2011-06-20

Three-Dimensional Galois Representations and a Conjecture of Ash, Doud, and Pollack

Vinh Xuan Dang
Brigham Young University - Provo

Three-Dimensional Galois Representations and a Conjecture of Ash, Doud and Pollack

Vinh Xuan Dang

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
Stephen Humphries
Paul Jenkins

Department of Mathematics

Brigham Young University

August 2011

Abstract

Three-Dimensional Galois Representations and a Conjecture of Ash, Doud and Pollack

Vinh Xuan Dang

Department of Mathematics

Master of Science

In the 1970's and 1980's, Jean-Pierre Serre formulated a conjecture connecting two-dimensional Galois representations and modular forms. The conjecture came to be known as Serre's modularity conjecture. It was recently proved by Khare and Wintenberger in 2008. Serre's conjecture has various important consequences in number theory. Most notably, it played a key role in the proof of Fermat's last theorem. A natural question is, "what is the analogue of Serre's conjecture for higher dimensional Galois representations?" In 2002, Ash, Doud and Pollack formulated a precise statement for a higher dimensional analogue of Serre's conjecture. They also provided numerous computational examples as evidence for this generalized conjecture. We consider the three-dimensional version of the Ash-Doud-Pollack conjecture. We find specific examples of three-dimensional Galois representations and computationally verify the generalized conjecture in all these examples.

Acknowledgments

I am grateful to my advisor Darrin Doud for his immense patience in guiding me through the work in this thesis and for introducing me to algebraic number theory. I am thankful for the generous financial support of the BYU mathematics department. I thank the professors, teachers and fellow graduate students who have taught and inspired me in the highly non-trivial pursuit of mathematical truths and beauties. I thank my parents, my brother and my dear Ngoc, without whose unconditional love and support my life would have been joyless.

Contents

List of Tables

Chapter 1. Introduction

In the 1970's and 1980's, Jean-Pierre Serre formulated a conjecture connecting two-dimensional Galois representations and modular forms. Serre's conjecture has many important consequences in number theory. In fact, the epsilon conjecture (proved by Ribet), a special case of Serre's conjecture, was a significant step towards the proof of Fermat's last theorem. In 2002, Ash, Doud and Pollack formulated a precise statement for a higher dimensional analogue of Serre's conjecture. This thesis is mainly concerned with testing the Ash-Doud-Pollack conjecture in the three dimensional case.

In Chapter 2, we provide the necessary background on modular forms and Galois representations to state Deligne's theorem (Theorem 2.23) and its converse, Serre's conjecture (Conjecture 2.24). These are the two important results that connect modular forms and two-dimensional Galois representations. We also mention various interesting applications of Deligne's theorem and Serre's conjecture.

In Chapter 3, we state the Ash-Doud-Pollack conjecture (Conjecture 3.1) and explain the essential elements in the conjecture. Roughly, the Ash-Doud-Pollack conjecture says that an n-dimensional Galois representation satisfying certain conditions is connected to an element of some cohomology group, a natural generalization of the space of modular forms in Serre's conjecture. "Connected" means that a certain equation, called the attachment equation (equation 3.1), one side of which encodes information about the representation and the other side of which encodes information about the element of the cohomology group, is satisfied. We also describe an important generalization of the predicted weights in Serre's conjecture due to Ash, Doud and Pollack and a procedure to predict these generalized weights due to Doud.

In Chapter 4, we present a construction, due to Doud, of specific three dimensional Galois

representations for which we can expect to do computations and verify the Ash-Doud-Pollack conjecture.

In Chapter 5, we describe our computations of the traces and cotraces related to the representations constructed in Chapter 4. These constitute the side of the attachment equation which encodes information about the representations.

In Chapter 6, we describe the cohomology computations, which form the remaining side of the attachment equation. We finally observe from our computations that the attachment equation is satisfied for all primes up to 47. Hence, the Ash-Doud-Pollack conjecture is computationally verified for the particular representations constructed in Chapter 4.

Chapter 2. The Interplay Between Modular Forms and Two-Dimensional Galois Representations

2.1 Modular Forms

Let $\mathcal{H}$ denote the upper half plane of $\mathbb{C}$, that is, $\mathcal{H} = \{z \in \mathbb{C} : Im(z) > 0\}$. Let $SL_2(\mathbb{Z}) = \{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) : a, b, c, d \in \mathbb{Z}, ad - bc = 1\}$. Then $SL_2(\mathbb{Z})$ acts on $\widehat{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$ as follows: for $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z})$, $\gamma z = \dfrac{az + b}{cz + d}$, for all $z \in \widehat{\mathbb{C}}$ with the convention that if $c \neq 0$, then $\gamma(-d/c) = \infty$, and $\gamma(\infty) = a/c$. If $c = 0$, then $\gamma(\infty) = \infty$. Note that

$$Im(\gamma z) = \frac{Im(z)}{|cz + d|^2},$$

where $Im(z)$ denotes the imaginary part of z. Hence, $\mathcal{H}$ is invariant under the above action of $SL_2(\mathbb{Z})$.

Definition 2.1. Let k be an integer. For $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z})$, the $|[\gamma]_k$ operator on the

space of functions from $\mathcal{H}$ to $\mathbb{C}$ is defined as:

$$(f|[\gamma]_k)(z) = (cz+d)^{-k} f(\gamma z). \tag{2.1}$$

Definition 2.2. Let k be an integer. We say that a function f is *weakly modular of weight* k if $f : \mathcal{H} \longrightarrow \mathbb{C}$ is meromorphic and f satisfies:

$$(f|[\gamma]_k)(z) = f(z), \text{ for all } \gamma \in SL_2(\mathbb{Z}) \text{ and } z \in \mathcal{H}. \tag{2.2}$$

Using the fact that $SL_2(\mathbb{Z})$ is generated by $S = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ and $T = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ ([19], pp. 78-79), one can show:

Proposition 2.3. *Let f be meromorphic on $\mathcal{H}$. f is weakly modular of weight k if and only if for all $z \in \mathcal{H}$:*

$$f(z+1) = f(z), \tag{2.3}$$

$$f(-1/z) = z^k f(z). \tag{2.4}$$

Now, (2.3) implies that f has a Fourier expansion in a neighborhood of 0, that is, $f(z) = \sum_{n \in \mathbb{Z}} a(n) q^n$ where $q = e^{2\pi i z}$.

The $a(n)$ are called the *Fourier coefficients* of f. If $a(n) = 0$ for $n < 0$, we say that f is holomorphic at ∞.

Definition 2.4. Let k be an integer. We say that a function $f : \mathcal{H} \longrightarrow \mathbb{C}$ is a *modular form of weight* k for $SL_2(\mathbb{Z})$ if:

(i) f is holomorphic on $\mathcal{H}$.

(ii) f is weakly modular of weight k.

(iii) f is holomorphic at ∞.

A modular form is a *cusp form* if $a(0) = 0$.

Example 2.5. Let $k > 2$ be an even integer, then $G_k(z) = \sum_{\substack{m,n\in\mathbb{Z} \\ (m,n)\neq(0,0)}} \frac{1}{(mz+n)^k}, z \in \mathcal{H}$ is a nonzero modular form of weight k for $SL_2(\mathbb{Z})$. See [15], Chapter 1.

More generally, one can define modular forms for congruence subgroups of $SL_2(\mathbb{Z})$.

Definition 2.6. Let N be a positive integer. Define $\Gamma_0(N) \supset \Gamma_1(N) \supset \Gamma(N)$ as:

$$\Gamma_0(N) = \{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z}) : c \equiv 0 \bmod N\}; \tag{2.5}$$

$$\Gamma_1(N) = \{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z}) : a \equiv d \equiv 1 \bmod N \text{ and } c \equiv 0 \bmod N\}; \tag{2.6}$$

$$\Gamma(N) = \{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z}) : a \equiv d \equiv 1 \bmod N \text{ and } b \equiv c \equiv 0 \bmod N\}. \tag{2.7}$$

These are subgroups of finite index of $SL_2(\mathbb{Z})$. Any subgroup Γ of $SL_2(\mathbb{Z})$ containing $\Gamma(N)$ is called a congruence subgroup of **level** N.

Definition 2.7. Let Γ be a congruence subgroup of $SL_2(\mathbb{Z})$, and Γ acts on $\mathbb{Q} \cup \{\infty\}$ in the natural way. The *cusps* of Γ are the Γ-equivalence classes of $\mathbb{Q} \cup \{\infty\}$.

Example 2.8. $SL_2(\mathbb{Z})$ has one cusp which can be taken to be ∞. Let p be a prime. Then $\Gamma_0(p)$ has two cusps, which can be taken to be 0 and ∞. Also, $\Gamma_0(p^2)$ has $p+1$ cusps, which can be taken to be 0, ∞ and $-1/kp$ for $k = 1, \ldots, p-1$.

Definition 2.9. Let k be an integer and let Γ be a congruence subgroup of level N and $\epsilon : (\mathbb{Z}/N\mathbb{Z})^\times \longrightarrow \mathbb{C}^\times$ be a Dirichlet character mod N. We say that a function $f : \mathcal{H} \longrightarrow \mathbb{C}$ is a *modular form of weight k for* Γ with character (or nebentype) ϵ if:

(i) f is holomorphic on $\mathcal{H}$.

(ii) $(f|[\gamma]_k)(z) = \epsilon(d)f(z)$, for all $\gamma = \{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma$ and $z \in \mathcal{H}$.

(iii) f is holomorphic at the cusps of Γ.

Remark 2.10. Condition (iii) means the following: consider the distinct Γ-equivalence classes in $\{\gamma(\infty), \gamma \in SL_2(\mathbb{Z})\}$; if for each equivalence class, we choose a representative $\gamma(\infty)$, then $(f|[\gamma]_k)(z) = \sum_{n\in\mathbb{Z}} a(n)q^{\frac{n}{N}}$ where $a(n) = 0$ whenever $n < 0$ (if this holds for a representative, it holds for any element of the class). If in addition we have $a(0) = 0$ at every cusp, then f is called a cusp form for Γ.

Let Γ be a congruence subgroup of $SL_2(\mathbb{Z})$. It is a standard result (see [15], Chapter 3) that for a fixed integer k, the space of modular forms of weight k for Γ with character ϵ (ϵ can be the trivial character), denoted by $\mathcal{M}_k(\Gamma, \epsilon)$, is a finite dimensional complex vector space and so is its subspace of cusp forms, denoted by $\mathcal{S}_k(\Gamma, \epsilon)$. There are important linear operators acting on $\mathcal{M}_k(\Gamma, \epsilon)$, called the Hecke operators. We shall follow [15] in defining the action of Hecke operators on modular forms.

Definition 2.11. Let Γ be a congruence subgroup, $f(z) = \sum_{n\geq 0} a(n)q^n \in \mathcal{M}_k(\Gamma, \epsilon)$ and p be a prime. The action of the Hecke operator T_p on $f(z)$ is defined as:

$$(T_p f)(z) = \sum_{n=0}^{\infty} (a(pn) + \epsilon(p)p^{k-1}a(n/p))q^n, \tag{2.8}$$

where $a(n/p) = 0$ if $p \nmid n$. More generally, for a positive integer $m \geq 2$, the action of T_m is defined as:

$$(T_m f)(z) = \sum_{n=0}^{\infty} \left(\sum_{d|gcd(m,n)} \epsilon(d)d^{k-1}a(mn/d^2) \right) q^n \tag{2.9}$$

One can show (see [15], Chapter 4) that these are indeed linear operators for the space of modular forms on which they act. Moreover, they preserve the subspace of cusp forms and they form a commuting family of linear operators.

Example 2.12. The space $\mathcal{S}_{32}(SL_2(\mathbb{Z}))$ has dimension 2 with a basis $\{f_1, f_2\}$ where $f_1 = q + 50220q^3 + 87866368q^4 + \mathcal{O}(q^5)$ and $f_2 = q^2 + 432q^3 + 39960q^4 + \mathcal{O}(q^5)$. Using formula (2.8) for T_2 (ϵ is trivial) and the fact that Hecke operators preserve $\mathcal{S}_{32}(SL_2(\mathbb{Z}))$, we get

$T_2(f_1) = 2235350016q^2 + \mathcal{O}(q^3) = 0 \cdot f_1 + 2235350016 \cdot f_2$ and $T_2(f_2) = q + 39960q^2 + \mathcal{O}(q^3) = 1 \cdot f_1 + 39960 \cdot f_2$. Thus, the matrix for T_2 is:

$$[T_2] = \begin{pmatrix} 0 & 1 \\ 2235350016 & 39960 \end{pmatrix}.$$

Definition 2.13. Let $f(z)$ be in $\mathcal{M}_k(\Gamma, \epsilon)$ where Γ is a congruence subgroup. If for every positive integer $m \geq 2$, there exists $\lambda_m \in \mathbb{C}$ such that $(T_m f)(z) = \lambda_m f(z)$, then $f(z)$ is called an *eigenform* for the Hecke operators T_m, λ_m is called the *eigenvalue* of T_m corresponding to f.

Example 2.14. The space $\mathcal{S}_{12}(SL_2(\mathbb{Z}))$ has dimension one and it contains the modular form $\Delta(z) = \sum_{n=1}^{\infty} \tau(n)q^n$, where τ is the Ramanujan τ function. Hence, $\mathcal{S}_{12}(SL_2(\mathbb{Z})) = \mathbb{C}\Delta$ and since Hecke operators are endomorphisms for $\mathcal{S}_{12}(SL_2(\mathbb{Z}))$, Δ is an eigenform in this space.

Let $f(z)$ be a normalized eigenform for $S_k(SL_2(\mathbb{Z}))$ or $S_k(\Gamma_1(N), \epsilon)$, where "normalized" means $f(z) = \sum_{n \geq 1} a(n)q^n$ and $a(1) = 1$ (note that $a(1) \neq 0$ for an eigenform). The following proposition exhibits a property of the $a(n)$ which is important in connecting modular forms and Galois representations.

Proposition 2.15. *For each n, a_n is an algebraic integer and the field $\mathbb{K} = \mathbb{Q}(\ldots, a_n, \ldots)$ obtained by adjoining all the Fourier coefficients of f into $\mathbb{Q}$ is a number field, i.e, a finite extension of $\mathbb{Q}$.*

Proof. See [7], pp. 233-234. ■

2.2 The Absolute Galois Group and Galois Representations

Throughout this thesis, we shall let $G_{\mathbb{Q}}$ denote $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$, the group of automorphisms of $\overline{\mathbb{Q}}$ fixing $\mathbb{Q}$ pointwise. One way to understand $G_{\mathbb{Q}}$ is to put on $G_{\mathbb{Q}}$ the Krull topology which admits as open sets all sets of the form $U = \emptyset$ or $U = \bigcup \sigma Gal(\overline{\mathbb{Q}}/\mathbb{K})$ where $\sigma \in G_{\mathbb{Q}}$ and

$\mathbb{K}/\mathbb{Q}$ runs through the finite Galois subextension of $\overline{\mathbb{Q}}/\mathbb{Q}$. This topology makes $G_{\mathbb{Q}}$ into a topological group with the following properties (see [17]).

Proposition 2.16. *$G_{\mathbb{Q}}$ is compact, Hausdorff and totally disconnected.*

Proposition 2.17. *The map $\mathbb{K} \longmapsto Gal(\overline{\mathbb{Q}}/\mathbb{K})$ gives a 1-1 correspondence between the subextension $\mathbb{K}/\mathbb{Q}$ of $\overline{\mathbb{Q}}/\mathbb{Q}$ and the closed subgroups of $G_{\mathbb{Q}}$. The open subgroups of $G_{\mathbb{Q}}$ correspond precisely to the finite subextensions of $\overline{\mathbb{Q}}/\mathbb{Q}$.*

Proposition 2.18. *$G_{\mathbb{Q}} = \varprojlim Gal(\mathbb{K}/\mathbb{Q})$ of the finite Galois groups $Gal(\mathbb{K}/\mathbb{Q})$.*

Remark 2.19. Proposition 2.18 gives us a useful way to interpret the elements of $G_{\mathbb{Q}}$. Recall that the inverse limit $\varprojlim Gal(\mathbb{K}/\mathbb{Q})$ is a subset of $\prod Gal(\mathbb{K}/\mathbb{Q})$ where $\mathbb{K}$ runs through all finite Galois extensions of $\mathbb{Q}$, in particular,

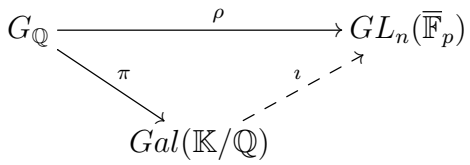
$$\varprojlim Gal(\mathbb{K}/\mathbb{Q}) = \{(\sigma_{\mathbb{K}}) \in \prod Gal(\mathbb{K}/\mathbb{Q}) : \text{ if } \mathbb{K} \subset \mathbb{L} \text{ then } \sigma_{\mathbb{L}}|_{\mathbb{K}} = \sigma_{\mathbb{K}}\}$$

Fix a prime l. Then there is a special element of $G_{\mathbb{Q}}$ associated to l, the Frobenius element at l, denoted by $Frob_l$. $Frob_l$ is the element of $G_{\mathbb{Q}}$ where each component is a Frobenius element of $Gal(\mathbb{K}/\mathbb{Q})$ for some finite Galois extension $\mathbb{K}$ (see appendix A for the definition of Frobenius elements of the Galois group of a finite Galois extension of $\mathbb{Q}$). Note that $Frob_l$ is only well-defined up to Galois conjugacy. We shall see that $Frob_l$ plays an important role in Serre's conjecture and the Ash-Doud-Pollack conjecture.

Definition 2.20. A Galois representation is a continuous homomorphism $\rho : G_{\mathbb{Q}} \longrightarrow GL_n(\overline{\mathbb{F}}_p)$ where continuity is with respect to the Krull topology on $G_{\mathbb{Q}}$ and the discrete topology on $GL_n(\overline{\mathbb{F}}_p)$.

Remark 2.21. Since ρ is continuous, $\mathrm{Ker}\rho$ is an open subgroup of $G_{\mathbb{Q}}$. If $\mathbb{K} = \mathrm{Fix}(\mathrm{Ker}\rho)$, the fixed field corresponding to $\mathrm{Ker}\rho$, then $\mathbb{K}/\mathbb{Q}$ is a finite, Galois extension by Proposition 2.17.

