On Serre's Conjecture Over Imaginary Quadratic Fields

Rebecca S. Torrey

A thesis submitted for the degree of

Doctor of Philosophy at

King's College London, University of London

Department of Mathematics

King's College London

Strand

London WC2R 2LS

United Kingdom

July 2009

For my mom

Declaration

This thesis is a presentation of my own original research work. Wherever contributions of others are involved, every effort has been made to indicate this clearly with due reference to the literature.

Signature: .... Date: ....

Abstract

In this thesis, I investigate a generalization to imaginary quadratic fields of the refined version of Serre's conjecture. I ask whether a conjecture analogous to that of Buzzard, Diamond and Jarvis will hold over imaginary quadratic fields. I wrote code to compute cohomological mod ℓ modular forms over $\mathbb{Q}(i)$ of arbitrary weight. I adapt methods of Ash et al., which make use of Borel-Serre duality to express the relevant space of modular forms as a homology group, and then use modular symbols methods generalizing work of Cremona and others. Using an approach of Wiese, I prove algebraically that the modular symbols method will work in this more general setting. With data computed by my program, I provide evidence for Serre's conjecture in this context.

Acknowledgements

First and foremost, I would like to take this opportunity to thank my supervisor, Fred Diamond. I am grateful to him for his support, for his unending patience and for sharing with me his wealth of knowledge in this beautiful subject.

Other mathematicians whose assistance, advice and work have helped make this thesis possible include Avner Ash, Kevin Buzzard, John Cremona, David Dummit, Frazer Jarvis, Mehmet Haluk Şengün and Gabor Wiese. I would also like to thank Manuel Breuning, David Burns and Payman Kassaei, and all the other excellent number theorists in London. It has been an honor to be a part of the London number theory community.

My thesis is quite computational in nature, and I owe many thanks to the technical support team of the King's College maths department, particularly to Dan Wade. I would also like to thank Paul Mitchell for providing computing resources for my code.

I started my PhD at Brandeis University and I owe a great deal to many people there. In particular, I would like to thank Ruth Charney, Jennifer Johnson-Leung and Susan Parker.

Most of all, I would like to thank my friends and family for their patience, love and support. I have made some great friends among my fellow PhD students, particularly Maria Alicia Lopez Osorio, Chunyan Mu, Aftab Pande and Mark Radosevich. Their humour and support are greatly appreciated. I would like to thank my Go teacher, Guo Juan, and all my Go playing friends. I give thanks to the many friends and family who came to visit me in London, providing little snippets of home, as well as all those who sent their love via post. There are also many old friends whose support from afar I greatly appreciate. I would particularly like to thank my parents Bruce and Kathi and my siblings Mark, Kate, David and Emma and also the matriarch of our wonderful family, Grandma Eileen Noble.

Finally, I would like to thank Rich Chalmers without whose patience, support and friendship this would not have been possible.

Table of contents

List of Tables

Introduction

The Langlands Program, started in the late 1960s by Robert Langlands, is a system of powerful conjectures connecting number theory to the representation theory of certain groups. It incorporates an earlier construction of Shimura which associates Galois representations to modular forms. Serre's conjecture, first formulated by Jean-Pierre Serre in a 1987 article [Ser87], provides a converse in characteristic ℓ to Shimura's construction.

Serre's conjecture states that any odd, irreducible representation

$$\rho : \mathrm{Gal}(K/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F}_q)$$

where K is a Galois number field and $\mathbb{F}_q$ is a finite field of characteristic ℓ, is modular, i.e., arises from a modular form. A refinement to Serre's conjecture gives the minimal weight and level of this modular form and, by work of Ribet and others, we know that Serre's conjecture holds if and only if the refined version holds. Recently, Khare and Wintenberger have completed the proof of Serre's conjecture using ideas and results of Dieulefait, Kisin, Taylor and Wiles.

It is natural to ask whether an analogous conjecture holds for representations of $\mathrm{Gal}(K/F)$ where F is an arbitrary number field. Buzzard, Diamond and Jarvis [BDJ] recently formulated a version of the refined Serre's conjecture in the case in which F is totally real and ℓ is unramified, where predicting the weights is much more complicated than for $F = \mathbb{Q}$. In this more general setting, it no longer makes sense to simply specify a minimal weight and level for the corresponding modular form. A more general notion of weight is needed. Also, the refined part of the conjecture takes the form of a recipe for *all* the weight combinations for modular forms giving rise to a particular representation. This recipe depends only on the local behavior of the representation ρ at primes above ℓ. There has been some progress, due to Gee, towards proving the equivalence of Serre's conjecture and the refined Serre's conjecture for totally real fields F, but crucial steps in the method of Khare and Wintenberger break down in this situation. If F is not totally real, then the situation is even less well understood. In this case, we do not even have a complete understanding of how to associate Galois representations to modular forms. This situation is the focus of my research.

