	I	L_1	L_6	L_7	L_4	L_5
L_3	L_3	L_2	L_1	I	L_7	L_6	L_5	L_4
L_4	L_4	L_5	L_6	L_7	I	L_1	L_2	L_3
L_5	L_5	L_4	L_7	L_6	L_1	I	L_3	L_2
L_6	L_6	L_7	L_4	L_5	L_2	L_3	I	L_1
L_7	L_7	L_6	L_5	L_4	L_3	L_2	L_1	I

Remark. It would be difficult to prove that we have found all S_4-extensions of $\mathbb{Q}$ containing K and unramified outside of $\mathcal{P}$. It is possible that we haven't. There could be more S_4-extensions of $\mathbb{Q}$ containing K and unramified outside of $\mathcal{P}$, and we have only found a subgroup of $\mathcal{T}$.

4.3 Constructing an S_4-extension containing a totally real cubic extension

When $F = \mathbb{Q}$ and $K/\mathbb{Q}$ is ramified at a single finite prime $p > 3$, Theorem 4.6 proves the first part of Theorem 4.5. To complete the proof of the Theorem, we need to show that there is at least one S_4-extension $L/\mathbb{Q}$ containing K ramified only at p when $K/\mathbb{Q}$ is totally real. Having $K/\mathbb{Q}$ totally real is equivalent to $p \equiv 1 \pmod 4$ by Lemma 3.7.

4.3.1 Factoring p. The ramification indexes of primes lying over p in $K/\mathbb{Q}$ must divide $[K : \mathbb{Q}] = 3$. Since $p > 3$, the ramification index of each prime lying over p must be prime to p. Thus the extension $K/\mathbb{Q}$ is tamely ramified. We know automatically that $p\mathfrak{O}_K$ either factors as $\mathfrak{p}^3$ or $\mathfrak{p}^2\mathfrak{p}'$. Assuming by way of contradiction that $p\mathfrak{O}_K = \mathfrak{p}^3$, then the ramification index

of p in the Galois closure of $K/\mathbb{Q}$ would have to be divisible by 3. Therefore the inertia field is either $\mathbb{Q}$, or the unique quadratic extension in the Galois closure, $\mathbb{Q}(\sqrt{p^*})$. If the inertia field is $\mathbb{Q}$, then the inertia group is non-cyclic, and p is wildly ramified by Theorem 2.15, a contradiction. If the unique quadratic subfield is $\mathbb{Q}(\sqrt{p^*})$, then $\mathbb{Q}(\sqrt{p^*})/\mathbb{Q}$ is an unramified extension of $\mathbb{Q}$, which is also a contradiction to [6, pg 198]. Therefore $p\mathfrak{O}_K = \mathfrak{p}^2\mathfrak{p}'$. We can then apply [16, pg 58] as in the proof of Lemma 3.6 to see that $v_p(\text{disc}(K)) = 1$. Since this is the only ramified prime, $\text{disc}(K) = \pm p$ by Theorem 2.6. By Stickelberger's Criterion, $\text{disc}(K) = p$, since $p \equiv 1 \pmod 4$.

Consider the narrow class number of K. If it is even, then Heilbronn has shown in [9] that $K/\mathbb{Q}$ is contained in an S_4-extension which is the Galois closure of a quartic field with the same discriminant, which gives us $n > 0$ in the context of Theorem 4.5. However, we will prove what we need, independent of Heilbronn (see Proposition 4.23). For now we will assume that the narrow class number of K is odd, and show that we can construct a quadratic extension of $K(\sqrt{v})/K$ for which $K(\sqrt{v})/\mathbb{Q}$ is not Galois and ramified only at p.

4.3.2 A key lemma. The key to constructing the quadratic extension we want is the following lemma.

Lemma 4.17 ([7, pg 102])**.** *Let $L = K(\sqrt{u})$ be a quadratic extension with $u \in \mathfrak{O}_K$, and let $\mathfrak{p}$ be a prime in $\mathfrak{O}_K$.*

(i) If $2u \notin \mathfrak{p}$, then $\mathfrak{p}$ is unramified in L.

(ii) If $2 \in \mathfrak{p}$, $u \notin \mathfrak{p}$, and $u = b^2 - 4c$ for some $b, c \in \mathfrak{O}_K$, then $\mathfrak{p}$ is unramified in L.

Proof. We follow the proof given in [7].