It follows that ρ factors through $Gal(\mathbb{K}/\mathbb{Q})$ in the sense that there exists $\imath : Gal(\mathbb{K}/\mathbb{Q}) \longrightarrow GL_n(\overline{\mathbb{F}}_p)$ such that the following diagram commutes:



where $\pi : G_{\mathbb{Q}} \longrightarrow Gal(\mathbb{K}/\mathbb{Q})$ is the natural projection, $\sigma \longmapsto \sigma|_{\mathbb{K}}$.

Since $\mathbb{K}/\mathbb{Q}$ is finite, it follows that the image of ρ is contained in $GL_n(\mathbb{F})$ for some finite subfield $\mathbb{F}$ of $\overline{\mathbb{F}}_p$, i.e, ρ has finite image.

Definition 2.22. Let l be a prime, we say that the representation $\rho : G_{\mathbb{Q}} \longrightarrow GL_n(\overline{\mathbb{F}}_p)$ is *unramified* at l if l is unramified in $\mathbb{K}/\mathbb{Q}$ where $\mathbb{K} = \text{Fix}(\text{Ker}\rho)$. Moreover, we say that the representation ρ is *odd* if $\det(\rho(c)) = -1$ where $c \in G_{\mathbb{Q}}$ is the complex conjugation automorphism.

2.3 Deligne's Theorem and Serre's Conjecture

We are now in a position to state Deligne's theorem and Serre's conjecture. These two fascinating results connect modular forms and two dimensional Galois representations.

Theorem 2.23 (Deligne)**.** *Let $f(z)$ be a normalized eigenform for $S_k(\Gamma_1(N), \epsilon)$ with Fourier expansion $f(z) = \sum_{n\geq 1} a(n)q^n, a(1) = 1$. Let $\mathbb{K} = \mathbb{Q}(\ldots, a_n, \ldots)$ and p be a prime, then for each ring homomorphism $\varphi : \mathcal{O}_{\mathbb{K}} \longrightarrow \overline{\mathbb{F}}_p$, where $\mathcal{O}_{\mathbb{K}}$ is the ring of integers of $\mathbb{K}$, there exists a representation:*

$$\rho = \rho_\varphi : G_{\mathbb{Q}} \longrightarrow GL_2(\overline{\mathbb{F}}_p)$$

unramified outside pN such that:

$$Tr(\rho(Frob_l)) = \varphi(a_l), \text{ and } \det(\rho(Frob_l)) = \varphi(l^{k-1}\epsilon(l)), \text{ for all } l \nmid pN \tag{2.10}$$

Essentially, Deligne's theorem says that modular forms give rise to Galois representations and they are related by equation (2.10). Serre asked whether the converse is true. He posed Conjecture (2.24) in [22] together with many implications and numerical examples supporting the conjecture.

Conjecture 2.24 (Serre)**.** *Let p be a prime and $\rho : G_{\mathbb{Q}} \longrightarrow GL_2(\overline{\mathbb{F}}_p)$ be an odd, irreducible Galois representation. Then there exist $f \in S_{k(\rho)}(\Gamma_1(N(\rho)), \epsilon(\rho))$ and φ such that equation (2.10) is satisfied, and there is a recipe for the weight $k(\rho)$, the level $N(\rho)$, and the character $\epsilon(\rho)$.*

Conjecture (2.24) is known as Serre's Modularity Conjecture. In short, it says that two-dimensional Galois representations are modular. It was recently proved by Khare and Wintenberger in [14].

2.4 Applications

The interplay between modular forms and Galois representations played an essential role in Wiles' proof of Fermat's Last Theorem (FLT). As described in [6], Serre's conjecture has an important special case called the epsilon conjecture which, together with the Shimura-Taniyama conjecture, would imply FLT. Ribet proved the epsilon conjecture, thus reducing the proof of FLT to a proof of the Shimura-Taniyama conjecture. Wiles proved a large part of the Shimura-Taniyama Conjecture which was sufficient to deduce FLT. However, if one assumes Serre's conjecture, FLT follows easily as a consequence. Indeed, in [22], Serre proved the following,

Theorem 2.25. *Let $p \geq 5$ be a prime number. Assume Conjecture 2.24, then the equation*

$$a^p + b^p = c^p$$

has no solution $a, b, c \in \mathbb{Z}$ with $abc \neq 0$.

In addition, applying theorem 2.25, he proved,

Theorem 2.26. *Let $p \geq 11$ be a prime number. Assume Conjecture 2.24. Let $L \neq p$ be a prime number in the set*

$$S = \{3, 5, 7, 11, 13, 17, 19, 23, 29, 53, 59\}$$

and let α be a nonnegative integer, then the equation

$$a^p + b^p + L^\alpha c^p = 0$$

has no solution $a, b, c \in \mathbb{Z}$ with $abc \neq 0$.

Moreover, he also presented a result of Mazur,

Theorem 2.27. *Assume conjecture 2.24, and let $L \neq 2$ be a prime that is not a Fermat or Mersenne prime, that is, L is a prime not of the form $2^n \pm 1$. Then there exists a number C_L such that for all prime $p \geq C_L$ and integer $\alpha \geq 0$, the equation*

$$a^p + b^p + L^\alpha c^p = 0$$

has no solution $a, b, c \in \mathbb{Z}$ with $abc \neq 0$.

To conclude this chapter, we mention an application of Deligne's theorem due to James and Ono. For each prime p, let $T_p(x)$ be the characteristic polynomial of the Hecke operators T_p acting on $\mathcal{S}_k(SL_2(\mathbb{Z}))$. Using a nice basis for $\mathcal{S}_k(SL_2(\mathbb{Z}))$ such as the one described in [10], one can prove that $T_p(x) \in \mathbb{Z}[x]$. It is an open problem (Maeda's Conjecture) that $T_p(x)$ is irreducible for all primes p. In [13], James and Ono applied Deligne's theorem to prove that $T_p(x)$ is irreducible for a positive proportion of primes p. They constructed Galois representations attached to specific eigenforms and used the properties of these representations as in Theorem 2.23 to prove

Theorem 2.28 (James-Ono)**.** *If there exist distinct primes p and l for which the polynomial $T_p(x)$ is irreducible in $\mathbb{F}_l[x]$, then:*

$$\#\{q < x : T_q(x) \text{ is irreducible in } \mathbb{Q}[x]\} \gg \frac{x}{\log x}.$$

Chapter 3. Ash-Doud-Pollack Conjecture

In this chapter, we follow [2] and [9] closely to describe the Ash-Doud-Pollack Conjecture which generalizes Serre's conjecture (2.24) to higher dimensional representations. We first give the statement of the generalized conjecture, and then explain the elements involved in the subsequent sections.

Conjecture 3.1 (Ash-Doud-Pollack)**.** *Let p be a prime and $\rho : G_{\mathbb{Q}} \longrightarrow GL_n(\overline{\mathbb{F}}_p)$ be an odd, irreducible Galois representation with level N and nebentype ϵ, which is unramified outside of pN. If V is a predicted weight for ρ (see section 3.4), then ρ is attached (in the sense of equation (3.1) in section 3.1) to an eigenclass in $H^s(\Gamma_0(N), V \otimes \epsilon)$ for some $s \geq 0$.*

Remark 3.2. (i) Roughly, one can think of the cohomology group $H^s(\Gamma_0(N), V \otimes \epsilon)$ as a vector space on which the Hecke operators defined in section 3.1 act. An eigenclass is a simultaneous eigenvector for these Hecke operators; it is clearly analogous to the eigenform in Serre's conjecture (2.24).

(ii) If $n = 3$, then s can be taken to be 3.

(iii) By [2], Theorem 3.7 and 3.8, Serre's conjecture is equivalent to the Ash-Doud-Pollack Conjecture for $n = 2$.

3.1 Hecke Operators and The Attachment Equation

Let p be a prime and n, N be positive integers with $gcd(N, p) = 1$. Let $\Gamma_0(N)$ be the subgroup of matrices in $SL_n(\mathbb{Z})$ whose first row is congruent to $(*, 0, \ldots, 0)$ mod N, and S_N be the subsemigroup of integral matrices in $GL_n(\mathbb{Q})$ satisfying the same congruence condition and having positive determinant relatively prime to N. Let $\mathcal{H}(N)$ be the $\overline{\mathbb{F}}_p$-algebra of double cosets $\Gamma_0(N)\backslash S_N/\Gamma_0(N)$. Then $\mathcal{H}(N)$ is a commutative algebra which acts on the cohomology and homology of $\Gamma_0(N)$. When a double coset acts on cohomology and homology, we call it a Hecke operator. $\mathcal{H}(N)$ clearly contains double cosets of the form $\Gamma_0(N)D(l,k)\Gamma_0(N)$ where l is a prime not dividing N, $0 \leq k \leq n$ and:

$$D(l,k) = \begin{pmatrix} 1 & & & & & \\ & \ddots & & & & \\ & & 1 & & & \\ & & & l & & \\ & & & & \ddots & \\ & & & & & l \end{pmatrix},$$

with the first $n-k$ diagonal entries equal to 1 and the last k diagonal entries equal to l. A Hecke operator generated by $D(l,k)$ is denoted by $T(l,k)$.

Definition 3.3. Let V be an $\mathcal{H}(pN)$-module and suppose that $v \in V$ is a simultaneous eigenvector for all $T(l,k)$, that is, $T(l,k)v = a(l,k)v$ where $a(l,k) \in \overline{\mathbb{F}}_p$ for all primes $l \nmid pN$ and all $0 \leq k \leq n$. Let $\rho : G_{\mathbb{Q}} \longrightarrow GL_n(\overline{\mathbb{F}}_p)$ be a Galois representation unramified outside pN, i.e, unramified at every prime $l \nmid pN$. We say that ρ is *attached* to v if the following equation holds for all $l \nmid pN$:

$$\sum_{k=0}^{n} (-1)^k l^{k(k-1)/2} a(l,k) X^k = \det(I - \rho(Frob_l)X). \tag{3.1}$$

Remark 3.4. In the right hand side of equation (3.1), the coefficient of X is $Tr(\rho(Frob_l))$ and the coefficient of X^n is $(-1)^n \det(\rho(Frob_l))$.

Remark 3.5. Consider the case $n = 3$; we shall call the coefficient of X^2 in the right hand side of (3.1) the *cotrace* of $\rho(Frob_l)$ and denote it by $T_2(\rho(Frob_l))$. For each $l \nmid pN$, equation (3.1) is satisfied if and only if $a(l,1) = Tr(\rho(Frob_l))$ and $la(l,2) = T_2(\rho(Frob_l))$ and $l^3a(l,3) = \det(\rho(Frob_l))$. However, the condition $l^3a(l,3) = \det(\rho(Frob_l))$ is automatic for our choice of weights (see 3.4 and [9]). Therefore, we have:

Proposition 3.6. *In the case of three-dimensional Galois representations, equation (3.1) is satisfied for appropriate weights if and only if*

$$a(l,1) = Tr(\rho(Frob_l)) \quad \textit{and} \quad la(l,2) = T_2(\rho(Frob_l)), \ \textit{for all } l \nmid pN. \tag{3.2}$$

3.2 Level and Nebentype

Let $\rho : G_{\mathbb{Q}} \longrightarrow GL_n(\overline{\mathbb{F}}_p)$ be a Galois representation. We shall follow [22] in defining the level and nebentype associated to ρ.

3.2.1 Level. For each prime $l \neq p$, fix a decomposition group D_l in $G_{\mathbb{Q}}$ together with a filtration of ramification subgroups $G_{l,i}$, $i \geq 0$ inside D_l. Note that $G_{l,0} = I_l$, the inertia group at l (see Appendix A and also [21], Chapter 4 for the definition of the ramification subgroups). For each $i \geq 0$ let $g_i = |\rho(G_{l,i})|$. Then g_i is a finite number since the image of ρ is finite. Let $M = \overline{\mathbb{F}}_p^n$, and let $G_{\mathbb{Q}}$ act on M via ρ in the natural way. Let M_i be the subspace of M fixed by $G_{l,i}$ and define:

$$n(l,\rho) = \sum_{i=0}^{\infty} \frac{g_i}{g_0} \dim M/M_i.$$

We have:

Proposition 3.7. *(i) $n(l,\rho)$ is a positive integer.*

(ii) $n(l,\rho) = 0$ if and only if $G_{l,0} = \{1\}$, that is, if and only if ρ is unramified at l.

(iii) $n(l,\rho) = \dim M/M_0$ if and only if $G_{l,1} = \{1\}$, that is, if and only if ρ is tamely ramified at l.

Proof. See [21], chapter IV and [20], section 19.3. ■

We are now in a position to define the level $N = N(\rho)$ associated to ρ.

Definition 3.8. With ρ as above, define the *level*:

$$N = N(\rho) = \prod_{l \neq p} l^{n(l,\rho)} \tag{3.3}$$

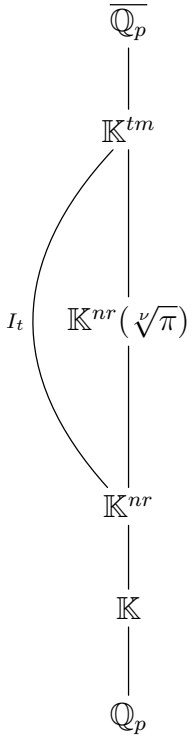
Clearly, N is finite since ρ is unramified for all but finitely many primes; moreover, N is relatively prime to p.

3.2.2 Nebentype. The determinant of ρ is a homomorphism $\det\rho : G_{\mathbb{Q}} \longrightarrow \overline{\mathbb{F}}_p^{\times}$. By [22], we can consider $\det\rho$ as a character of $G_{\mathbb{Q}}$ whose conductor divides pN, where N is the level of ρ defined in (3.3). It follows that (see [22]) $\det\rho$ can be factored as $\det\rho = \omega^k\epsilon$ where ω is the mod p cyclotomic character of $G_{\mathbb{Q}}$, k is an integer $0 \leq k \leq p-2$, and ϵ is a Dirichlet character $\epsilon : (\mathbb{Z}/N\mathbb{Z})^{\times} \longrightarrow \overline{\mathbb{F}}_p^{\times}$. Here ϵ is called the *nebentype* of ρ.

3.3 Fundamental Characters

We define the notion of fundamental characters of level n following the level 1 case defined by Serre in [22]. These fundamental characters play a prominent role in predicting the weights for both Serre's conjecture and the Ash-Doud-Pollack conjecture, a topic we do not treat in any depth for this thesis. We shall, however, need them in an essential way when computing the trace of the specific Galois representations constructed in Chapter 4 (see Section 5.1).

Fix a prime p and a positive integer n, let $\mathbb{K}$ be a finite extension of $\mathbb{Q}_p$, the field of p-adic numbers. Let $\mathbb{K}^{tm}$ be the maximal tamely ramified extension of $\mathbb{K}$. Let $\mathbb{K}^{nr}$ be the maximal unramified extension of $\mathbb{K}$. See [17], Chapter 2, Section 7 for the existence and uniqueness of $\mathbb{K}^{nr}$ and $\mathbb{K}^{tm}$. Let $\nu = p^n - 1$ and let π be a uniformizer of $\mathbb{K}$, then we have the sequence of Galois extensions $\mathbb{K}^{nr} \subset K^{nr}(\sqrt[\nu]{\pi}) \subset \mathbb{K}^{tm}$. Let $I_t = Gal(\mathbb{K}^{tm}/\mathbb{K}^{nr})$. Then by Galois theory, $Gal(\mathbb{K}^{nr}(\sqrt[\nu]{\pi})/\mathbb{K}^{nr})$ is a quotient of I_t. The relations among these fields are summarized in the following diagram.



The group $Gal(\mathbb{K}^{nr}(\sqrt[\nu]{\pi})/\mathbb{K}^{nr})$ is isomorphic to μ_ν, the group of ν-th roots of unity, via the isomorphism $\sigma \longmapsto \dfrac{\sigma(\sqrt[\nu]{\pi})}{\sqrt[\nu]{\pi}}$. Also, μ_ν is isomorphic to $\mathbb{F}_{p^n}^\times$ via an explicit map. Indeed, $\mu_\nu \subset \mathbb{K}^{nr}$. Let $\mathfrak{p}^{nr}$ be the unique maximal ideal of $\mathbb{K}^{nr}$. Then $\mathbb{K}^{nr}/\mathfrak{p}^{nr} \cong \overline{\mathbb{F}}_p$ via the canonical map and so this gives an embedding $\mu_\nu \hookrightarrow \overline{\mathbb{F}}_p$. Since every element of μ_ν has order dividing $p^n - 1$, the image of μ_ν under this embedding is $\mathbb{F}_{p^n}^\times$.

Therefore, we get a homomorphism $\psi : I_t \longrightarrow \mathbb{F}_{p^n}^\times$ as follows:

$$I_t \longrightarrow Gal(\mathbb{K}^{nr}(\sqrt[\nu]{\pi})/\mathbb{K}^{nr}) \xrightarrow{\cong} \mu_\nu \xrightarrow{\cong} \mathbb{F}_{p^n}^\times$$
$$\psi$$

Let $\varphi : \mathbb{F}_{p^n}^\times \longrightarrow \mathbb{F}_{p^n}^\times$ be the Frobenius automorphism, $\varphi(x) = x^p$. For each $1 \leq j \leq n$, let $\psi_{n,j} = \varphi^j \circ \psi$. The homomorphisms $\psi_{n,1}, \ldots, \psi_{n,n}$ are called the *fundamental characters of level n*.

Remark 3.9. By the fact that I_t is a procyclic group (see [22]), any character of I_t with finite image is a power of some fundamental character.

3.4 Weights

By the work of Eichler-Shimura (see [23], Chapter 8), Ash-Stevens (in [3] and [4]), and Ash-Doud-Pollack (in [2]), the natural generalization of the weight in Serre's conjecture is an irreducible $GL_n(\mathbb{F}_p)$-module. The complete set of irreducible $GL_n(\mathbb{F}_p)$-modules can be parameterized by the set of p-restricted n-tuples (see Definition 3.10). This is attributed to Green by Doty and Walker (see [8]). Doud (in [9]) gave a procedure to predict the weights V for which one can expect to find an eigenclass in $H^s(\Gamma_0(N), V \otimes \epsilon)$ attached to a supersingular Galois representation ρ, that is, Conjecture 3.1 holds. We shall describe this procedure here.

Definition 3.10. An n-tuple of integers $(a_{n-1}, \ldots, a_0)$ is *p-restricted* if for $1 \leq i \leq n-1$,

$$0 \leq a_i - a_{i-1} \leq p-1,$$

and

$$0 \leq a_0 \leq p-2.$$

By [8], one has:

Proposition 3.11. *The set of irreducible $\overline{\mathbb{F}}_p[GL_n(\mathbb{F}_p)]$-modules is in one-to-one correspondence with the set of all p-restricted n-tuples.*

When an irreducible module corresponds to a p-restricted tuple, say $(a_{n-1}, \ldots, a_0)$, we shall denote the module by $F(a_{n-1}, \ldots, a_0)$.

Now, for a supersingular Galois representation ρ, by [2], Theorem 2.16, the restriction of ρ to the inertia group at p can be diagonalized in terms of the fundamental characters of level n, $\psi_{n,j}, 1 \leq j \leq n$ defined in section 3.3. In particular,

$$\rho|_{I_p} \sim \begin{pmatrix} \psi_{n,1}^m & & \\ & \ddots & \\ & & \psi_{n,n}^m \end{pmatrix},$$

for some positive integer m.

Let $a_0, \ldots, a_{n-1}$ be integers such that:

$$m \equiv a_0 + a_1 p + \ldots + a_{n-1} p^{n-1} (\text{mod } p^n - 1).$$

Let $(b_{n-1}, \ldots, b_0)$ be a relabelling of the a_i such that $b_i \geq b_{i-1}$ for $0 \leq i \leq n-1$. Define $c_i = b_i - i$. If the n-tuple $c_{n-1}, \ldots, c_0$ is p-restricted, then $F(c_{n-1}, \ldots, c_0)$ is a weight for which one can expect Conjecture 3.1 holds.

Example 3.12. If $n = 3, p = 11, m = 14$ (which will appear later in our calculations), then the predicted weights, given by the above procedure, are $F(19, 11, 1)$, $F(9, 1, 1)$, $F(10, 9, 2)$, $F(1, 0, 0)$, $F(11, 10, 0)$, and $F(20, 12, 9)$. (See Appendix B.3 for the calculations of these weights using GP-Pari).

Chapter 4. Building Three-Dimensional Galois Representations

This thesis is concerned with testing the Ash-Doud-Pollack conjecture in the three-dimensional case. In this chapter, we shall describe a construction (developed in [9]) of explicit three dimensional Galois representations which makes the computations of the important quantities in both sides of equation (3.1) possible and thus allows us to verify that the conjecture is valid in many cases. We start with some preliminaries from class field theory and representation theory.

4.1 Global Class Field Theory

4.1.1 Ray Class Groups and Ray Class Characters. We shall define some basic notions of global class field theory (as in [5]) which will be needed in our construction.

Definition 4.1. Let $\mathbb{K}$ be a number field. A modulus $\mathfrak{m}$ of $\mathbb{K}$ is a pair $(\mathfrak{m}_0, \mathfrak{m}_\infty)$ where $\mathfrak{m}_0$ is an ideal of $\mathcal{O}_\mathbb{K}$, the ring of integers of $\mathbb{K}$, and $\mathfrak{m}_\infty$ is a set of real embeddings of $\mathbb{K}$. We write this formally as $\mathfrak{m} = \mathfrak{m}_0\mathfrak{m}_\infty$.

Example 4.2. $\mathfrak{m} = (2)(3)^2(5)^3\infty$ is a modulus of $\mathbb{Q}$ where $\mathfrak{m}_0 = (2)(3)^2(5)^3$ and $\mathfrak{m}_\infty = \infty$ is the unique real embedding of $\mathbb{Q}$ into $\mathbb{C}$. In general, a modulus $\mathfrak{m}$ of $\mathbb{Q}$ is either (n) or $(n)\infty$ where n is an integer.

Definition 4.3. Let $\mathfrak{m} = \mathfrak{m}_0\mathfrak{m}_\infty$ and $\mathfrak{n} = \mathfrak{n}_0\mathfrak{n}_\infty$ be two moduli of $\mathbb{K}$. We say that $\mathfrak{n}$ divides $\mathfrak{m}$ if $\mathfrak{n}_0|\mathfrak{m}_0$, i.e, $\mathfrak{n}_0 \supset \mathfrak{m}_0$ and $\mathfrak{n}_\infty \subset \mathfrak{m}_\infty$. In particular, we say that a prime $\mathfrak{p}$ of $\mathbb{K}$ divides $\mathfrak{m}$ if $\mathfrak{p}$ divides $\mathfrak{m}_0$.

Throughout the rest of this section, let $\mathfrak{m} = \mathfrak{m}_0\mathfrak{m}_\infty$ be a modulus of $\mathbb{K}$.

Definition 4.4. Let $\mathfrak{a}$ be a fractional ideal of $\mathbb{K}$, i.e, a finitely generated $\mathcal{O}_{\mathbb{K}}$-submodule of $\mathbb{K}$; it is a standard result (see [17], Chapter 1), that the set of fractional ideals of the Dedekind domain $\mathcal{O}_{\mathbb{K}}$ is a free Abelian group generated by the prime ideals of $\mathcal{O}_{\mathbb{K}}$. Consequently, $\mathfrak{a}$ can be factored uniquely as $\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}(\mathfrak{a})}$ where $v_{\mathfrak{p}}(\mathfrak{a})$ are integers and $v_{\mathfrak{p}}(\mathfrak{a}) = 0$ for all but finitely many prime ideals $\mathfrak{p}$ of $\mathcal{O}_{\mathbb{K}}$. The $v_{\mathfrak{p}}(\mathfrak{a})$ is called the $\mathfrak{p}$-*adic valuation of* $\mathfrak{a}$. We say that $\mathfrak{a}$ is *coprime to the modulus* $\mathfrak{m}$ if $v_{\mathfrak{p}}(\mathfrak{a}) = 0$ for all $\mathfrak{p}|\mathfrak{m}_0$. The set of fractional ideals of $\mathbb{K}$ comprime to $\mathfrak{m}$ is denoted by $I_{\mathfrak{m}}(\mathbb{K})$. $I_{\mathfrak{m}}(\mathbb{K})$ is a group under multiplication.

Definition 4.5. Let α be an element of $\mathbb{K}^{\times}$, we say that

$$\alpha \equiv 1 \, (mod^{*}\mathfrak{m})$$

if $v_{\mathfrak{p}}(\alpha - 1) \geq v_{\mathfrak{p}}(\mathfrak{m}_0)$ for all prime $\mathfrak{p}$ dividing $\mathfrak{m}_0$, and $\sigma(\alpha) > 0$ for all embeddings $\sigma \in \mathfrak{m}_{\infty}$. Note that $v_{\mathfrak{p}}(\alpha - 1)$ is defined to be the $\mathfrak{p}$-adic valuation of the fractional principal ideal $(\alpha - 1)\mathcal{O}_{\mathbb{K}}$.

Let $P_{\mathfrak{m}}(\mathbb{K}) = \{\alpha\mathcal{O}_{\mathbb{K}} : \alpha \equiv 1(mod^{*}\mathfrak{m})\}$, that is, the set of principal fractional ideals of $\mathcal{O}_{\mathbb{K}}$ generated by elements $\alpha \equiv 1(mod^{*}\mathfrak{m})$. Clearly, $P_{\mathfrak{m}}(\mathbb{K})$ is a subgroup of $I_{\mathfrak{m}}(\mathbb{K})$. Define $Cl_{\mathfrak{m}}(\mathbb{K}) = I_{\mathfrak{m}}(\mathbb{K})/P_{\mathfrak{m}}(\mathbb{K})$. $Cl_{\mathfrak{m}}(\mathbb{K})$ is called the *ray class group* modulo $\mathfrak{m}$ of $\mathbb{K}$.

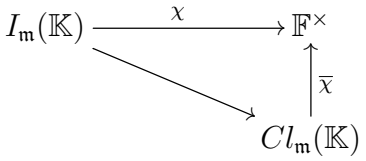
Example 4.6. (i) If $\mathfrak{m}_0 = \mathcal{O}_{\mathbb{K}}$ and $\mathfrak{m}_{\infty} = \emptyset$, then $I_{\mathfrak{m}}(\mathbb{K}) = I(\mathbb{K})$, the group of fractional ideals of $\mathbb{K}$ and $P_{\mathfrak{m}}(\mathbb{K}) = P(\mathbb{K})$, the group of fractional principal ideals of $\mathbb{K}$. Hence, $Cl_{\mathfrak{m}}(\mathbb{K}) = I(\mathbb{K})/P(\mathbb{K}) = Cl(\mathbb{K})$, the ideal class group of $\mathbb{K}$.

(ii) Let $\mathbb{K} = \mathbb{Q}$ and $\mathfrak{m} = (n)$ be a modulus of $\mathbb{K}$ where n is a positive integer, then $Cl_{\mathfrak{m}}(\mathbb{K}) \cong (\mathbb{Z}/n\mathbb{Z})^{\times}/\{\pm 1\}$. If $\mathfrak{m} = (n)\infty$, then $Cl_{\mathfrak{m}}(\mathbb{K}) \cong (\mathbb{Z}/n\mathbb{Z})^{\times}$.

For a number field $\mathbb{K}$ and a modulus $\mathfrak{m}$ of $\mathbb{K}$, $Cl_{\mathfrak{m}}(\mathbb{K})$ is a finite Abelian group (see [5], section 3.2). Its cardinality is denoted by $h_m(\mathbb{K})$. In general, it is difficult to compute ray class groups by hand. Fortunately, this can be done quite easily for certain types of number fields using, for instance, Magma or GP/Pari (see Appendix B.1).

Definition 4.7. Let $\mathfrak{m}$ be a modulus of the number field $\mathbb{K}$. A *ray class character* χ modulo $\mathfrak{m}$ is a group homomorphism from $I_{\mathfrak{m}}(\mathbb{K})$ to the multiplicative group $\mathbb{F}^{\times}$ of a field $\mathbb{F}$ such that $P_{\mathfrak{m}}(\mathbb{K}) \subset \mathrm{Ker}(\chi)$.

Remark 4.8. Since $P_{\mathfrak{m}}(\mathbb{K}) \subset \mathrm{Ker}(\chi)$, χ induces a homomorphism $\overline{\chi} : Cl_{\mathfrak{m}}(\mathbb{K}) = I_{\mathfrak{m}}(\mathbb{K})/P_{\mathfrak{m}}(\mathbb{K}) \longrightarrow \mathbb{F}^{\times}$ such that the diagram



commutes. Therefore, we can identify ray class characters χ modulo $\mathfrak{m}$ with characters $\overline{\chi}$ of the finite Abelian group $Cl_{\mathfrak{m}}(\mathbb{K})$.

4.1.2 Artin Reciprocity.

We state a simplified version of one of the most important theorems of class field theory, the Artin Reciprocity Theorem, which will be utilized in our computations.

Theorem 4.9. *Let $\mathbb{K}$ be a number field and $\mathfrak{m}$ be a modulus of $\mathbb{K}$. Then there exists a field extension $\mathbb{K}_{\mathfrak{m}}$ of $\mathbb{K}$ (called the* ray class field *modulo $\mathfrak{m}$ of $\mathbb{K}$) such that $\mathbb{K}_{\mathfrak{m}}/\mathbb{K}$ is an Abelian extension and the Galois group $Gal(\mathbb{K}_{\mathfrak{m}}/\mathbb{K})$ is isomorphic to $Cl_{\mathfrak{m}}(\mathbb{K})$, the ray class group modulo $\mathfrak{m}$ of $\mathbb{K}$. Moreover, the only primes of $\mathbb{K}$ that are ramified in $\mathbb{K}_{\mathfrak{m}}$ are the primes dividing $\mathfrak{m}$.*

There is a canonical isomorphism from $Cl_{\mathfrak{m}}(\mathbb{K}) = I_{\mathfrak{m}}(\mathbb{K})/P_{\mathfrak{m}}(\mathbb{K})$ to $Gal(\mathbb{K}_{\mathfrak{m}}/\mathbb{K})$. Let us describe it here, assuming the existence of $\mathbb{K}_{\mathfrak{m}}$. We first define a map, denoted by $\left(\frac{\cdot}{\mathbb{K}_m/\mathbb{K}}\right)$, called the *Artin map*, from $I_{\mathfrak{m}}(\mathbb{K})$ to $Gal(\mathbb{K}_{\mathfrak{m}}/\mathbb{K})$.

For a fractional ideal $\mathfrak{a} \in I_{\mathfrak{m}}(\mathbb{K})$, factor $\mathfrak{a}$ as $\mathfrak{a} = \prod_{\mathfrak{p}|\mathfrak{a}} \mathfrak{p}^{v_{\mathfrak{p}}(\mathfrak{a})}$. Since $\mathfrak{a}$ is coprime to $\mathfrak{m}$, none of the prime divisors of $\mathfrak{a}$ divides $\mathfrak{m}$. It follows that the prime divisors $\mathfrak{p}$ of $\mathfrak{a}$ are all unramified in $\mathbb{K}_{\mathfrak{m}}$ since $\mathbb{K}_{\mathfrak{m}}$ is ramified only at the primes dividing $\mathfrak{m}$ by construction (see [17], chapter 6). Moreover, also by construction, $\mathbb{K}_{\mathfrak{m}}/\mathbb{K}$ is an Abelian extension. Therefore,

$Frob_{\mathfrak{p}}$ is a well-defined element of $Gal(\mathbb{K}_{\mathfrak{m}}/\mathbb{K})$ for each $\mathfrak{p}|\mathfrak{a}$ (see Appendix A, Remark A.4). Thus, we can define $\left(\frac{\mathfrak{a}}{\mathbb{K}_{\mathfrak{m}}/\mathbb{K}}\right)$ as:

$$\left(\frac{\mathfrak{a}}{\mathbb{K}_{\mathfrak{m}}/\mathbb{K}}\right) = \prod_{\mathfrak{p}|\mathfrak{a}} Frob_{\mathfrak{p}}^{v_{\mathfrak{p}}(\mathfrak{a})},$$

where the product of the $Frob_{\mathfrak{p}}$ is the group product of $Gal(\mathbb{K}_{\mathfrak{m}}/\mathbb{K})$.

One can show that

$$\left(\frac{\cdot}{\mathbb{K}_m/\mathbb{K}}\right) : I_{\mathfrak{m}}(\mathbb{K}) \longrightarrow Gal(\mathbb{K}_{\mathfrak{m}}/\mathbb{K})$$

is a well-defined surjective group homomorphism whose kernel is $P_m(\mathbb{K})$ and therefore, it induces an isomorphism from $I_{\mathfrak{m}}(\mathbb{K})/P_{\mathfrak{m}}(\mathbb{K}) = Cl_{\mathfrak{m}}(\mathbb{K})$ to $Gal(\mathbb{K}_{\mathfrak{m}}/\mathbb{K})$. In particular, $\left(\frac{\mathfrak{p}}{\mathbb{K}_{\mathfrak{m}}/\mathbb{K}}\right) = Frob_{\mathfrak{p}}$ for every prime ideal $\mathfrak{p}$ of $\mathbb{K}$ which does not divide $\mathfrak{m}$.

4.2 Induced Representations

We shall define induced representations as in [12], chapter 3. Throughout this section, a representation of a group G is a homomorphism $\rho : G \longrightarrow GL(V)$ where V is a finite dimensional vector space over a field $\mathbb{F}$ and $GL(V)$ is the group of automorphisms of V. There is a natural action of G on V, namely, for any $g \in G, v \in V$, $g \cdot v = \rho(g)(v)$. This action makes V into a G-module. By abuse of language, V itself is called a representation of G, and we shall also interchangeably refer to both V and ρ as a representation of G.

Definition 4.10. Let G be a group and H be a subgroup of G of finite index, and let R be a complete set of left coset representatives for G/H. Let V be a representation of G and let W be a H-stable subspace of V, that is, $hW = W$ for all $h \in H$; W is then a representation of H. We say that the representation V is *induced* by W, denoted as $V = Ind_H^G W$ if

$$V = \bigoplus_{r \in R} rW.$$

Remark 4.11. (i) This definition is independent of the choice of coset representatives. In fact, if r and s represent the same coset of H, that is, $rH = sH$, then $r = sh$ for some $h \in H$. It follows that $rW = shW = sW$.

(ii) By definition, each $v \in V$ can be written uniquely as $v = \sum_{r \in R} rw_r$ with $w_r \in W$.

(iii) It follows immediately from the definition that $dim(V) = \sum_{r \in R} dim(rW) = [G : H]dim(W)$.

Example 4.12. (i) Let G be a finite group of order n and V be an n-dimensional vector space with a basis $\{e_g\}_{g \in G}$, indexed by G. Define an action of G on V as $s \cdot e_g = e_{sg}$ for each $s \in G$ and extend linearly. This action makes V into a representation of G, called the *regular representation* of G. Let H be a subgroup of G and W be the subspace of V with basis $\{e_h\}_{h \in H}$. Then $V = Ind_H^G W$.

(ii) Let V_1, V_2 be representations of G induced by representations W_1, W_2 of a subgroup of finite index H of G, respectively. Then $V_1 \oplus V_2$ is induced by $W_1 \oplus W_2$.

The following proposition guarantees that given a subgroup H of finite index of a group G and a representation W of H, there always exists a representation V of G that is induced from W and V is unique up to isomorphism.

Proposition 4.13. *Let H be a subgroup of finite index of a group G and W be a representation of H, then there exists a unique representation V of G, up to isomorphism, such that $V = Ind_H^G W$.*

Proof. See [20], Theorem 11. ■

Let V be a representation of G. We define an important function associated to V, called the character of V, denoted by χ_{V}.