(i) The polynomial $x^2 - u$ has discriminant $4u \notin \mathfrak{p}$, therefore $x^2 - u$ is separable modulo $\mathfrak{p}$, see [10, pg 259]. Therefore $\mathfrak{p}$ is unramified by Theorem 2.7.

(ii) We can write $L = K(\beta)$ with $\beta = \frac{-b+\sqrt{u}}{2}$. Now β is a root of $x^2 + bx + c$, which has discriminant $b^2 - 4c = u \notin \mathfrak{p}$. Therefore $\mathfrak{p}$ is unramified by Theorem 2.7. □

4.3.3 Units of $\mathfrak{O}_K$ mod 4. We begin by considering the units of $\mathfrak{O}_K$. Since $K/\mathbb{Q}$ is totally real, Dirichlet's Unit Theorem (Theorem 2.10) implies that the unit group of $\mathfrak{O}_K$ is isomorphic to $\mathbb{Z}^2 \times \{\pm 1\}$. Let u_1, u_2 be generators. Then modulo squares, the units of $\mathfrak{O}_K$ are given by $\pm 1, \pm u_1, \pm u_2, \pm u_1 u_2$. To apply condition (ii) of Lemma 4.17 we consider the structure of $(\mathfrak{O}_K/4\mathfrak{O}_K)^\times$.

Theorem 4.18. *Let $K/\mathbb{Q}$ be a cubic extension and $\mathfrak{q}$ a prime of K lying over 2. Let f be the inertial degree of $\mathfrak{q} \mid 2$. Then*

$$(\mathfrak{O}_K/\mathfrak{q}^2)^\times \cong \begin{cases} \mathbb{Z}/2 & \text{if } f = 1, \\ \mathbb{Z}/2 \times \mathbb{Z}/6 & \text{if } f = 2, \\ \mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/14 & \text{if } f = 3. \end{cases}$$

Proof. Consider the sequence

$$0 \to \mathfrak{O}_K/\mathfrak{q} \xrightarrow{\phi} (\mathfrak{O}_K/\mathfrak{q}^2)^\times \xrightarrow{\psi} (\mathfrak{O}_K/\mathfrak{q})^\times \to 1 \tag{4.1}$$

with the following maps. The map $\phi : \mathfrak{O}_K/q \to (\mathfrak{O}_K/\mathfrak{q}^2)^\times$ is given by $\alpha + \mathfrak{q} \mapsto 1 + \alpha\pi + \mathfrak{q}^2$, where $\pi \in \mathfrak{O}_K$ is chosen such that $v_\mathfrak{q}(\pi) = 1$. The map $\psi : (\mathfrak{O}_K/\mathfrak{q}^2)^\times \to (\mathfrak{O}_K/\mathfrak{q})^\times$ is given by $\alpha + \mathfrak{q}^2 \mapsto \alpha + \mathfrak{q}$.

I claim that the sequence is exact. The map ψ is just reduction mod $\mathfrak{q}$, which is a surjective homomorphism. We have that ϕ is a homomorphism, since

$$\begin{aligned} \phi(\alpha + \beta + \mathfrak{q}) &= 1 + \pi(\alpha + \beta) + \mathfrak{q}^2 \\ &= 1 + \pi\alpha + \pi\beta + \pi^2\alpha\beta + \mathfrak{q}^2 \\ &= (1 + \pi\alpha + \mathfrak{q}^2)(1 + \pi\beta + \mathfrak{q}^2) \\ &= \phi(\alpha + \mathfrak{q})\phi(\beta + \mathfrak{q}). \end{aligned}$$

The map ϕ is injective, since if $\phi(\alpha + \mathfrak{q}) = 1 + \mathfrak{q}^2$,

$$1 + \mathfrak{q}^2 = \phi(\alpha + \mathfrak{q}) = 1 + \alpha\pi + \mathfrak{q}^2,$$

which implies that $\alpha\pi \in \mathfrak{q}^2$. Thus $v_{\mathfrak{q}}(\alpha\pi) \geq 2$, so $v_{\mathfrak{q}}(\alpha) \geq 1$, therefore $\alpha \in \mathfrak{q}$. The composition of ϕ and ψ is 0:

$$\psi\phi(\alpha + \mathfrak{q}) = \psi(1 + \pi\alpha + \mathfrak{q}^2) = 1 + \pi\alpha + \mathfrak{q} = 1 + \mathfrak{q}.$$

Suppose that $\psi(\alpha + \mathfrak{q}^2) = 1 + \mathfrak{q}$. Then $\alpha - 1 \in \mathfrak{q}$. We can write $\mathfrak{q} = (\pi, \tau)$, with $v_{\mathfrak{q}}(\tau) \geq 2$ (see [17, pg 61]) so that $\alpha - 1 = \beta\pi + \gamma\tau$ for some $\beta, \gamma \in \mathfrak{O}_K$. In particular,

$$\alpha + \mathfrak{q}^2 = 1 + \beta\pi + \mathfrak{q}^2 = \phi(\beta + \mathfrak{q}).$$

Therefore the sequence is exact.