Definition 4.14. Let V be a representation of G, the *character* χ_{V} is a function $\chi_{\mathrm{V}} : G \longrightarrow \mathbb{F}$ defined by:

$$\chi_{\mathrm{V}}(g) = Tr(g|_{\mathrm{V}}), \text{ for all } g \in G$$

where $g|_{\mathrm{V}}$ is the element of $GL(V)$ given by, $g|_{\mathrm{V}} : V \longrightarrow V$, $g|_{\mathrm{V}}(v) = gv,$ for all $v \in V$.

The following theorem (see [20], chapter 3, theorem 12) lets one compute χ_{V} from χ_{W} if V is the induced representation $V = Ind_H^G W$.

Theorem 4.15 (Frobenius formula)**.** *Assume the hypotheses of definition (4.10). If* $V = Ind_H^G W$*, then*

$$\chi_V(g) = \sum_{\substack{r \in R \\ r^{-1}gr \in H}} \chi_W(r^{-1}gr), \forall g \in G$$

Proof. We have, $V = \bigoplus_{r \in R} rW$. For each $g \in G$, g permutes the direct summands rW and only those summands rW that are stable under the action of g contribute to the trace of $g|_{\mathrm{V}}$; but rW is stable under g if and only if $r^{-1}gr \in H$. Therefore,

$$\chi_{\mathrm{V}}(g) = Tr(g|_{\mathrm{V}}) = \sum_{\substack{r \in R \\ r^{-1}gr \in H}} Tr(g|_{\mathrm{rW}}) = \sum_{\substack{r \in R \\ r^{-1}gr \in H}} Tr(r^{-1}gr|_{\mathrm{W}}) = \sum_{\substack{r \in R \\ r^{-1}gr \in H}} \chi_{\mathrm{W}}(r^{-1}gr).$$

■

4.3 Three Dimensional Representations Induced from Ray Class Characters

4.3.1 The Construction. Now, we are in the position to present the construction in [9] of the three dimensional Galois representations which allow us to verify the Ash-Doud-Pollack Conjecture (3.1) for various cases.

Fix a prime p and let $\mathbb{K}$ be an S_3-extension of $\mathbb{Q}$ with a fixed cubic subfield $\mathbf{F}$ satisfying:

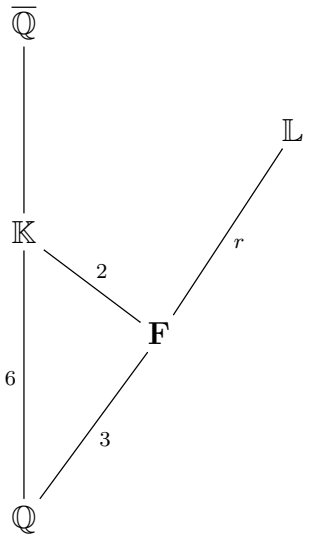
(i) The inertial degree of p in $\mathbb{K}/\mathbb{Q}$ is 3.

(ii) The class number of $\mathbf{F}$, $h(\mathbf{F})$ is 1.

(iii) The discriminant $disc(\mathbf{F}/\mathbb{Q})$ satisfies $|disc(\mathbf{F}/\mathbb{Q})| = q$, where $q > 3$ is a prime.

(iv) $\mathbb{L}$, the ray class field modulo p of $\mathbf{F}$ (to be precise, the modulus is $p\mathcal{O}_{\mathbf{F}}$), has Galois group $Gal(\mathbb{L}/\mathbf{F})$ cyclic of order r with $r|(p^3-1)$, $r \nmid (p^2-1)$ or $r \nmid (p-1)$.

The relation among these fields is summarized in the following diagram:



Condition (i) implies that p is totally inert in $\mathbf{F}$; that is, $p\mathcal{O}_{\mathbf{F}} = \mathfrak{p}$, where $\mathfrak{p}$ is a prime ideal of $\mathcal{O}_{\mathbf{F}}$. Condition (ii) is equivalent to saying that $\mathcal{O}_{\mathbf{F}}$, the ring of integers of $\mathbf{F}$, is a principal ideal domain (PID). In fact, as mentioned in Section 1.6 of [17], we have,

Proposition 4.16. *Let $\mathbf{F}$ be a number field with ring of integers $\mathcal{O}_{\mathbf{F}}$. Then $h(\mathbf{F}) = 1$ if and only if $\mathcal{O}_{\mathbf{F}}$ is a PID.*

Proof. Suppose $h(\mathbf{F}) = 1$, recall that the class number is the order of $Cl(\mathbf{F})$, the ideal class group of $\mathbf{F}$ and that $Cl(\mathbf{F}) = I(\mathbf{F})/P(\mathbf{F})$ where $I(\mathbf{F})$ is the group of fractional ideals of $\mathbf{F}$ and $P(\mathbf{F})$ is the subgroup of $I(\mathbf{F})$ consisting of fractional principal ideals of $\mathbf{F}$. Therefore, every fractional ideal of $\mathbf{F}$ is principal and in particular, every ideal of $\mathcal{O}_{\mathbf{F}}$ is principal, i.e., $\mathcal{O}_{\mathbf{F}}$ is a PID.

Conversely, suppose that $\mathcal{O}_{\mathbf{F}}$ is a PID. Let $\mathfrak{a}$ be a fractional ideal of $\mathbf{F}$. By definition, $\mathfrak{a}$ is a finitely generated $\mathcal{O}_{\mathbf{F}}$-submodule of $\mathbf{F}$, generated by elements $a_1, \ldots, a_k$ of $\mathbf{F}$. Let d

be a common denominator of the a_j. Then $d\mathfrak{a} \subset \mathcal{O}_{\mathbf{F}}$ and thus $d\mathfrak{a}$ is actually an ideal of $\mathcal{O}_{\mathbf{F}}$. By assumption, $d\mathfrak{a}$ is principal, that is, $d\mathfrak{a} = \alpha\mathcal{O}_{\mathbf{F}}$ for some $\alpha \in \mathcal{O}_{\mathbf{F}}$. It follows that $\mathfrak{a} = \left(\frac{\alpha}{d}\right)\mathcal{O}_{\mathbf{F}}$. Therefore, every fractional ideal of $\mathbf{F}$ is principal and so, $I(\mathbf{F}) = P(\mathbf{F})$ which implies $h(\mathbf{F}) = 1$. ■

Proposition 4.17. *Condition (iii) of section 4.3.1 implies that* $\mathbb{K}/\mathbb{Q}$ *is ramified only at* $|disc(\mathbf{F}/\mathbb{Q})| = q$ *with ramification index* 2.

Proof. By Theorem 24 and Theorem 34 in [16], a rational prime l is ramified in a number field $\mathbf{F}$ if and only if l divides $|disc(\mathbf{F}/\mathbb{Q})|$. In particular, $|disc(\mathbf{F}/\mathbb{Q})| = q$ implies that q is the only prime that is ramified in $\mathbf{F}$. It follows that $q\mathcal{O}_{\mathbf{F}}$ factors in $\mathbf{F}$ as either $q\mathcal{O}_{\mathbf{F}} = \mathfrak{q}^3$ or $q\mathcal{O}_{\mathbf{F}} = \mathfrak{q}_1^2\mathfrak{q}_2$. Since $q > 3$, $\mathbf{F}$ is tamely ramified over $\mathbb{Q}$ (see Appendix A) and this excludes the first option for factorization; otherwise, the power of q in $|disc(\mathbf{F}/\mathbb{Q})|$ must be $e(\mathfrak{q}|q) - 1 = 2$ (Proposition 13, Chapter 3, [21]), contradicting our assumption. Therefore, $q\mathcal{O}_{\mathbf{F}} = \mathfrak{q}_1^2\mathfrak{q}_2$. Since $\mathbb{K}/\mathbb{Q}$ is Galois, by the discussion preceding Definition A.1 in Appendix A, the ramification index and inertia degree of any prime of $\mathbb{K}$ lying over q depend only on q; call these e and f, respectively. Since ramification indices are multiplicative in towers (see [16], p. 65), the factorization of q in $\mathbf{F}$ implies that $2|e$. Let g be the number of primes of $\mathbb{K}$ lying over q. By the factorization of q in $\mathbf{F}$, we have $g \geq 2$. By Appendix A again, $efg = [\mathbb{K} : \mathbb{Q}] = 6$ and it must follow that $e = 2, g = 3$ and $f = 1$. Therefore, q factors in $\mathbb{K}$ as $q\mathcal{O}_{\mathbb{K}} = (\mathfrak{Q}_1\mathfrak{Q}_2\mathfrak{Q}_3)^2$. We have thus showed that $\mathbb{K}/\mathbb{Q}$ is ramified at q with ramification index 2. Now, we show that q is the only prime ramified in $\mathbb{K}$. It suffices to show that $disc(\mathbb{K}/\mathbb{Q})$ is only divisible by q. Since $e = 2$ and $q > 3$, $\mathbb{K}/\mathbb{Q}$ is tamely ramified, by Proposition 13 of [21], $disc(\mathbb{K}/\mathbb{Q}) = q^{\sum_{i=1}^{g}(e-1)f} = q^3$ and we are done. ■

Now consider condition (iv) of 4.3.1. By remark (4.8), we can identify the ray class characters modulo p with the characters of $Cl_p(\mathbf{F})$. By Theorem 4.9, $Cl_p(\mathbf{F})$ is isomorphic to $Gal(\mathbb{L}/\mathbf{F})$; and by condition (iv), $Gal(\mathbb{L}/\mathbf{F}) \cong \mathbb{Z}/r\mathbb{Z}$ where $r|(p^3-1)$. Whence, there exist

$\varphi(r)$ ray class characters modulo p having order r with values in $\mathbb{F}_{p^3}^{\times}$. Indeed, this follows from:

Proposition 4.18. *Let r, s be positive integers then:*

$$Hom_{\mathbb{Z}}(\mathbb{Z}/r\mathbb{Z}, \mathbb{Z}/s\mathbb{Z}) \cong \mathbb{Z}/t\mathbb{Z},$$

where $t = gcd(r, s)$.

Proof. This is Exercise 10.2.6 in [11]. Let M be an $\mathbb{Z}$-module and $Ann_M(r)$ be the annihilator in M of r. We first show that $Hom_{\mathbb{Z}}(\mathbb{Z}/r\mathbb{Z}, M) \cong Ann_M(r)$.

In fact, define a map $\Psi : Hom_{\mathbb{Z}}(\mathbb{Z}/r\mathbb{Z}, M) \longrightarrow Ann_M(r)$ as follows: for an element f in $Hom_{\mathbb{Z}}(\mathbb{Z}/r\mathbb{Z}, M)$, define $\Psi(f) = \alpha$ if $f(\overline{1}) = \alpha$. Since $0 = f(\overline{r}) = rf(\overline{1}) = r\alpha$, Ψ is well-defined. It is a homomorphism. Moreover, for any $\beta \in Ann_M(r)$, define $f_\beta : \mathbb{Z}/r\mathbb{Z} \longrightarrow M$ by $f(\overline{k}) = k\beta$. Then $f_\beta \in Hom_{\mathbb{Z}}(\mathbb{Z}/r\mathbb{Z}, M)$ and $\Psi(f_\beta) = \beta$. Hence, Ψ is a surjective homomorphism. It is easy to see that it is also injective and so we obtain an isomorphism between $Hom_{\mathbb{Z}}(\mathbb{Z}/r\mathbb{Z}, M)$ and $Ann_M(r)$.

Now let $M = \mathbb{Z}/s\mathbb{Z}$. We claim that $Ann_M(r) = \mathbb{Z}/t\mathbb{Z}$. Indeed, $\alpha \in Ann_M(r)$ if and only if $\alpha \in \mathbb{Z}/s\mathbb{Z}$ and $r\alpha = 0$, if and only if $\alpha \in \mathbb{Z}/s\mathbb{Z}$ and $|\alpha|$ divides $gcd(r, s) = t$. Thus, $Ann_M(r)$ is the subgroup of the cyclic group $\mathbb{Z}/r\mathbb{Z}$ consisting of elements of order dividing t, and it follows that it must be isomorphic to $\mathbb{Z}/t\mathbb{Z}$. ■

Apply Proposition (4.18) with $s = p^3 - 1$, and $r|s$. We obtain $Hom_{\mathbb{Z}}(Gal(\mathbb{L}/\mathbf{F}), \mathbb{F}_{p^3}^{\times}) \cong Hom_{\mathbb{Z}}(\mathbb{Z}/r\mathbb{Z}, \mathbb{Z}/(p^3 - 1)\mathbb{Z}) \cong \mathbb{Z}/r\mathbb{Z}$ and so there are $\varphi(r)$ group homomorphisms from $Gal(\mathbb{L}/\mathbf{F})$ to $\mathbb{F}_{p^3}^{\times}$ of order r. Therefore, there are $\varphi(r)$ ray class characters modulo p of order r. Let $\chi : Gal(\mathbb{L}/\mathbf{F}) \longrightarrow \mathbb{F}_{p^3}^{\times}$ be one of them. Then all such characters are of the forms χ^j where $1 \leq j \leq r$ and $gcd(j, r) = 1$.

Let $G_{\mathbf{F}} = Gal(\overline{\mathbb{Q}}/\mathbf{F})$ and $\theta : G_{\mathbf{F}} \longrightarrow Gal(\mathbb{L}/\mathbf{F})$ be the natural projection, $\theta(\sigma) = \sigma|_{\mathbb{L}}$ for $\sigma \in G_{\mathbf{F}}$. Then for each j we obtain a character $\overline{\chi}_j : G_{\mathbf{F}} \longrightarrow \mathbb{F}_{p^3}^{\times}$ by composition:

$$G_{\mathbf{F}} \xrightarrow{\quad\theta\quad} Gal(\mathbb{L}/\mathbf{F}) \xrightarrow{\quad\chi^j\quad} \mathbb{F}_{p^3}^{\times}, \qquad G_{\mathbf{F}} \xrightarrow{\quad\overline{\chi}_j\quad} \mathbb{F}_{p^3}^{\times}$$

Consider $\overline{\chi}_j$ as a one dimensional representation of $G_{\mathbf{F}}$. Put $\rho_j = Ind_{G_{\mathbf{F}}}^{G_{\mathbb{Q}}} \overline{\chi}_j$. Since $[G_{\mathbb{Q}} : G_{\mathbf{F}}] = [\mathbf{F} : \mathbb{Q}] = 3$, Remark 4.11 part (iii), tells us that ρ_j is a three dimensional representation of $G_{\mathbb{Q}}$. Thus, we have finally delivered the construction of three dimensional Galois representations induced from ray class characters of a cubic subfield of an S_3-extension of $\mathbb{Q}$.

Doud ([9]) showed that a three dimensional Galois representation ρ constructed this way is supersingular. The level of ρ, as defined in equation (3.3), is $N(\rho) = q$. The nebentype of ρ, as defined in 3.2.2, is ϵ_q, the unique quadratic character mod q. More specifically, $\epsilon_q = \left(\frac{\cdot}{q}\right)$, the Legendre symbol (see Section 5.2). Here, $q = disc(\mathbf{F}/\mathbb{Q})$ is the unique prime ramified in $\mathbb{K}/\mathbb{Q}$ by Proposition 4.17.

Moreover, the following theorem (Doud [9]) gives properties of these representations which are essential in computing the trace and cotrace.

Theorem 4.19. *Let ψ be one of the $\overline{\chi}_j$ and $\rho : G_{\mathbb{Q}} \longrightarrow GL_3(\mathbb{F}_{p^3})$ be the representation induced from ψ as in the above construction; let V (resp. W) be the $G_{\mathbb{Q}}$ (resp. $G_{\mathbb{F}}$) modules corresponding to ρ (resp. ψ). Let $\pi : G_{\mathbb{Q}} \longrightarrow Gal(\mathbb{K}/\mathbb{Q})$ be the natural projection, and let $\{g_0, g_1, g_2\}$ be a complete set of coset representatives for $G_{\mathbb{Q}}/G_{\mathbf{F}}$. Then ρ satisfies:*

(i) If $g \in G_{\mathbb{Q}}$ with $\pi(g)$ having order 1, then $\rho(g)$ has eigenvalues $\psi(g_j^{-1} g g_j)$ for $j = 0, 1, 2$. As a result, $Tr(\rho(g)) = \sum_{j=0}^{2} \psi(g_j^{-1} g g_j)$ and $T_2(\rho(g)) = \sum_{i<j} \psi(g_i^{-1} g g_i)\psi(g_j^{-1} g g_j)$.

(ii) If $g \in G_{\mathbb{Q}}$ with $\pi(g)$ having order 2, then for exactly one $j, 0 \leq j \leq 2$, $g' = g_j^{-1} g g_j$ is an element of $G_{\mathbf{F}}$, and $Tr(\rho(g)) = \psi(g')$, $T_2(\rho(g)) = \psi(g')^{-1} \det(\rho(g))$.

(iii) If $g \in G_{\mathbb{Q}}$ with $\pi(g)$ having order 3, then $Tr(\rho(g)) = T_2(\rho(g)) = 0$.

Proof. (i) Suppose $g \in G_{\mathbb{Q}}$ and $|\pi(g)| = 1$. Then $g|_{\mathbb{K}} = id_{\mathbb{K}}$, in particular, g fixes $\mathbb{K}$ and so it fixes $\mathbf{F}$, that is, $g \in G_{\mathbf{F}}$. Since $G_{\mathbf{F}}$ is a closed subgroup of $G_{\mathbb{Q}}$, we must have $g_j^{-1} g g_j \in G_{\mathbf{F}}$ for $j = 0, 1, 2$. Let w be an arbitrary element of W, we claim that for any $j = 0, 1, 2$, $g_j \cdot w$ is an eigenvector of $\rho(g)$ with corresponding eigenvalues $\psi(g_j^{-1} g g_j)$. Here:

$$\rho : \ G_{\mathbb{Q}} \longrightarrow GL(V) \longrightarrow GL_3(\mathbb{F}_{p^3}).$$

$$g \longmapsto \rho(g) \longmapsto [\rho(g)]$$

We have:

$$\begin{aligned} [\rho(g)](g_j \cdot w) &= \rho(g)(g_j \cdot w) = g \cdot (g_j \cdot w) = (g g_j) \cdot w \\ &= (g_j (g_j^{-1} g g_j)) \cdot w = g_j \cdot ((g_j^{-1} g g_j) \cdot w) \\ &= g_j \cdot (\psi(g_j^{-1} g g_j) w) = \rho(g_j)((\psi(g_j^{-1} g g_j) w) \\ &= \psi(g_j^{-1} g g_j) \rho(g_j)(w) = \psi(g_j^{-1} g g_j)(g_j \cdot w) \end{aligned}$$

Here we used the fact that $g_j^{-1} g g_j \in G_{\mathbf{F}}$ and $\psi : G_{\mathbf{F}} \longrightarrow \mathbb{F}_{p^3}^{\times}$ is a 1-dimensional representation; so $(g_j^{-1} g g_j) \cdot w = \psi(g_j^{-1} g g_j) w$ by definition.

It follows that $\rho(g)$ has eigenvalues $\psi(g_j^{-1} g g_j)$ for $j = 0, 1, 2$ and the formula for the trace and cotrace of $\rho(g)$ follows at once.

(ii) Suppose that $|\pi(g)| = 2$. Then $|\pi(g_j^{-1} g g_j)| = |\pi(g)| = 2$ for $j = 0, 1, 2$. Thus, there exists exactly one j such that $g' = g_j^{-1} g g_j$ fixes $\mathbb{F}$ and so, $g' \in G_{\mathbf{F}}$. By the Frobenius formula, (Theorem 4.15), we have:

$$Tr(\rho(g)) = \sum_{\substack{j=0 \\ g_j^{-1} g g_j \in G_{\mathbf{F}}}}^{2} \psi(g_j^{-1} g g_j) = \psi(g').$$

To compute the cotrace $T_2(\rho(g))$ note that, for a 3-by-3 matrix A, the cotrace of A is

$T_2(A) = \lambda_1\lambda_2 + \lambda_1\lambda_3 + \lambda_2\lambda_3 = (\frac{1}{\lambda_1} + \frac{1}{\lambda_2} + \frac{1}{\lambda_3})\lambda_1\lambda_2\lambda_3 = Tr(A^{-1})\det(A)$ where λ_j are the eigenvalues of A. Thus, it follows that $T_2(\rho(g)) = \psi(g')^{-1}\det(\rho(g))$.

(iii) Suppose that $|\pi(g)| = 3$. Then none of the $g_j^{-1}gg_j$ is in $G_{\mathbf{F}}$, by the Frobenius formula again, $Tr(\rho(g)) = 0$ and by the above relation between the trace and cotrace, $T_2(\rho(g)) = 0$.

■

4.3.2 Examples. We search for S_3-extensions $\mathbb{K}$ of $\mathbb{Q}$ that satisfy the conditions at the beginning of this section, using GP/Pari [1] (see appendix B.2 for the codes) and Jones' table of number fields ramified at specified primes (available at `http://hobbes.la.asu.edu/NFDB/`). We found the following examples of such extensions for small primes p.

p	5	7	11	13
Defining Polynomial	$x^3 - x^2 + x - 8$	$x^3 - x^2 - 2x + 5$	$x^3 - x^2 + x + 2$	$x^3 - 2x - 3$
Level	1619	439	139	211
Nebentype	$\left(\frac{\cdot}{1619}\right)$	$\left(\frac{\cdot}{439}\right)$	$\left(\frac{\cdot}{139}\right)$	$\left(\frac{\cdot}{211}\right)$

Table 4.1: Defining polynomials for S_3-extensions.

Chapter 5. Computing the Trace and Cotrace

The purpose of this thesis is to construct specific examples of three-dimensional representations and verify Conjecture 3.1 in these examples. Recall that for the three-dimensional case, Conjecture 3.1 says that for every predicted weight $F(c_2, c_1, c_0)$ (as in 3.4), there exists an eigenclass $v \in H^3(\Gamma_0(N), F(c_2, c_1, c_0) \otimes \epsilon)$ such that v is attached to ρ. More specifically, v is attached to ρ if and only if

$$a(l,1) = Tr(\rho(Frob_l)) \quad \text{and} \quad la(l,2) = T_2(\rho(Frob_l)), \text{ for all prime } l \nmid pN$$

where $a(l,1)$ and $a(l,2)$ are the eigenvalues corresponding to v of the Hecke operators $T(l,2)$ and $T(l,2)$, respectively.

In this chapter, we shall compute $Tr(\rho(Frob_l))$ and $T_2(\rho(Frob_l))$ for the representations ρ constructed in Section 4.3 of the previous chapter.

5.1 Computation Strategy

5.1.1 An Important Observation. Our computation strategy relies on the following crucial observation, made in [9]:

Theorem 5.1. *Fix a prime p and let $\mathbf{K}$ be an S_3-extension of $\mathbb{Q}$ with a fixed cubic subfield $\mathbf{F}$ satisfying the conditions of section 4.3.1. Let $l \nmid pN$ be a prime. Suppose l factors in $\mathbf{F}$ as $l\mathcal{O}_{\mathbf{F}} = \mathfrak{p}_l\mathfrak{p}_l'$ where the inertia degree of $\mathfrak{p}_l$ and $\mathfrak{p}_l'$ over l is 1 and 2, respectively. By Proposition 4.16, $\mathcal{O}_{\mathbf{F}}$ is a PID, hence, $\mathfrak{p}_l = \alpha\mathcal{O}_{\mathbf{F}}$ for some $\alpha \in \mathcal{O}_{\mathbf{F}}$. Then*

$$Tr(\rho(Frob_l)) = \overline{\alpha}^m, \tag{5.1}$$

where $\overline{\alpha}$ is the image of α under the canonical projection $\mathcal{O}_{\mathbf{F}} \longrightarrow \mathcal{O}_{\mathbf{F}}/\mathfrak{p}$; $\mathfrak{p}$ is the unique prime in $\mathbf{F}$ lying over p, and m is a positive integer such that $\frac{p^3-1}{r} | m$.

Remark 5.2. Note that $Tr(\rho(Frob_l))$ is an element of $\mathbb{F}_{p^3}^{\times}$ and here we tacitly identify $\mathbb{F}_{p^3}^{\times}$ with $(\mathcal{O}_{\mathbf{F}}/\mathfrak{p})^{\times}$.

Proof. By part (ii) of 4.19, $Tr(\rho(Frob_l)) = \chi(Frob_{\mathfrak{p}_l})$ where χ is the ray class character that induces ρ. By Remark 3.9, the character χ is a power of a fundamental character of level 3. For simplicity, we can choose χ such that $\chi = \psi_{3,1}^m$ where $m = \frac{p^3-1}{r}$ and $\psi_{3,1}$ is a fundamental character of level 3 (see Section 3.3). We shall show that $\psi_{3,1}^m(Frob_{\mathfrak{p}_l}) = \overline{\alpha}^m$.

Let $\mathbf{F}_{\mathfrak{p}}$ denote the completion of $\mathbf{F}$ at the prime ideal $\mathfrak{p}$, $\mathbf{F}_{\mathfrak{p}}$ is a finite extension of $\mathbb{Q}_p$. Let $\mathbf{L}$ be the ray class field modulo p of $\mathbf{F}$. By Theorem 4.9, $\mathbf{L}/\mathbf{F}$ is ramified only at $\mathfrak{p}$. It

follows that the decomposition field $\mathbf{L}^D$ of a prime of $\mathbf{L}$ lying over $\mathfrak{p}$ is an unramified, abelian extension of $\mathbf{F}$, and hence, $[\mathbf{L}^D : \mathbf{F}]$ divides $h(\mathbf{F})$, the class number of $\mathbf{F}$. But $h(\mathbf{F}) = 1$ by assumption, so $\mathbf{L}^D = \mathbf{F}$ and it follows that $\mathfrak{p}$ lying under a unique prime of $\mathbf{L}$. Let $\mathbf{L}_\mathfrak{p}$ denote the completion of $\mathbf{L}$ at the unique prime of $\mathbf{L}$ lying over $\mathfrak{p}$. By properties of completion, $\mathbf{F}_\mathfrak{p}$ contains μ_r, the r^{th} roots of unity; moreover, $\mathbf{L}_\mathfrak{p} = \mathbf{F}_\mathfrak{p}\left(\sqrt[r]{p}\right)$.

Let $(\cdot, \mathbf{L}_\mathfrak{p}/\mathbf{F}_\mathfrak{p})$ denote the local norm residue symbol (see [17], section 6.1), it is a map:

$$(\cdot, \mathbf{L}_\mathfrak{p}/\mathbf{F}_\mathfrak{p}) : \mathbf{F}_\mathfrak{p}^\times \longrightarrow Gal(\mathbf{L}_\mathfrak{p}/\mathbf{F}_\mathfrak{p})$$

Let σ_α denote $(\alpha, \mathbf{L}_\mathfrak{p}/\mathbf{F}_\mathfrak{p})$, σ_α is an element of $Gal(\mathbf{L}_\mathfrak{p}/\mathbf{F}_\mathfrak{p})$. Let $\left(\frac{\cdot,\cdot}{\mathfrak{p}}\right)$ denote the Hilbert symbol, it is a map:

$$\left(\frac{\cdot,\cdot}{\mathfrak{p}}\right) : \mathbf{F}_\mathfrak{p}^\times/\mathbf{F}_\mathfrak{p}^{\times r} \times \mathbf{F}_\mathfrak{p}^\times/\mathbf{F}_\mathfrak{p}^{\times r} \longrightarrow \mu_r$$

By [17], chapter 5, proposition 3.1, we have

$$\left(\frac{\alpha, p}{\mathfrak{p}}\right) = \frac{(\alpha, \mathbf{L}_\mathfrak{p}/\mathbf{F}_\mathfrak{p})\left(\sqrt[r]{p}\right)}{\sqrt[r]{p}} = \frac{\sigma_\alpha\left(\sqrt[r]{p}\right)}{\sqrt[r]{p}}$$

On the other hand, since p is a uniformizer of $\mathbf{F}_\mathfrak{p}$, we have $\psi_{3,1}^m(\sigma_\alpha) = \overline{\left(\frac{\sigma_\alpha\left(\sqrt[r]{p}\right)}{\sqrt[r]{p}}\right)}$ by definition (see section 3.3, remark 3.9). Therefore,

$$\psi_{3,1}^m(\sigma_\alpha) = \overline{\left(\frac{\alpha, p}{\mathfrak{p}}\right)} \tag{5.2}$$

By [17], Chapter 5, Proposition 3.4,

$$\overline{\left(\frac{\alpha, p}{\mathfrak{p}}\right)} = \frac{1}{(\overline{\alpha})^{\frac{p^3-1}{r}}} = \frac{1}{\overline{\alpha}^m} \tag{5.3}$$

So, it remains to determine the relationship between σ_α and $Frob_{\mathfrak{p}_l}$. By the product

formula ([17], Chapter 6, Corollary 5.7), we have

$$\prod_{\mathfrak{s}} (\alpha, \mathbf{L}_{\mathfrak{s}}/\mathbf{F}_{\mathfrak{s}}) = 1 \tag{5.4}$$

where the product runs through all the prime ideals $\mathfrak{s}$ of $\mathbf{F}$. $\mathbf{F}_{\mathfrak{s}}$ denotes the completion of $\mathbf{F}$ at $\mathfrak{s}$, $\mathbf{L}_{\mathfrak{s}}$ denotes the completion of $\mathbf{L}$ at a prime ideal of $\mathbf{L}$ lying over $\mathfrak{s}$; and $(\alpha, \mathbf{L}_{\mathfrak{s}}/\mathbf{F}_{\mathfrak{s}})$ denotes the local norm residue symbol evaluated at α.

Now, note that if $\mathfrak{s} \neq \mathfrak{p}, \mathfrak{p}_l$, then $\mathbf{L}_{\mathfrak{s}}/\mathbf{F}_{\mathfrak{s}}$ is an unramified extension and α is a unit of $\mathbf{F}_{\mathfrak{s}}$ and hence, $(\alpha, \mathbf{L}_{\mathfrak{s}}/\mathbf{F}_{\mathfrak{s}}) = 1$ by [17], chapter 5, lemma 3.3. Whence, equation (5.4) is reduced to:

$$1 = (\alpha, \mathbf{L}_{\mathfrak{p}}/\mathbf{F}_{\mathfrak{p}})\,(\alpha, \mathbf{L}_{\mathfrak{p}_l}/\mathbf{F}_{\mathfrak{p}_l}) = \sigma_\alpha\,(\alpha, \mathbf{L}_{\mathfrak{p}_l}/\mathbf{F}_{\mathfrak{p}_l})$$

By [17], chapter 6, section 7, $(\alpha, \mathbf{L}_{\mathfrak{p}_l}/\mathbf{F}_{\mathfrak{p}_l}) = Frob_{\mathfrak{p}_l}$ since α is a uniformizer of $\mathbf{F}_{\mathfrak{p}_l}$. Therefore, $\sigma_\alpha Frob_{\mathfrak{p}_l} = 1$, equivalently, $\sigma_\alpha = Frob_{\mathfrak{p}_l}^{-1}$. Combine this with equation (5.2) and (5.3), we then have,

$$\psi_{3,1}^m(Frob_{\mathfrak{p}_l}^{-1}) = \psi_{3,1}^m(\sigma_\alpha) = \left(\frac{\alpha, p}{\mathfrak{p}}\right) = \frac{1}{\overline{\alpha}^m}$$

and it follows that

$$\psi_{3,1}^m(Frob_{\mathfrak{p}_l}) = \overline{\alpha}^m$$

Hence,

$$Tr(\rho(Frob_l)) = \chi(Frob_{\mathfrak{p}_l}) = \psi_{3,1}^m(Frob_{\mathfrak{p}_l}) = \overline{\alpha}^m.$$

■

5.1.2 Strategy. Based on theorem 5.1, the computational strategy is as follows (see section 5.3.1 for a detailed implementation of this strategy for the case $p = 5$, level 1619):

First, find the smallest prime l such that theorem 5.1 is applicable. Let $\zeta = Tr(\rho(Frob_l))$, then $\zeta = \overline{\alpha}^m$. Let $g(x)$ be the minimal polynomial polynomial of α^m over $\mathbb{Q}$ then $g(x)$ is a

monic polynomial with integer coefficients since $\alpha^m \in \mathcal{O}_{\mathbf{F}}$. If we identify $\mathbb{F}_{p^3}^{\times}$ with $(\mathcal{O}_{\mathbf{F}}/\mathfrak{p})^{\times}$, then $\overline{\alpha}^m$ is a root of $\overline{g}(x)$ over $\mathbb{F}_p$ where $\overline{g}(x)$ is the reduction mod p of $g(x)$. Hence, we have just determined $\zeta = Tr(\rho(Frob_l))$ up to conjugacy which is all we can expect when computing with Frobenius elements.

Remark 5.3. Note that for this strategy to work, in addition to l being a prime such that theorem 5.1 is applicable, we need $\overline{x}$ to be a generator of $\mathbb{Z}/r\mathbb{Z}$ where $\overline{x}$ is the element of the ray class group corresponding to $\mathfrak{p}_l$ under the Artin map. In the computations that we carried out, the smallest prime l satisfying the hypotheses of theorem 5.1 happens to also have this property.

Next, for a prime $l' \nmid pN$ and $l' \neq l$, there are only three possibilities for the factorization of l' in $\mathbf{F}$:

(i) l' is inert in $\mathcal{O}_{\mathbf{F}}$, in which case, $\pi(Frob_{l'})$ has order 3 in $Gal(\mathbf{K}/\mathbb{Q})$ and by part (iii) of theorem 4.19, $Tr(\rho(Frob_{l'})) = T_2(\rho(Frob_{l'})) = 0$.

(ii) l' factors in $\mathcal{O}_{\mathbf{F}}$ into $\mathfrak{p}_{l'}$ and $\mathfrak{p}'_{l'}$ where the inertia degrees of $\mathfrak{p}_{l'}$ and $\mathfrak{p}'_{l'}$ over l' are 1 and 2, respectively. To compute $Tr(\rho(Frob_{l'}))$, we could apply theorem 5.1. However, a much more efficient method is to use Artin reciprocity theorem (theorem 4.9) to get $Tr(\rho(Frob_{l'}))$ from $Tr(\rho(Frob_l))$. More specifically, since $Gal(\mathbf{L}/\mathbf{F}) \cong \mathbb{Z}/r\mathbb{Z}$ by construction, we can use Pari to compute with the Artin map to get $\mathfrak{p}_l \longleftrightarrow \overline{x} \in \mathbb{Z}/r\mathbb{Z}$ and $\mathfrak{p}_{l'} \longleftrightarrow \overline{y} = k\overline{x} \in \mathbb{Z}/r\mathbb{Z}$. It follows that $\chi(Frob_{\mathfrak{p}_{l'}}) = \chi(Frob_{\mathfrak{p}_l}^k) = \chi(Frob_{\mathfrak{p}_l})^k = \zeta^k$ and hence, $Tr(\rho(Frob_{l'})) = \chi(Frob_{\mathfrak{p}_{l'}}) = \zeta^k$ and the cotrace $T_2(\rho(Frob_l))$ is computed by applying theorem 4.19, part (ii). In particular, to compute the cotrace, we just have to compute $\det(\rho(Frob_{l'}))$ (see section 5.2 for this computation).

(iii) l' splits in $\mathcal{O}_{\mathbf{F}}$ into three primes $\mathfrak{p}_{l',1}$, $\mathfrak{p}_{l',2}$, $\mathfrak{p}_{l',3}$, each with inertia degree 1 over l'. Then we can compute $\chi(Frob_{\mathfrak{p}_{l',j}})$ for $1 \leq j \leq 3$ by applying Artin reciprocity theorem as in the previous case. And then we apply part (i) of theorem 4.19 to get $Tr(\rho(Frob_{l'})) =$

$$\sum_{j=1}^{3} \chi(Frob_{\mathfrak{p}_{l',j}}) \text{ and } T_2(\rho(g)) = \sum_{i<j} \chi(Frob_{\mathfrak{p}_{l',i}})\chi(Frob_{\mathfrak{p}_{l',j}}).$$

This process allows us to compute $Tr(\rho(Frob_l))$ and $T_2(\rho(Frob_l))$ for all the primes $l \nmid pN$.