We have that $\mathfrak{O}_K/\mathfrak{q} \cong (\mathbb{Z}/2\mathbb{Z})^f$, and $(\mathfrak{O}_K/\mathfrak{q})^\times$ is cyclic of order $2^f - 1$. Since the orders are relatively prime, the sequence splits by Theorem 2.26 and Theorem 2.25. When $f = 1$, we obtain $(\mathfrak{O}_K/\mathfrak{q}^2)^\times \cong \mathbb{Z}/2 \times 1$. When $f = 2$,

$$(\mathfrak{O}_K/\mathfrak{q}^2)^\times \cong (\mathbb{Z}/2)^2 \times \mathbb{Z}/3 = \mathbb{Z}/2 \times \mathbb{Z}/6.$$

When $f = 3$,

$$(\mathfrak{O}_K/\mathfrak{q}^2)^\times \cong (\mathbb{Z}/2)^3 \times \mathbb{Z}/7 = \mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/14.$$

□

Corollary 4.19. *Let $K/\mathbb{Q}$ be a non-Galois cubic extension in which 2 is unramified. Let f be the inertial degree of any prime over 2 in the Galois closure of $K/\mathbb{Q}$. Then*

$$(\mathfrak{O}_K/4\mathfrak{O}_K)^\times \cong \mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/2\ell,$$

where $\ell = 2^f - 1$.

Proof. The three options for factorizations of $2\mathfrak{O}_K$ are $2\mathfrak{O}_K = \mathfrak{q}_1\mathfrak{q}_2\mathfrak{q}_3$ with $f = 1$, $2\mathfrak{O}_K = \mathfrak{q}\mathfrak{q}'$ with $f = 2$, and $2\mathfrak{O}_K = \mathfrak{q}$ with $f = 3$. We consider each case using the previous result and the Chinese Remainder Theorem, see [17, pg 253].

If $2\mathfrak{O}_K = \mathfrak{q}_1\mathfrak{q}_2\mathfrak{q}_3$, all primes have inertial degree 1. Thus $(\mathfrak{O}_K/\mathfrak{q}_i^2)^\times \cong \mathbb{Z}/2$ for $i = 1, 2, 3$, and

$$(\mathfrak{O}_K/4\mathfrak{O}_K)^\times \cong \prod_{i=1}^{3}(\mathfrak{O}_K/\mathfrak{q}_i^2)^\times \cong \mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/2 \cong \mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/2\ell.$$

If $2\mathfrak{O}_K = \mathfrak{q}\mathfrak{q}'$, one of the two primes (without loss of generality $\mathfrak{q}$) has inertial degree 2, and the other has inertial degree 1. So $(\mathfrak{O}_K/\mathfrak{q}^2)^\times \cong \mathbb{Z}/2 \times \mathbb{Z}/6$, and $(\mathfrak{O}_K/\mathfrak{q}'^2)^\times \cong \mathbb{Z}/2$. Putting these together we have

$$(\mathfrak{O}_K/4\mathfrak{O}_K)^\times \cong (\mathfrak{O}_K/\mathfrak{q}^2)^\times \times (\mathfrak{O}_K/\mathfrak{q}'^2)^\times \cong \mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/6 \cong \mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/2\ell.$$

If $2\mathfrak{O}_K = \mathfrak{q}$ is prime, then

$$(\mathfrak{O}_K/4\mathfrak{O}_K)^\times = (\mathfrak{O}_K/\mathfrak{q}^2)^\times \cong \mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/14 \cong \mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/2\ell.$$

□

The important consequence of Corollary 4.19 is that $(\mathfrak{O}_K/4\mathfrak{O}_K)^\times$ has a unique subgroup of order 8, and the elements of order dividing 2 are exactly the ℓth powers. We now consider the units of $\mathfrak{O}_K$ mod 4.