5.2 Computing $\det(\rho(Frob_l))$

In our computation strategy above (section 5.1.2), to compute the cotrace $T_2(\rho(Frob_l))$ in case (ii), we need to compute $\det(\rho(Frob_l))$. By [2],

$$det(\rho(Frob_l)) = \omega_p^m(Frob_l)\epsilon_q(Frob_l) \tag{5.5}$$

where ω_p is the cyclotomic character mod p and ϵ_q is the unique quadratic character mod q (recall that q is the level of ρ). We show how to compute the each of the ingredients in the right side of equation (5.5) in this section.

5.2.1 The Cyclotomic Character.

Proposition 5.4. *Let n be a positive integer and $\zeta_n = e^{\frac{2\pi i}{n}}$, then $Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$.*

Proof. An automorphism $\sigma \in Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ is completely determined by its action on ζ_n. In particular, $\sigma\zeta_n = \zeta_n^k$ for some k satisfying $1 \leq k \leq n$ and $gcd(k, n) = 1$ since σ must map ζ_n to a primitive n^{th} root of unity. It follows that there are precisely $\varphi(n)$ automorphisms in $Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q})$.

Define a map $\varrho : Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \longrightarrow (\mathbb{Z}/n\mathbb{Z})^\times$ as follows: for $\sigma \in Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ such that $\sigma\zeta_n = \zeta_n^k$, set $\varrho(\sigma) = \overline{k}$. This is well-defined by the above argument. Let $\tau \in Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ such that $\tau\zeta_n = \zeta_n^l$, $1 \leq l \leq n, gcd(l, n) = 1$; then $\sigma\tau\zeta_n = \zeta^{kl}$. Thus, $\varrho(\sigma\tau) = \overline{kl} = \overline{k} \cdot \overline{l} = \varrho(\sigma)\varrho(\tau)$. So, ϱ is a homomorphism. It is easy to see that ϱ is bijective, hence, it is an isomorphism. ■

Definition 5.5. Let p be a prime, then $Gal(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ is isomorphic to $(\mathbb{Z}/p\mathbb{Z})^\times = \mathbb{F}_p^\times$ via

the canonical isomorphism $\varrho : Gal(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \longrightarrow \mathbb{F}_p^\times$ as in proposition 5.4. Let $\pi : G_\mathbb{Q} \longrightarrow Gal(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ be the natural projection. Let $\omega_p = \varrho \circ \pi$, then $\omega_p : G_\mathbb{Q} \longrightarrow \mathbb{F}_p^\times$ is called the **cyclotomic character** mod p.

Theorem 5.6. *Let ω_p be the cyclotomic character mod p. Then for each prime $l \neq p$, $\omega_p(Frob_l) = \bar{l}$.*

Proof. First note that $\pi(Frob_l)$ is the Frobenius element at l of $Gal(\mathbb{Q}(\zeta_p)/\mathbb{Q})$, which, by abuse of notation, is also denoted by $Frob_l$. It suffices to show that $\varrho(Frob_l) = \bar{l}$ where ϱ is the canonical isomorphism as before. Since l is unramified in $\mathbb{Q}(\zeta_p)$ and $Gal(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ is Abelian, $Frob_l$ is well-defined and is the unique element in $Gal(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ satisfying:

$$Frob_l\alpha \equiv \alpha^l (\text{mod } l\mathbb{Z}[\zeta_p]), \text{ for all } \alpha \in \mathbb{Z}[\zeta_p]$$

by definition A.3. We claim that $Frob_l$ is the map σ_l that sends ζ_p to ζ_p^l.

In fact, if $\sigma_l\zeta_p = \zeta_p^l$, then for any element $\alpha \in \mathbb{Z}[\zeta_p]$, $\alpha = \sum_j a_j\zeta_p^j, a_j \in \mathbb{Z}$, we have, $\sigma_l(\alpha) = \sigma_l(\sum_j a_j\zeta_p^j) = \sum_j a_j\zeta_p^{lj} \equiv (\sum_j a_j\zeta_p^j)^l = \alpha^l (\text{mod } l\mathbb{Z}[\zeta_p])$. Thus, $Frob_l = \sigma_l$ and hence, $\varrho(Frob_l) = \varrho(\sigma_l) = \bar{l}$ by definition of ϱ. ■

5.2.2 The Quadratic Character.

Definition 5.7. Let q be an odd prime and $\mathbb{M} = \mathbb{Q}(\sqrt{q^*})$ be the quadratic extension of $\mathbb{Q}$ ramified only at q where $q^* = (-1)^{\frac{q-1}{2}}q$. Identify $Gal(\mathbb{M}/\mathbb{Q})$ with $\{\pm 1\}$ via the obvious isomorphism ϕ. Let $\pi : G_\mathbb{Q} \longrightarrow Gal(\mathbb{M}/\mathbb{Q})$ be the natural projection. Let $\epsilon_q = \phi \circ \pi$, then ϵ_q is called the **quadratic character** mod q.

Theorem 5.8. *Let q be a prime and let ϵ_q be the quadratic character mod q. Then for each prime $l \neq q$, we have, $\epsilon_q(Frob_l) = \left(\frac{l}{q}\right)$ where $\left(\frac{\cdot}{q}\right)$ is the Legendre symbol.*

Proof. $\epsilon_q(Frob_l)$ is 1 (resp. -1) if and only if l splits in $\mathbb{M}$ (resp. l does not split in $\mathbb{M}$), if and only if q^* is a square mod l (resp. q^* is not a square mod l). Therefore, $\epsilon(Frob_l) = \left(\frac{q^*}{l}\right)$.

Claim: $\left(\frac{q^*}{l}\right) = \left(\frac{l}{q}\right)$. Indeed, if $q^* = q$, that is, $q \equiv 1 (\text{mod } 4)$, then $\left(\frac{q}{l}\right) = \left(\frac{l}{q}\right)$ by the quadratic reciprocity law. If $q^* = -q$, that is, $q \equiv 3 (\text{mod } 4)$, then $\left(\frac{-q}{l}\right) = \left(\frac{-1}{l}\right)\left(\frac{q}{l}\right) = (-1)^{\frac{l-1}{2}}\left(\frac{l}{q}\right)(-1)^{\frac{l-1}{2}} = \left(\frac{l}{q}\right)$. ■

5.3 Computational Results

5.3.1 Case $p = 5$, level 1619. Recall that the defining polynomial for the S_3-extension $\mathbf{K}$ satisfying the requirements in section 4.3.1 is $f(x) = x^3 - x^2 + x - 8$. Keep the same notation as in that section, fix a cubic subfield $\mathbf{F}$ of $\mathbf{K}$, and let $\mathbf{L}$ be the ray class field modulo 5 of $\mathbf{F}$. $Gal(\mathbf{L}/\mathbf{F}) \cong \mathbb{Z}/62\mathbb{Z}$. 2 factors in $\mathcal{O}_\mathbf{F}$ into two primes $\mathfrak{p}_2$ and $\mathfrak{p}_2'$ with inertia degree 1 and 2, respectively. An integral basis for $\mathcal{O}_\mathbf{F}$ is $\{1, \beta, \beta^2\}$ where β is a root of $f(x)$ satisfying $\mathbf{F} = \mathbb{Q}(\beta)$. Using GP/Pari, we have, $\mathfrak{p}_2 = (2 - \beta)\mathcal{O}_\mathbf{F}$. Put $\alpha = 2 - \beta$.

Now, we apply the computation strategy described in 5.1.2. Let $\zeta = Tr(\rho(Frob_2))$; by theorem 5.1, $\zeta = \overline{\alpha}^4$. The minimal polynomial for $\overline{\alpha}^4$ over $\mathbb{F}_5$ is $\overline{g}(x) = x^3 + 3x^2 + 4$. Thus, we have just determined ζ up to conjugacy, it is a root of $x^3 + 3x^2 + 4$ over $\mathbb{F}_5$.

To compute $T_2(\rho(Frob_2))$, we first invoke theorem 4.19, part (ii), to get:

$$T_2(\rho(Frob_2)) = Tr(\rho(Frob_2))^{-1} \det(\rho(Frob_2))$$

Next, we use equation (5.5), theorem 5.6 and theorem 5.8 to get:

$$\det(\rho(Frob_2)) = \omega_5^m(Frob_2)\epsilon_{1619}(Frob_2) = \overline{2}^4\left(\frac{2}{1619}\right)$$

Doing calculations in $\mathbb{F}_5(\zeta) \cong \mathbb{F}_{5^3}$, we have,

$$T_2(\rho(Frob_2)) = \zeta^{-1}\left(\overline{2}^4\right)\left(\overline{-1}\right) = 4\zeta^2 + 2\zeta$$

Now, to compute $Tr(\rho(Frob_l))$ and $T_2(\rho(Frob_l))$ for a prime $l \neq 2$, we first use GP/Pari

to find that $\mathfrak{p}_2$ corresponds to $\overline{11} \in \mathbb{Z}/62\mathbb{Z}$ under the Artin map. Since $\overline{11}$ generates $\mathbb{Z}/62\mathbb{Z}$, we can apply the strategy in 5.1.2. $Tr(\rho(Frob_l))$ and $T_2(\rho(Frob_l))$ will depend on how l factors in $\mathcal{O}_{\mathbf{F}}$. For instance, 3 is inert in $\mathcal{O}_{\mathbf{F}}$; so, $Tr(\rho(Frob_3)) = T_2(\rho(Frob_3)) = 0$.

7 factors in $\mathcal{O}_{\mathbf{F}}$ into two primes $\mathfrak{p}_7$ and $\mathfrak{p}_7'$ with inertia degree 1 and 2, respectively. $\mathfrak{p}_7$ corresponds to $\overline{39} = 43 \cdot \overline{11} \in \mathbb{Z}/62\mathbb{Z}$. Therefore,

$$Tr(\rho(Frob_7)) = \chi(Frob_{\mathfrak{p}_7}) = \chi(Frob_{\mathfrak{p}_2})^{43} = Tr(\rho(Frob_2))^{43} = \zeta^{43} = \zeta^2 + 2\zeta + 1$$

$$T_2(\rho(Frob_7)) = Tr(\rho(Frob_7))^{-1} \det(\rho(Frob_7)) = (\zeta^2 + 2\zeta + 1)^{-1}(\overline{7})^4 \left(\frac{7}{1619}\right) = 3\zeta^2 + 2\zeta$$

11 splits completely in $\mathcal{O}_{\mathbf{F}}$ into $\mathfrak{p}_{11,1}, \mathfrak{p}_{11,2}, \mathfrak{p}_{11,3}$. Using the Artin reciprocity theorem again, we get $\mathfrak{p}_{11,1} \longleftrightarrow \overline{4} = 6 \cdot \overline{11}$, $\mathfrak{p}_{11,2} \longleftrightarrow \overline{26} = 8 \cdot \overline{11}$, $\mathfrak{p}_{11,3} \longleftrightarrow \overline{32} = 48 \cdot \overline{11}$. Thus,

$$Tr(\rho(Frob_{11})) = \sum_{j=1}^{3} \chi(Frob_{\mathfrak{p}_{11,j}}) = \chi(Frob_{\mathfrak{p}_2})^6 + \chi(Frob_{\mathfrak{p}_2})^8 + \chi(Frob_{\mathfrak{p}_2})^{48} = \zeta^6 + \zeta^8 + \zeta^{48} = 3\zeta$$

$$T_2(\rho(Frob_{11})) = \sum_{i<j} \chi(Frob_{\mathfrak{p}_{11,i}})\chi(Frob_{\mathfrak{p}_{11,j}}) = 2\zeta^2 + 2\zeta + 2$$

Continuing this process, we get table 5.1 which gives $Tr(\rho(Frob_l))$ and $T_2(\rho(Frob_l))$ for all the primes $2 \leq l \leq 47$.

l	2	3	5	7	11	13	17	19
$Tr(\rho(Frob_l))$	ζ	0	$*$	$\zeta^2 + 2\zeta + 1$	3ζ	$2\zeta + 3$	0	$4\zeta^2 + 3\zeta + 1$
$T_2(\rho(Frob_l))$	$4\zeta^2 + 2\zeta$	0	$*$	$3\zeta^2 + 2\zeta$	$2\zeta^2 + 2\zeta + 2$	$\zeta^2 + 4\zeta + 4$	0	$\zeta^2 + 3\zeta + 1$

23	29	31	37	41	43	47
$2\zeta^2 + 2\zeta + 4$	0	$2\zeta^2 + 1$	$4\zeta^2 + 3\zeta + 1$	$2\zeta^2 + 3\zeta + 4$	$3\zeta^2 + 4\zeta + 2$	ζ
$\zeta^2 + 3\zeta + 3$	0	$2\zeta^2 + \zeta + 4$	$3\zeta^2 + 2\zeta + 3$	$\zeta^2 + 2$	$\zeta^2 + 2\zeta + 4$	$4\zeta^2 + 2\zeta$

Table 5.1: Traces and Cotraces $p = 5$, $N = 1619$, $m = 4$

We shall proceed exactly like this for the rest of the cases in this section. The results are summarized in table 5.1 to 5.3.

5.3.2 Case $p = 7$, level 439. The defining polynomial for $\mathbf{K}$ is $f(x) = x^3 - x^2 - 2x + 5$. ζ is a root of $\overline{g}(x) = x^3 + 5$ over $\mathbb{F}_7$.

l	2	3	5	7	11	13	17	19	23	29	31	37	41	43	47
$Tr(\rho(Frob_l))$	0	ζ	0	$*$	0	0	ζ	0	$4\zeta^2$	0	4ζ	ζ^2	4	4	ζ^2
$T_2(\rho(Frob_l))$	0	$6\zeta^2$	0	$*$	0	0	$6\zeta^2$	0	3ζ	0	$5\zeta^2$	5ζ	5	5	5ζ

Table 5.2: Traces and Cotraces $p = 11$, $N = 139$, $m = 14$

5.3.3 Case $p = 11$, level 139. The defining polynomial for $\mathbf{K}$ is $f(x) = x^3 - x^2 + x + 2$. ζ is a root of $\overline{g}(x) = x^3 + 4x^2 + 6x + 6$ over $\mathbb{F}_{11}$.

l	2	3	5	7	11	13	17	19
$Tr(\rho(Frob_l))$	ζ	$7\zeta^2 + 6\zeta + 8$	0	0	$*$	0	$10\zeta^2 + 4\zeta + 4$	$\zeta^2 + 3\zeta + 9$
$T_2(\rho(Frob_l))$	$10\zeta^2 + 7\zeta + 5$	$4\zeta^2 + 2\zeta + 10$	0	0	$*$	0	$2\zeta^2 + 2\zeta + 5$	$6\zeta^2 + 10\zeta + 1$

l	23	29	31	37	41	43	47
$Tr(\rho(Frob_l))$	$8\zeta^2 + 10\zeta + 6$	0	0	$8\zeta^2 + 9\zeta + 9$	$\zeta + 3$	$9\zeta^2 + 5\zeta + 4$	$10\zeta^2 + 2\zeta + 7$
$T_2(\rho(Frob_l))$	$5\zeta^2 + 8\zeta + 7$	0	0	$8\zeta^2 + 7\zeta + 9$	$7\zeta + 6$	$2\zeta^2 + 7\zeta + 4$	$6\zeta^2 + 10\zeta + 2$

Table 5.3: Traces and Cotraces $p = 11$, $N = 139$, $m = 14$

Chapter 6. Cohomology Computations

In the previous chapters, we compute $Tr(\rho(Frob_l))$ and $T_2(\rho(Frob_l))$ for a representation ρ constructed by the method of section 4.3. In this chapter, we shall describe the computations

	$F(3,3,3)$	
l	$m(l,1)$	$m(l,2)$
2	$\begin{pmatrix} 0&2&0&2&0&2 \\ 0&0&4&4&2&1 \\ 1&1&3&0&1&4 \\ 3&0&2&2&2&2 \\ 0&4&1&3&2&2 \\ 3&3&4&3&4&0 \end{pmatrix}$	$\begin{pmatrix} 4&1&4&0&0&1 \\ 3&4&4&1&1&1 \\ 0&3&2&4&3&2 \\ 0&0&3&3&1&1 \\ 1&2&1&3&3&0 \\ 3&1&3&1&3&3 \end{pmatrix}$
3	$\begin{pmatrix} 0&0&0&0&0&0 \\ 0&0&0&0&0&0 \\ 0&0&0&0&0&0 \\ 0&0&0&0&0&0 \\ 0&0&0&0&0&0 \\ 0&0&0&0&0&0 \end{pmatrix}$	$\begin{pmatrix} 0&0&0&0&0&0 \\ 0&0&0&0&0&0 \\ 0&0&0&0&0&0 \\ 0&0&0&0&0&0 \\ 0&0&0&0&0&0 \\ 0&0&0&0&0&0 \end{pmatrix}$
7	$\begin{pmatrix} 3&1&2&2&3&1 \\ 0&0&3&2&4&0 \\ 0&2&3&4&3&2 \\ 4&1&1&2&2&4 \\ 2&2&1&4&1&2 \\ 4&3&4&4&3&1 \end{pmatrix}$	$\begin{pmatrix} 3&3&4&2&4&3 \\ 0&2&1&2&3&4 \\ 4&1&3&4&4&1 \\ 1&3&4&3&1&2 \\ 4&2&2&3&4&2 \\ 1&0&2&4&3&0 \end{pmatrix}$
11	$\begin{pmatrix} 3&2&0&3&0&0 \\ 1&1&0&2&1&0 \\ 3&3&4&4&1&2 \\ 3&2&4&2&4&2 \\ 2&3&2&4&4&4 \\ 3&0&3&1&0&0 \end{pmatrix}$	$\begin{pmatrix} 3&3&1&4&0&0 \\ 4&1&4&0&1&3 \\ 0&2&2&0&4&3 \\ 0&3&3&0&1&3 \\ 4&4&1&3&1&3 \\ 0&2&2&3&3&2 \end{pmatrix}$
13	$\begin{pmatrix} 1&2&4&0&2&0 \\ 4&4&4&0&2&2 \\ 4&4&0&2&1&2 \\ 0&1&0&2&3&4 \\ 3&2&3&2&1&1 \\ 3&2&2&1&1&1 \end{pmatrix}$	$\begin{pmatrix} 3&4&3&3&4&0 \\ 2&2&1&3&0&2 \\ 3&3&3&3&2&4 \\ 2&2&2&2&1&3 \\ 2&0&4&2&4&0 \\ 2&1&2&0&4&3 \end{pmatrix}$
17	$\begin{pmatrix} 0&0&0&0&0&0 \\ 0&0&0&0&0&0 \\ 0&0&0&0&0&0 \\ 0&0&0&0&0&0 \\ 0&0&0&0&0&0 \\ 0&0&0&0&0&0 \end{pmatrix}$	$\begin{pmatrix} 0&0&0&0&0&0 \\ 0&0&0&0&0&0 \\ 0&0&0&0&0&0 \\ 0&0&0&0&0&0 \\ 0&0&0&0&0&0 \\ 0&0&0&0&0&0 \end{pmatrix}$
19	$\begin{pmatrix} 0&0&1&1&3&1 \\ 2&2&4&4&4&2 \\ 3&3&2&3&0&1 \\ 2&0&2&1&0&3 \\ 0&1&2&0&1&3 \\ 2&1&0&2&0&1 \end{pmatrix}$	$\begin{pmatrix} 1&0&3&2&2&4 \\ 3&3&2&4&4&0 \\ 4&2&4&3&0&4 \\ 0&0&1&4&0&2 \\ 4&2&0&3&1&0 \\ 0&2&0&4&2&4 \end{pmatrix}$

Table 6.1: Hecke matrices, $p = 5$, $N = 1619$, $F(3,3,3)$

	$F(3,2,0)$	
l	$m(l,1)$	$m(l,2)$
2	$\begin{pmatrix} 0&0&0 \\ 0&0&0 \\ 0&0&0 \end{pmatrix}$	$\begin{pmatrix} 0&0&0 \\ 0&0&0 \\ 0&0&0 \end{pmatrix}$
3	$\begin{pmatrix} 5&3&4 \\ 4&5&4 \\ 1&0&4 \end{pmatrix}$	$\begin{pmatrix} 5&4&5 \\ 4&4&6 \\ 4&6&5 \end{pmatrix}$
5, 11, 13	$\begin{pmatrix} 0&0&0 \\ 0&0&0 \\ 0&0&0 \end{pmatrix}$	$\begin{pmatrix} 0&0&0 \\ 0&0&0 \\ 0&0&0 \end{pmatrix}$
17	$\begin{pmatrix} 5&3&4 \\ 4&5&4 \\ 1&0&4 \end{pmatrix}$	$\begin{pmatrix} 5&4&5 \\ 4&4&6 \\ 4&6&5 \end{pmatrix}$
19	$\begin{pmatrix} 0&0&0 \\ 0&0&0 \\ 0&0&0 \end{pmatrix}$	$\begin{pmatrix} 0&0&0 \\ 0&0&0 \\ 0&0&0 \end{pmatrix}$
23	$\begin{pmatrix} 3&1&3 \\ 1&1&5 \\ 1&5&3 \end{pmatrix}$	$\begin{pmatrix} 4&1&6 \\ 6&4&6 \\ 5&0&6 \end{pmatrix}$
29	$\begin{pmatrix} 0&0&0 \\ 0&0&0 \\ 0&0&0 \end{pmatrix}$	$\begin{pmatrix} 0&0&0 \\ 0&0&0 \\ 0&0&0 \end{pmatrix}$
31	$\begin{pmatrix} 6&5&2 \\ 2&6&2 \\ 4&0&2 \end{pmatrix}$	$\begin{pmatrix} 3&1&3 \\ 1&1&5 \\ 1&5&3 \end{pmatrix}$
37	$\begin{pmatrix} 6&2&6 \\ 2&2&3 \\ 2&3&6 \end{pmatrix}$	$\begin{pmatrix} 2&4&3 \\ 3&2&3 \\ 6&0&3 \end{pmatrix}$
41	$\begin{pmatrix} 4&0&0 \\ 0&4&0 \\ 0&0&4 \end{pmatrix}$	$\begin{pmatrix} 2&0&0 \\ 0&2&0 \\ 0&0&2 \end{pmatrix}$
43	$\begin{pmatrix} 4&0&0 \\ 0&4&0 \\ 0&0&4 \end{pmatrix}$	$\begin{pmatrix} 2&0&0 \\ 0&2&0 \\ 0&0&2 \end{pmatrix}$
47	$\begin{pmatrix} 6&2&6 \\ 2&2&3 \\ 2&3&6 \end{pmatrix}$	$\begin{pmatrix} 5&3&4 \\ 4&5&4 \\ 1&0&4 \end{pmatrix}$

Table 6.2: Hecke matrices, $p = 7$, $N = 439$, $F(3,2,0)$

of $a(l,1)$ and $a(l,2)$ corresponding to the eigenclass $v \in H^3(\Gamma_0(N), F(c_2,c_1,c_0)\otimes\epsilon)$ for several predicted weights $F(c_2,c_1,c_0)$ and verify that proposition 3.6 and hence, the attachment equation (3.2) is satisfied for primes $2 \leq l \leq 47$. Consequently, conjecture 3.1 is valid in all these cases.

6.1 Doud's program

Doud's program computes the matrices for the action of the Hecke operators $T(l,k)$ on $H^3(\Gamma_0(N), F(c_2,c_1,c_0)\otimes\epsilon)$. We shall denote by $m(l,k)$ the matrix for the Hecke operator $T(l,k)$ and call such a matrix a Hecke matrix. Tables 6.1, 6.2 and 6.3 give $m(l,k)$ for the action of $T(l,k)$ on cohomology group corresponding to certain specific weights.

	$F(9,1,1)$		$F(10,9,2)$	
l	$m(l,1)$	$m(l,2)$	$m(l,1)$	$m(l,2)$
2	$\begin{pmatrix} 5 & 6 & 4 \\ 6 & 10 & 10 \\ 1 & 6 & 3 \end{pmatrix}$	$\begin{pmatrix} 4 & 8 & 1 \\ 4 & 0 & 2 \\ 9 & 1 & 4 \end{pmatrix}$	$\begin{pmatrix} 5 & 3 & 4 \\ 5 & 4 & 5 \\ 6 & 9 & 9 \end{pmatrix}$	$\begin{pmatrix} 10 & 1 & 6 \\ 2 & 6 & 8 \\ 6 & 8 & 3 \end{pmatrix}$
3	$\begin{pmatrix} 9 & 9 & 8 \\ 10 & 10 & 5 \\ 6 & 8 & 9 \end{pmatrix}$	$\begin{pmatrix} 9 & 3 & 8 \\ 9 & 0 & 3 \\ 8 & 6 & 0 \end{pmatrix}$	$\begin{pmatrix} 2 & 8 & 4 \\ 5 & 3 & 9 \\ 4 & 9 & 1 \end{pmatrix}$	$\begin{pmatrix} 4 & 9 & 2 \\ 8 & 1 & 3 \\ 0 & 10 & 4 \end{pmatrix}$
5, 7, 13	$\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$	$\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$	$\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$	$\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$
17	$\begin{pmatrix} 3 & 9 & 1 \\ 1 & 2 & 7 \\ 4 & 6 & 9 \end{pmatrix}$	$\begin{pmatrix} 4 & 7 & 10 \\ 6 & 9 & 7 \\ 4 & 8 & 6 \end{pmatrix}$	$\begin{pmatrix} 4 & 4 & 0 \\ 0 & 10 & 1 \\ 5 & 0 & 0 \end{pmatrix}$	$\begin{pmatrix} 0 & 0 & 3 \\ 1 & 0 & 8 \\ 1 & 4 & 8 \end{pmatrix}$
19	$\begin{pmatrix} 1 & 0 & 5 \\ 8 & 4 & 8 \\ 3 & 3 & 3 \end{pmatrix}$	$\begin{pmatrix} 7 & 5 & 8 \\ 0 & 7 & 7 \\ 4 & 10 & 5 \end{pmatrix}$	$\begin{pmatrix} 0 & 6 & 6 \\ 2 & 9 & 1 \\ 4 & 8 & 10 \end{pmatrix}$	$\begin{pmatrix} 9 & 7 & 6 \\ 2 & 3 & 4 \\ 8 & 8 & 7 \end{pmatrix}$
23	$\begin{pmatrix} 4 & 4 & 6 \\ 2 & 2 & 1 \\ 10 & 6 & 4 \end{pmatrix}$	$\begin{pmatrix} 9 & 2 & 8 \\ 9 & 0 & 3 \\ 8 & 6 & 0 \end{pmatrix}$	$\begin{pmatrix} 7 & 6 & 3 \\ 1 & 5 & 4 \\ 3 & 4 & 9 \end{pmatrix}$	$\begin{pmatrix} 4 & 9 & 2 \\ 8 & 1 & 3 \\ 0 & 10 & 4 \end{pmatrix}$
29, 31	$\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$	$\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$	$\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$	$\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$
37	$\begin{pmatrix} 2 & 9 & 2 \\ 7 & 6 & 2 \\ 9 & 0 & 4 \end{pmatrix}$	$\begin{pmatrix} 9 & 2 & 4 \\ 7 & 2 & 1 \\ 10 & 8 & 5 \end{pmatrix}$	$\begin{pmatrix} 5 & 3 & 10 \\ 7 & 4 & 10 \\ 8 & 6 & 3 \end{pmatrix}$	$\begin{pmatrix} 7 & 2 & 6 \\ 2 & 10 & 0 \\ 10 & 8 & 10 \end{pmatrix}$
41	$\begin{pmatrix} 8 & 6 & 4 \\ 6 & 2 & 10 \\ 1 & 6 & 6 \end{pmatrix}$	$\begin{pmatrix} 1 & 8 & 9 \\ 8 & 4 & 6 \\ 5 & 8 & 2 \end{pmatrix}$	$\begin{pmatrix} 8 & 3 & 4 \\ 5 & 7 & 5 \\ 6 & 9 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 4 & 9 \\ 3 & 7 & 3 \\ 8 & 1 & 10 \end{pmatrix}$
43	$\begin{pmatrix} 9 & 0 & 1 \\ 6 & 3 & 6 \\ 5 & 5 & 5 \end{pmatrix}$	$\begin{pmatrix} 7 & 5 & 8 \\ 0 & 7 & 7 \\ 4 & 10 & 5 \end{pmatrix}$	$\begin{pmatrix} 0 & 10 & 10 \\ 7 & 4 & 9 \\ 3 & 6 & 2 \end{pmatrix}$	$\begin{pmatrix} 9 & 7 & 6 \\ 2 & 3 & 4 \\ 8 & 8 & 7 \end{pmatrix}$
47	$\begin{pmatrix} 7 & 8 & 4 \\ 0 & 7 & 9 \\ 2 & 5 & 6 \end{pmatrix}$	$\begin{pmatrix} 8 & 6 & 3 \\ 0 & 8 & 4 \\ 7 & 1 & 10 \end{pmatrix}$	$\begin{pmatrix} 8 & 9 & 3 \\ 1 & 5 & 2 \\ 4 & 4 & 7 \end{pmatrix}$	$\begin{pmatrix} 6 & 4 & 5 \\ 9 & 1 & 7 \\ 3 & 3 & 8 \end{pmatrix}$

Table 6.3: Hecke matrices, case $p = 11, N = 139, F(9,1,1)$ and $F(10,9,2)$

Remark 6.1. For the case $p = 11$ level $N = 139$ and weight $F(1,0,0)$, the Hecke matrices have dimension 26-by-26 and we shall not present them here.

6.2 Eigenvectors and Eigenvalues

Since the operators $T(l,k)$ commute, there exists a simultaneous eigenvector for the matrices $m(l,k)$. In fact, we have

Proposition 6.2. *Let $T_1, T_2, \ldots$ be commuting linear operators on a finite dimensional vector space V over an algebraically closed field $\mathbb{F}$. Then they have a simultaneous eigenvector.*

Proof. Since $\mathbb{F}$ is algebraically closed, T_1 has an eigenvalue, say λ_1. Let $V_1 = \{v \in V : T_1 v = \lambda_1 v\}$, the eigenspace corresponding to λ_1 for T_1. Clearly, V_1 is a nontrivial subspace of V.

We claim that T_2 maps V_1 into V_1. Indeed, if $\alpha \in V_1$, then

$$T_1T_2\alpha = T_2T_1\alpha = T_2(\lambda\alpha) = \lambda(T_2\alpha)$$

So, by the definition of V_1, $T_2\alpha \in V_1$. It follows that T_2 is a linear operator on V_1 and hence, it has an eigenvalue λ_2. Let V_2 be the eigenspace corresponding to λ_2 for $T_2|_{V_1}$. Then V_2 is nontrivial and $V \supset V_1 \supset V_2$. Continue like this, we have a nonincreasing sequence of nontrivial subspaces $V \supset V_1 \supset V_2 \supset V_3 \supset \ldots$

Since V is finite dimensional, the sequence will eventually stabilize. Therefore, $W = \bigcap_{j\geq 1} V_j$ is nontrivial. Choose an element $w \neq 0$ of W then $T_jw = \lambda_j w, \forall j$, that is, w is a simultaneous eigenvector for $T_1, T_2, \ldots$ ■

For the case $p = 5, N = 1619$ with weight $F(3,3,3)$, the Hecke matrices have entries in $\mathbb{F}_5$. The eigenvectors have entries in $\mathbb{F}_{5^3} \cong \mathbb{F}_5(\zeta)$ where ζ is a root of $\overline{g}(x) = x^3 + 3x^2 + 4$. A simultaneous eigenvector for the matrices in table 6.1 is $v = (1, 4\zeta^2 + 3\zeta + 4, 4\zeta^2 + 2\zeta + 2, 4\zeta + 2, 4\zeta^2 + 2, 2\zeta^2 + 4\zeta + 4)^T$. We compute the eigenvalues corresponding to v and verify that they satisfy

$$a(l,1) = Tr(\rho(Frob_l)) \quad \text{and} \quad la(l,2) = T_2(\rho(Frob_l)), \forall \text{ prime } 2 \leq l \leq 19$$

Note that here we stop at $l = 19$ due to limitations of Doud's program.

For the case $p = 7, N = 38$ with weight $F(3,2,0)$, the Hecke matrices have entries in $\mathbb{F}_7$. The eigenvectors have entries in $\mathbb{F}_{7^3} \cong \mathbb{F}_7(\zeta)$ where ζ is a root of $\overline{g}(x) = x^3 + 5$. A simultaneous eigenvector for the matrices in table 6.2 is $v = (1, \zeta^2 + 5\zeta + 4, 3\zeta^2 + 2\zeta)^T$. We also verify that the eigenvalues corresponding to v satisfy proposition 3.6 for prime $2 \leq l \leq 47$.

For the case $p = 11, N = 139$, the Hecke matrices have entries in $\mathbb{F}_{11}$. The eigenvectors have entries in $\mathbb{F}_{11^3} \cong \mathbb{F}_{11}(\zeta)$ where ζ is a root of $\overline{g}(x) = x^3+4x^2+6x+6$ over $\mathbb{F}_{11}$. With weight

$F(9,1,1)$, a simultaneous eigenvector for the matrices in table 6.3 is $v = (1, \zeta^2+1, 5\zeta^2+\zeta)^T$. With weight $F(10,9,2)$, a simultaneous eigenvector is $v = (1, 2\zeta^2+\zeta+10, 2\zeta^2+3\zeta)^T$. With weight $F(1,0,0)$, a simultaneous eigenvector is $v = (v_j)_{1\leq j\leq 26}^T$ where $v_1 = 1$, $v_2 = 8\zeta^2+2\zeta+10$, $v_3 = 8\zeta^2+10\zeta+4$, $v_4 = 6\zeta^2+9\zeta+10$, $v_5 = \zeta^2+3\zeta+8$, $v_6 = 4\zeta^2+10\zeta+1$, $v_7 = 5\zeta^2+5\zeta+3$, $v_8 = 7\zeta^2+8\zeta+5$, $v_9 = 9\zeta^2+z+10$, $v_{10} = 8\zeta^2+10\zeta+2$, $v_{11} = 9\zeta^2+4\zeta+5$, $v_{12} = 9\zeta^2+10\zeta+7$, $v_{13} = 9\zeta^2+10\zeta+4$, $v_{14} = \zeta^2+6\zeta+7$, $v_{15} = 5\zeta^2+7$, $v_{16} = 6\zeta^2+\zeta+8$, $v_{17} = 6\zeta^2+5\zeta+6$, $v_{18} = 10\zeta+2$, $v_{19} = \zeta^2+3\zeta+3$, $v_{20} = 2\zeta^2+8\zeta+7$, $v_{21} = 3\zeta^2+2\zeta+9$, $v_{22} = 7\zeta^2+3\zeta+6$, $v_{23} = 8\zeta^2+9$, $v_{24} = 2\zeta+3$, $v_{25} = 10\zeta^2+10\zeta$, $v_{26} = 3\zeta^2+\zeta+3$. The eigenvalues corresponding to v also satisfy Proposition 3.6 for prime $2 \leq l \leq 47$.

Therefore, Conjecture 3.1 is valid up to $l = 47$ in all these cases.