Proposition 4.20. *Let $K/\mathbb{Q}$ be a totally real non-Galois cubic extension with odd narrow class number. Let $\ell = 2^f - 1$, where f is the inertial degree of any prime lying over 2 in the Galois closure of $K/\mathbb{Q}$. Let $\{u_1, u_2\}$ be a system of fundamental units for $\mathfrak{O}_K$, and $S = \{\pm 1, \pm u_1^\ell, \pm u_2^\ell, \pm(u_1u_2)^\ell\}$. Then the elements of S have distinct images in $(\mathfrak{O}_K/4\mathfrak{O}_K)^\times$.*

Proof. Suppose by way of contradiction that two elements of S are congruent modulo 4, then since ℓ is odd, their quotient u is a non-square unit congruent to 1 modulo 4. Note that $2u \notin \mathfrak{p}$

for all $\mathfrak{p} \nmid 2$, and for $\mathfrak{p} \mid 2$, $u \notin \mathfrak{p}$, and $u = 1^2 - 4c$ for some $c \in \mathfrak{O}_K$. Therefore $K(\sqrt{u})/K$ is an unramified quadratic extension by Lemma 4.17. However, this is a contradiction, since the narrow class number of K is odd. □

Corollary 4.21. *Let $K/\mathbb{Q}$ be a totally real non-Galois cubic extension and $\ell = 2^f - 1$, where f is the inertial degree of any prime lying over 2 in the Galois closure of $K/\mathbb{Q}$. Let $\{u_1, u_2\}$ be a system of fundamental units for $\mathfrak{O}_K$, and $S = \{\pm 1, \pm u_1^\ell, \pm u_2^\ell, \pm (u_1 u_2)^\ell\}$. Suppose that the images of S are distinct in $(\mathfrak{O}_K/4\mathfrak{O}_K)^\times$ and let H be the image of S in $(\mathfrak{O}_K/4\mathfrak{O}_K)^\times$. Then H is the subgroup of order 8 in $(\mathfrak{O}_K/4\mathfrak{O}_K)^\times$, and a complete set of coset representatives for H consists of the squares in $(\mathfrak{O}_K/4\mathfrak{O}_K)^\times$.*

Proof. The set H consists of eight distinct ℓth powers of $(\mathfrak{O}_K/4\mathfrak{O}_K)^\times$. By Corollary 4.19,

$$|((\mathfrak{O}_K/4\mathfrak{O}_K)^\times)^\ell| = 8,$$

so these are all ℓth powers. It is clear that the product and inverses of ℓth powers are again ℓth powers, so H is a subgroup. There are exactly ℓ squares in $(\mathfrak{O}_K/4\mathfrak{O}_K)^\times$, since by Corollary 4.19,

$$|((\mathfrak{O}_K/4\mathfrak{O}_K)^\times)^2| = \ell.$$

But H contains only one square, namely the image of 1. Therefore each coset of H contains exactly 1 of the ℓ squares. □

4.3.4 Constructing a quadratic extension of K. We now have enough to construct a quadratic extension of $K(\sqrt{u})/K$ which is unramified outside of primes above p, in the case where the narrow class number of K is odd.

Theorem 4.22. *Let $K/\mathbb{Q}$ be a totally real non-Galois cubic extensions ramified at only one prime $p > 3$. Assume that the narrow class number of K is odd. Let $p\mathfrak{O}_K = \mathfrak{p}^2\mathfrak{p}'$ be the factorization into prime ideals. Then there is a quadratic extension of K in which the only finite prime that ramifies is $\mathfrak{p}$.*

Proof. Let h be the narrow class number of K, so that $\mathfrak{p}^h$ is principal, say $\mathfrak{p}^h = \pi\mathfrak{O}_K$. Then the image of πS in $(\mathfrak{O}_K/4\mathfrak{O}_K)^\times$ is a coset of H, therefore πS contains an element v which is a square mod 4 by Corollary 4.21. Observe that v cannot be a square in $\mathfrak{O}_K$, since it generates an odd power of $\mathfrak{p}$. Now we apply Lemma 4.17. Since $p \neq 2$ and $v = b^2 - 4c$ for some $b, c \in \mathfrak{O}_K$, $K(\sqrt{v})/K$ is unramified at primes above 2, and unramified outside of $\mathfrak{p}$ for primes not above 2. □

Proposition 4.23. *If the narrow class number of K is even, then there exists a quadratic extension $K(\sqrt{v})/K$ which is unramified (outside of ∞).*

Proof. The narrow class group is an abelian group of order divisible by 2. Thus there is a subgroup of index 2, which corresponds under the Galois correspondence to a quadratic extension unramified outside of ∞. □

So whether the narrow class number is odd or even, we have constructed a quadratic extension of K, unramified outside of $\{p, \infty\}$ above $\mathbb{Q}$.