Appendix A. The Frobenius Automorphism

Let $\mathbb{L}/\mathbb{K}$ be a Galois extension of number fields of degree $n = [\mathbb{L} : \mathbb{K}]$ with Galois group $G = Gal(\mathbb{L}/\mathbb{K})$. Let $\mathfrak{p}$ be a prime ideal of $\mathbb{K}$, the ideal $\mathfrak{p}\mathcal{O}_\mathbb{L}$ factors uniquely in $\mathcal{O}_\mathbb{L}$ as $\mathfrak{p}\mathcal{O}_\mathbb{L} = \prod_{1\leq j\leq g} \mathfrak{P}_j^{e_j}$. For each j, $1 \leq j \leq g$, $\mathfrak{P}_j$ is a prime ideal of $\mathcal{O}_\mathbb{L}$; we say that $\mathfrak{P}_j$ lies over $\mathfrak{p}$, denoted by, $\mathfrak{P}_j|\mathfrak{p}$ and we have $\mathfrak{P}_j \cap \mathcal{O}_\mathbb{K} = \mathfrak{p}$. The nonnegative integer e_j is called the *ramification index* of $\mathfrak{P}_j$ over $\mathfrak{p}$, and the integer $f_j = [\mathcal{O}_\mathbb{L}/\mathfrak{P}_j : \mathcal{O}_\mathbb{K}/\mathfrak{p}]$ is called the inertia degree of $\mathfrak{P}_j$ over $\mathfrak{p}$. G acts transitively on the set of prime ideals of $\mathcal{O}_\mathbb{L}$ lying over the prime $\mathfrak{p}$, i.e, for any $\mathfrak{P}_i, \mathfrak{P}_j$, there exists $\sigma \in G$ such that $\sigma(\mathfrak{P}_i) = \mathfrak{P}_j$; additionally, since $\mathbb{L}/\mathbb{K}$ is Galois, e_j, f_j depend only on $\mathfrak{p}$, that is, $e_j = e, f_j = f,$ for all $1 \leq j \leq g$ and we also have $efg = n$ (see [21], section 1.7 for proofs). We say that $\mathfrak{p}$ is *unramified* in $\mathbb{L}$ if $e = 1$, $\mathfrak{p}$ is *totally ramified* (resp. *totally inert*) in $\mathbb{L}$ if $f = g = 1$ (resp. $e = g = 1$), $\mathfrak{p}$ *splits completely* in $\mathbb{L}$ if $e = f = 1$. Finally, we say that the extension $\mathbb{L}/\mathbb{K}$ is *tamely ramified* at $\mathfrak{p}$ if the characteristic of the field $\mathcal{O}_\mathbb{K}/\mathfrak{p}$ does not divide e, equivalently, p does not divide e where $p\mathbb{Z} = \mathfrak{p} \cap \mathbb{Z}$; if p does divide e, we say that $\mathbb{L}/\mathbb{K}$ is *wildly ramified* at $\mathfrak{p}$.

Definition A.1. Assume the hypotheses of the preceding paragraph, let $\mathfrak{P}$ be a prime lying over $\mathfrak{p}$.

(i) The *decomposition group* of $\mathfrak{P}$ over $\mathfrak{p}$, denoted by $D(\mathfrak{P}/\mathfrak{p})$ is defined as:

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

(ii) The k^{th} *ramification group* of $\mathfrak{P}$ over $\mathfrak{p}$, denoted by $G_k(\mathfrak{P}/\mathfrak{p})$ is defined as:

$$G_k(\mathfrak{P}/\mathfrak{p}) = \{\sigma \in G : \sigma(x) \equiv x (\text{mod } \mathfrak{P}^{k+1}), \forall x \in \mathcal{O}_{\mathbb{L}}\}$$

(iii) The *inertia group* of $\mathfrak{P}$ over $\mathfrak{p}$, denoted by $I(\mathfrak{P}/\mathfrak{p})$ is $I(\mathfrak{P}/\mathfrak{p}) = G_0(\mathfrak{P}/\mathfrak{p})$, that is,

$$I(\mathfrak{P}/\mathfrak{p}) = \{\sigma \in G : \sigma(x) \equiv x (\text{mod } \mathfrak{P}), \forall x \in \mathcal{O}_{\mathbb{L}}\}$$

We gather some important properties of decomposition groups and ramification groups in the following proposition:

Proposition A.2. *(i) $I(\mathfrak{P}/\mathfrak{p})$ is a subgroup of $D(\mathfrak{P}/\mathfrak{p})$; more generally, we have the chain $G \supset D(\mathfrak{P}/\mathfrak{p}) \supset I(\mathfrak{P}/\mathfrak{p}) \supset G_1(\mathfrak{P}/\mathfrak{p}) \supset \ldots$ and eventually, there exists n such that $G_k(\mathfrak{P}/\mathfrak{p}) = \{1_G\}, \forall k \geq n$.*

(ii) $|D(\mathfrak{P}/\mathfrak{p})| = ef$ by the orbit-stabilizer theorem.

(iii) The extension $\mathcal{O}_{\mathbb{L}}/\mathfrak{P}\Big/\mathcal{O}_{\mathbb{K}}/\mathfrak{p}$ is Galois. Denote $Gal(\mathcal{O}_{\mathbb{L}}/\mathfrak{P}\Big/\mathcal{O}_{\mathbb{K}}/\mathfrak{p})$ by $\overline{G}$; then $\overline{G}$ is cyclic of order f. Each $\sigma \in D(\mathfrak{P}/\mathfrak{p})$ induces an automorphism $\overline{\sigma} \in \overline{G}$ as follows:

$\overline{\sigma} : \mathcal{O}_{\mathbb{L}}/\mathfrak{P} \longrightarrow \mathcal{O}_{\mathbb{L}}/\mathfrak{P}$ given by $\overline{\sigma}(x + \mathfrak{P}) = \sigma(x) + \mathfrak{P}$.

(iv) The map $\Psi : D(\mathfrak{P}/\mathfrak{p}) \longrightarrow \overline{G}$ given by $\sigma \longmapsto \overline{\sigma}$ is a surjective group homomorphism whose kernel is $I(\mathfrak{P}/\mathfrak{p})$. Consequently, $D(\mathfrak{P}/\mathfrak{p})\big/I(\mathfrak{P}/\mathfrak{p}) \cong \overline{G}$ and is cyclic of order f, hence, $|I(\mathfrak{P}/\mathfrak{p})| = e$. As a result, if $\mathfrak{p}$ is unramified in $\mathbb{L}$, then $I(\mathfrak{P}/\mathfrak{p}) = \{1_G\}$.

(v) By the property of finite extensions of finite fields, the cyclic group $\overline{G}$ is generated by its Frobenius element $\overline{\phi}$, in particular, $\overline{\phi} : \mathcal{O}_{\mathbb{L}}/\mathfrak{P} \longrightarrow \mathcal{O}_{\mathbb{L}}/\mathfrak{P}$ satisfying $\overline{\phi}(x+\mathfrak{P}) = x^{||\mathfrak{p}||}+\mathfrak{P}$ where $||\mathfrak{p}|| = |\mathcal{O}_{\mathbb{K}}/\mathfrak{p}|$.

(vi) If $\mathfrak{p}$ is unramified in $\mathbb{L}$, then $\Psi : D(\mathfrak{P}/\mathfrak{p}) \longrightarrow \overline{G}$ is an isomorphism and the preimage of $\overline{\phi}$ is the unique element σ of $D(\mathfrak{P}/\mathfrak{p})$ satisfying $\sigma(x) \equiv x^{||\mathfrak{p}||}(mod\ \mathfrak{P})$ for all $x \in \mathcal{O}_{\mathbb{L}}$.

Proof. See [16], chapter 4, and [17], chapter 1. ■

Definition A.3. Let $\mathbb{L}/\mathbb{K}$ be a finite Galois extension of number fields with Galois group G and $\mathfrak{p}$ be a prime of $\mathbb{K}$ unramified in $\mathbb{L}$. Let $\mathfrak{P}$ be a prime of $\mathbb{L}$ lying over $\mathfrak{p}$, the Frobenius element of $\mathfrak{P}$ over $\mathfrak{p}$, denoted by $Frob_{\mathfrak{P}}$, is the unique element of G satisfying:

$$Frob_{\mathfrak{P}}(x) \equiv x^{||\mathfrak{p}||}(\text{mod } \mathfrak{P}), \forall x \in \mathcal{O}_{\mathbb{L}}$$

where $||\mathfrak{p}|| = |\mathcal{O}_{\mathbb{K}}/\mathfrak{p}|$.

Remark A.4. (i) By proposition A.2, $Frob_{\mathfrak{P}}$ generates $D(\mathfrak{P}/\mathfrak{p})$ and thus, its order is f.

(ii) Let $\mathfrak{P}, \sigma(\mathfrak{P})$, where $\sigma \in G$, be primes of $\mathbb{L}$ lying over the prime $\mathfrak{p}$, then $Frob_{\sigma(\mathfrak{P})} = \sigma Frob_{\mathfrak{P}}\sigma^{-1}$. Hence, if $\mathbb{L}/\mathbb{K}$ is an Abelian extension, $Frob_{\mathfrak{P}}$ depends only on $\mathfrak{p}$ and it is denoted by $Frob_{\mathfrak{p}}$. It follows that for an Abelian extension $\mathbb{L}/\mathbb{K}$ and a prime $\mathfrak{p}$ of $\mathbb{K}$ unramified in $\mathbb{L}$, $Frob_{\mathfrak{p}}$ is the unique element of the Galois group satisfying:

$$Frob_{\mathfrak{p}}(x) \equiv x^{||\mathfrak{p}||}(\text{mod } \mathfrak{p}\mathcal{O}_{\mathbb{L}}), \text{ for all } x \in \mathcal{O}_{\mathbb{L}}$$

We state an important theorem about Frobenius automorphisms.

Theorem A.5 (Chebotarev Density Theorem)**.** *Let $\mathbb{L}/\mathbb{K}$ be a finite Galois extension of number fields with Galois group G. Let $\mathcal{K}$ be a conjugacy class of G, then the density of the set*

$\{$*unramified primes $\mathfrak{p}$ of $\mathbb{K}$ such that there exists prime $\mathfrak{P}|\mathfrak{p}$ of $\mathbb{L}$ with $Frob_{\mathfrak{P}} \in \mathcal{K}$*$\}$

is $\frac{|\mathcal{K}|}{|G|}$.

Proof. See [17], theorem 13.4. ■

Remark A.6. Theorem A.5 implies, among other things, that the set of prime ideals of $\mathbb{K}$ which split completely in $\mathbb{L}$, denoted by $Spl(\mathbb{L}/\mathbb{K})$, has density $\frac{1}{|G|}$. It turns out that Abelian extensions $\mathbb{L}$ of $\mathbb{K}$ can be studied via $Spl(\mathbb{L}/\mathbb{K})$. Class field theory characterizes $Spl(\mathbb{L}/\mathbb{K})$ in terms of arithmetic of $\mathbb{K}$ solely. See [17], chapter 5-7 for a beautiful treatment of this topic.

Appendix B. Computer Codes

B.1 Trace and Cotrace Calculations

In this section, we show how to use GP/Pari to calculate various important elements in our computations of the trace and cotrace for the case $p = 5$, level 1619 (section 5.3.1).

```
f = x^3 - x^2 + x - 8;
% Declare the defining polynomial for F
bnf = bnfinit(f);
% Create the number field F
bnr = bnrinit(bnf,5);
% Create L the ray class field modulus 5 of F
bnr[5];
% Find the ray class group mod 5 of F, that is, the Galois group of L/F
idealprimedec(bnf,2);
% Determine the factorization of 2 in the number ring of F
p2 = %[1];
% Identify the prime with intertia degree 1 in the above factorization
```

```
bnfisprincipal(bnf,p2);
% Find the generator of p2 in terms of an integral basis for F
```

These steps help us find α (see section 5.3.1), $\alpha = 2 - \beta$ where β is a root of f such that $\mathbb{F} = \mathbb{Q}(\beta)$. Then we use Magma to find the minimal polynomial of $\overline{\alpha}^4$ over $\mathbb{F}_5$ as follows,

```
Q:=Rationals();
Qx<x>:=PolynomialRing(Q);
f:=x^3 - x^2 + x - 8;
K<t>:=Numberfield(f);
Z_K:=RingOfIntegers(K);
Basis(Z_K,K);
a = (2-t)^4;
g = MinimalPolynomial(a);
F5:=FiniteField(5);
P<x>:=PolynomialRing(F5);
g;
F<z>:=ext<F5|g>;
F;
```

These steps help us find the minimal polynomial $\overline{g}(x) = x^3 + 3x^2 + 4$ of $\overline{\alpha}$ over $\mathbb{F}_5$. We also create the field $\mathbb{F}_5(\zeta)$ in which we do our cotrace calculations. Moreover, when we get the Hecke matrices from Doud's program, we also do calculations in $\mathbb{F}_5(\zeta)$ to find the simultaneous eigenvector.

Now, we need to invoke the Artin reciprocity theorem to find $Tr(\rho(Frob_l))$ for a prime $l \neq 2$. We can use GP/Pari to compute with the Artin map as follows,

```
bnrisprincipal(bnr,q2,flag==1);
% Find the element of the ray class group corresponding to q2
```

```
idealprimedec(bnf,l);
ql;
% A prime in F lying over l, which one depends on how l factors.
bnrisprincipal(bnr,ql,flag==1);
for(k=1,61,if(Mod(j*x,62)==Mod(y,62),print(k)))
% x, y are elements of the ray class group
% corresponding to q2 and ql, respectively
```

After this step, we are able to determine the power k where $\chi(Frob_{\mathfrak{p}_l}) = \chi(Frob_{\mathfrak{p}_2}^k)$ which is needed for our computations in section 5.3.1.

B.2 Finding S_3-extensions of $\mathbb{Q}$

We use GP/Pari to search through the table of number fields ramified at specified primes (available at `http://hobbes.la.asu.edu/NFDB/`) to find the S_3-extensions satisfying the conditions in section 4.3.1.

```
v =[f1,f2,...,fn]
% Create a vector whose components are the defining polynomials given by
% the table of number fields
% Then search through these polynomials to find the one satisfying our conditions
w = vector(length(v),j,0)
for(j=1,length(v),nf = nfinit(v[j]);
P = idealprimedec(nf,p);
if(P[1].f == 3,w[j] = v[j]))
for (j=1,length(w),if(w[j]!=0,bnf=bnfinit(w[j]));
bnr = bnrinit(bnf,p);
print(bnr[5]);print(w[j]));
```

```
for(j=1,length(w),G = bnfclassunit(f);
print(G[5,1][1]))
```

After searching through the table, we found the four examples for small primes p as in section 4.3.2.

B.3 Parameterizing the Weights

In this section, we show how to use GP/Pari to find the predicted weights for the case $n = 3, p = 11, m = 14$ (section 3.4, example 3.12). The weights for the other cases can be found in a similar way.

```
for(a=0,33,
for(b=0,33,
for(c=0,33,
if(Mod(a+11*b+121*c,1330)==Mod(14,1330),print(a,",",b,",",c)))))
w = [w1,w2,...,wn];
for(j=1,length(w),
if(w[j][1]-2-w[j][2]+1<11 && w[j][2]-1-w[j][3]<11 && w[j][3]<10,
print(w[j])))
```

Bibliography

[1] *PARI/GP, version* `2.1.5`. Bordeaux, 2003. `http://pari.math.u-bordeaux.fr/`.

[2] Avner Ash, Darrin Doud, and David Pollack. Galois representations with conjectural connections to arithmetic cohomology. *Duke Math. J.*, 112(3):521–579, 2002.

[3] Avner Ash and Glenn Stevens. Cohomology of arithmetic groups and congruences between systems of Hecke eigenvalues. *J. Reine Angew. Math.*, 365:192–220, 1986.

[4] Avner Ash and Glenn Stevens. Modular forms in characteristic l and special values of their L-functions. *Duke Math. J.*, 53(3):849–868, 1986.

[5] Henri Cohen. *Advanced topics in computational number theory*, volume 193 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2000.

[6] Gary Cornell, Joseph H. Silverman, and Glenn Stevens, editors. *Modular forms and Fermat's last theorem*. Springer-Verlag, New York, 1997. Papers from the Instructional Conference on Number Theory and Arithmetic Geometry held at Boston University, Boston, MA, August 9–18, 1995.

[7] Fred Diamond and Jerry Shurman. *A first course in modular forms*, volume 228 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2005.

[8] Stephen R. Doty and Grant Walker. The composition factors of $\mathbf{F}_p[x_1, x_2, x_3]$ as a $\mathrm{GL}(3, p)$-module. *J. Algebra*, 147(2):411–441, 1992.

[9] Darrin Doud. Supersingular Galois representations and a generalization of a conjecture of Serre. *Experiment. Math.*, 16(1):119–128, 2007.

[10] Darrin Doud and Paul Jenkins. p-adic properties of coefficients of weakly holomorphic modular forms. *Int. Math. Res. Not. IMRN*, (16):3184–3206, 2010.

[11] David S. Dummit and Richard M. Foote. *Abstract algebra*. John Wiley & Sons Inc., Hoboken, NJ, third edition, 2004.

[12] William Fulton and Joe Harris. *Representation theory*, volume 129 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1991. A first course, Readings in Mathematics.

[13] Kevin James and Ken Ono. A note on the irreducibility of Hecke polynomials. *J. Number Theory*, 73(2):527–532, 1998.

[14] Chandrashekhar Khare and Jean-Pierre Wintenberger. Serre's modularity conjecture. I, II. *Invent. Math.*, 178(3):485–504, 505–586, 2009.

[15] L. J. P. Kilford. *Modular forms*. Imperial College Press, London, 2008. A classical and computational introduction.

[16] Daniel A. Marcus. *Number fields*. Springer-Verlag, New York, 1977. Universitext.

[17] Jürgen Neukirch. *Algebraic number theory*, volume 322 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1999. Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder.

[18] Kenneth A. Ribet and William A. Stein. Lectures on Serre's conjectures. In *Arithmetic algebraic geometry (Park City, UT, 1999)*, volume 9 of *IAS/Park City Math. Ser.*, pages 143–232. Amer. Math. Soc., Providence, RI, 2001.

[19] J.-P. Serre. *A course in arithmetic*. Springer-Verlag, New York, 1973. Translated from the French, Graduate Texts in Mathematics, No. 7.

[20] Jean-Pierre Serre. *Linear representations of finite groups*. Springer-Verlag, New York, 1977. Translated from the second French edition by Leonard L. Scott, Graduate Texts in Mathematics, Vol. 42.

[21] Jean-Pierre Serre. *Local fields*, volume 67 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1979. Translated from the French by Marvin Jay Greenberg.

[22] Jean-Pierre Serre. Sur les représentations modulaires de degré 2 de $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. *Duke Math. J.*, 54(1):179–230, 1987.

[23] Goro Shimura. *Introduction to the arithmetic theory of automorphic functions*. Publications of the Mathematical Society of Japan, No. 11. Iwanami Shoten, Publishers, Tokyo, 1971. Kanô Memorial Lectures, No. 1.