4.3.5 The Galois closure of $K(\sqrt{v})$. We now show that in either case the quadratic extension we have constructed has S_4-Galois closure over $\mathbb{Q}$, as desired.

When the narrow class number of K is odd, let $K(\sqrt{v})/K$ denote the quadratic extension constructed in in Theorem 4.22. Then primes above p in $K(\sqrt{v})$ do not have the same ramification index (see Theorem 4.22). Therefore $K(\sqrt{v})/\mathbb{Q}$ is not a Galois extension.

Suppose that the narrow class number of K is even. In this case, let $K(\sqrt{v})/K$ denote the unramified (outside of ∞) quadratic extension of constructed in Proposition 4.23. Then the primes above p in $K(\sqrt{v})$ do not have the same ramification indexes either, since $p\mathfrak{O}_K$ factors as $p\mathfrak{O}_K = \mathfrak{p}^2\mathfrak{p}'$ in K. Therefore $K(\sqrt{v})/\mathbb{Q}$ is not a Galois extension in this case either.

In both cases, $K(\sqrt{v})/\mathbb{Q}$ is not Galois, so the following theorem applies.

Theorem 4.24. *Let $K/\mathbb{Q}$ be a totally real non-Galois cubic extensions ramified only at one prime $p > 3$. Let $K(\sqrt{v})/K$ be a quadratic extension such that $K/\mathbb{Q}$ is non-Galois and*

unramified outside of $\{p, \infty\}$. *Then the Galois group of the Galois closure of* $K(\sqrt{v})/\mathbb{Q}$ *is isomorphic to* S_4.

Proof. Since $K(\sqrt{v})/\mathbb{Q}$ has a cubic subfield (namely K), the possible Galois groups by [6, pg 331] are

$$C_6, \quad S_3, \quad D_6, \quad A_4, \quad S_4, \quad A_4 \times C_2, \quad S_4 \times C_2.$$

Note that $K(\sqrt{v})/\mathbb{Q}$ is not the Galois closure of $K/\mathbb{Q}$ since $K(\sqrt{v})/\mathbb{Q}$ is not a Galois extension. However, the Galois closure of $K(\sqrt{v})/\mathbb{Q}$ must contain the Galois closure of $K/\mathbb{Q}$. Therefore the group has a proper S_3-quotient. This eliminates C_6, S_3, A_4, and $A_4 \times C_2$. Since the Galois closure of $K(\sqrt{v})/\mathbb{Q}$ is ramified only at $p > 2$, there is a unique quadratic sub-extension, namely $\mathbb{Q}(\sqrt{p^*})/\mathbb{Q}$ (see [17, pg 33]). Thus the Galois group has a unique subgroup of index 2, which eliminates D_6 and $S_4 \times C_2$. The only remaining option is for the Galois group of the Galois closure of $K(\sqrt{v})/\mathbb{Q}$ to be isomorphic to S_4. □

4.3.6 Proof of Theorem 4.5.

We can now prove Wong's conjecture.

Proof of Theorem 4.5. Suppose that $K/\mathbb{Q}$ has discriminant plus or minus a power of a prime $p > 3$. This implies that $K/\mathbb{Q}$ is ramified only at $p > 3$. Applying Theorem 4.6, the number of S_4-extensions of $\mathbb{Q}$ containing K is $2^n - 1$ for some $n \geq 0$.

Suppose that $K/\mathbb{Q}$ is totally real. Let h be the narrow class number of K. If h is even, we can apply [9] to construct an S_4-extension of K with discriminant a power of p, or we can use Proposition 4.23 and Theorem 4.24. If h is odd, we apply Theorem 4.22 and Theorem 4.24. In either case, this shows that $n > 0$. □

Bibliography

[1] A. O. L. Atkin and J. Lehner, *Hecke operators on* $\Gamma_0(m)$, Math. Ann. **185** (1970), 134–160. MR 0268123 (42 #3022)

[2] Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265, Computational algebra and number theory (London, 1993). MR MR1484478

[3] Kevin Childers and Darrin Doud, *Octahedral extensions with a common cubic subfield*, (2015), in review.

[4] ———, *Proof of a conjecture of Wong concerning octahedral Galois representations of prime power conductor*, J. Number Theory **154** (2015), 101–104. MR 3339567

[5] John Coates and S. T. Yau (eds.), *Elliptic curves, modular forms & Fermat's last theorem*, International Press, Cambridge, MA, 1997. MR 1605709 (99d:11002)

[6] Henri Cohen, *A course in computational algebraic number theory*, Graduate Texts in Mathematics, vol. 138, Springer-Verlag, Berlin, 1993. MR 1228206 (94i:11105)

[7] David A. Cox, *Primes of the form* $x^2 + ny^2$, second ed., Pure and Applied Mathematics (Hoboken), John Wiley & Sons, Inc., Hoboken, NJ, 2013, Fermat, class field theory, and complex multiplication. MR 3236783

[8] A. Fröhlich and M. J. Taylor, *Algebraic number theory*, Cambridge Studies in Advanced Mathematics, vol. 27, Cambridge University Press, Cambridge, 1993. MR 1215934 (94d:11078)

[9] H. Heilbronn, *On the* 2*-classgroup of cubic fields*, Studies in Pure Mathematics (Presented to Richard Rado), Academic Press, London, 1971, pp. 117–119. MR 0280461 (43 #6181)

[10] Nathan Jacobson, *Basic algebra. I*, second ed., W. H. Freeman and Company, New York, 1985. MR 780184 (86d:00001)

[11] ———, *Basic algebra. II*, second ed., W. H. Freeman and Company, New York, 1989. MR 1009787 (90m:00007)

[12] John W. Jones and David P. Roberts, *A database of number fields*, J. Comput. Math. **17** (2014), no. 1, 595–618.

[13] Chandrashekhar Khare and Jean-Pierre Wintenberger, *Serre's modularity conjecture. I*, Invent. Math. **178** (2009), no. 3, 485–504. MR 2551763 (2010k:11087)

[14] ———, *Serre's modularity conjecture. II*, Invent. Math. **178** (2009), no. 3, 505–586. MR 2551764 (2010k:11088)

[15] Felix Klein, *Lectures on the icosahedron and the solution of equations of the fifth degree*, revised ed., Dover Publications, Inc., New York, N.Y., 1956, Translated into English by George Gavin Morrice. MR 0080930 (18,329c)

[16] Serge Lang, *Algebraic number theory*, second ed., Graduate Texts in Mathematics, vol. 110, Springer-Verlag, New York, 1994. MR 1282723 (95f:11085)

[17] Daniel A. Marcus, *Number fields*, Springer-Verlag, New York-Heidelberg, 1977, Universitext. MR 0457396 (56 #15601)

[18] Jürgen Neukirch, *Class field theory*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 280, Springer-Verlag, Berlin, 1986. MR 819231 (87i:11005)

[19] ———, *Algebraic number theory*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 322, Springer-Verlag, Berlin, 1999. MR 1697859 (2000m:11104)

[20] M. Scott Osborne, *Basic homological algebra*, Graduate Texts in Mathematics, vol. 196, Springer-Verlag, New York, 2000. MR 1757274 (2001d:18013)

[21] Jean-Pierre Serre, *Modular forms of weight one and Galois representations*, Algebraic number fields: L-functions and Galois properties (Proc. Sympos., Univ. Durham, Durham, 1975), Academic Press, London, 1977, pp. 193–268. MR 0450201 (56 #8497)

[22] ———, *Local fields*, Graduate Texts in Mathematics, vol. 67, Springer-Verlag, New York-Berlin, 1979, Translated from the French by Marvin Jay Greenberg. MR 554237 (82e:12016)

[23] ———, *Sur les représentations modulaires de degré* 2 *de* $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, Duke Math. J. **54** (1987), no. 1, 179–230. MR 885783 (88g:11022)

[24] The PARI Group, Bordeaux, *PARI/GP version* `2.7.0`, 2014, available from `http://pari.math.u-bordeaux.fr/`.

[25] M.-F. Vignéras, *Représentations galoisiennes paires*, Glasgow Math. J. **27** (1985), 223–237. MR 819841 (87c:11109)

[26] Charles A. Weibel, *An introduction to homological algebra*, Cambridge Studies in Advanced Mathematics, vol. 38, Cambridge University Press, Cambridge, 1994. MR 1269324 (95f:18001)

[27] Siman Wong, *Arithmetic of octahedral sextics*, J. Number Theory **145** (2014), 245–272. MR 3253303

Index