Some computational evidence is available for generalizations of Serre's conjecture to number fields. Dembélé [DDR] has done computations of arbitrary weight mod ℓ modular forms over totally real fields F, providing evidence for the conjecture of Buzzard, Diamond and Jarvis. For imaginary quadratic fields, Figueiredo [Fig99] provided some computational evidence for Serre's conjecture, but he worked only with weight two modular forms. More recently, Şengün [Ş08] proved non-existence of certain representations and has done some computations of arbitrary weight modular forms over imaginary quadratic fields.

In this thesis, I ask whether a conjecture analogous to that of Buzzard, Diamond and Jarvis will hold over imaginary quadratic fields. I wrote code to compute cohomological mod ℓ modular forms over $\mathbb{Q}(i)$ of arbitrary weight. My approach differs from that of Şengün, who computes cohomology. Instead, I compute homology using modular symbols methods generalizing work of Cremona [Cre84] and others. This homological method seems to be more promising for adapting methods developed by Cremona and others for computing forms over imaginary quadratic fields of class number greater than one.

In Chapter 2, I review the classical case, i.e. Serre's conjecture over $\mathbb{Q}$. I give basic definitions and some basic facts about modular forms and Galois representations in this setting. I state Serre's original conjecture and discuss work that has been done on the conjecture itself and towards generalizations of the conjecture.

In Chapter 3, I define Serre weights and review the conjecture of Buzzard, Diamond and Jarvis (BDJ) over totally real fields. I then define mod ℓ modular forms cohomologically for imaginary quadratic fields and ask whether the BDJ conjecture will hold in the imaginary quadratic case.

I compute examples of Galois representations in Chapter 4. Some of these examples arise from polynomials, some are from elliptic curves and others are constructed using class field theory. For each I find the level and character and then compute the predicted weights using the BDJ conjecture. I compute the predicted weights for two of the three examples given in Figueiredo's thesis.

In Chapter 5, I prove that the modular symbols method can be used to compute the space of modular forms in which I am interested. To account for the higher weights, one needs to compute cohomology with non-trivial coefficients. In this case, Cremona's geometric approach becomes intractable. I adapt methods of Ash et al., which make use of Borel-Serre duality to express the relevant space of modular forms as a homology group. From Borel-Serre [BS73], we have an isomorphism

$$H^2(\Gamma, V) \xrightarrow{\sim} H_0(\Gamma, St \otimes V),$$

where St denotes the Steinberg module, and V denotes a "Serre weight", i.e., an irreducible $\bar{\mathbb{F}}_\ell$-representation of

$$G = GL_2(\mathcal{O}_K/\ell\mathcal{O}_K).$$

Following Ash in [Ash94], I describe the Steinberg module in terms of universal minimal modular symbols. This allows one to sidestep the geometric argument, and prove algebraically that the modular symbols method can be used to compute $H_0(\Gamma, St \otimes V)$.

In order to obtain a description of the space which can actually be used for computations, one must be able to go from modular symbols to Manin symbols (M-symbols). Without recourse to Cremona's geometric method, I needed a different way to justify this conversion. Following an approach of Wiese [Wie05], I prove algebraically that one can use M-symbols to compute this homology space for $K = \mathbb{Q}(i)$.

In Chapter 6, I present computational evidence in support of the conjecture. I summarize the algorithm used in my program to compute the cohomological $\bmod \ell$ modular forms over $\mathbb{Q}(i)$. Finally, I give tables of systems of eigenvalues matching the traces of $\rho(\mathrm{Frob}_\mathfrak{p})$ of the Galois representations ρ computed in Chapter 4.

Classical Serre's Conjecture

Serre's conjecture relates Galois representations to modular forms. In this chapter, we set the stage by reviewing the classical case. We will give basic definitions of modular forms and Galois representations and then state Serre's original and refined modularity conjectures. Finally we give a brief overview of the current status of Serre's conjecture (which is now a theorem) and indicate various work undertaken towards understanding the more general situation.

2.1 Modular Forms

We start by giving the classical definition of modular forms (i.e., over $\mathbb{Q}$). Modular forms are functions on the upper half of the complex plane which satisfy certain symmetry and "boundedness" conditions. To describe these conditions in more detail, we first need some notation. Let

$$\mathfrak{h} = \{z \in \mathbb{C} \mid \operatorname{Im}(z) > 0\}$$

be the complex upper half plane. The *modular group*

$$\mathrm{SL}_2(\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{Z} \text{ and } ad - bc = 1 \right\}$$

acts on $\mathfrak{h}$ by fractional linear transformations: for $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$, and $z \in \mathfrak{h}$, we have

$$g(z) = \frac{az + b}{cz + d}.$$

Any subgroup Γ of $\mathrm{SL}_2(\mathbb{Z})$ which contains the subgroup

$$\Gamma(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \mid \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \mod N \right\}$$

for some positive integer N is called a *congruence subgroup*. The *level* of a congruence subgroup Γ is the smallest N such that $\Gamma(N) \subseteq \Gamma$. We define two important congruence subgroups in particular:

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \mid \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \mod N \right\}$$

and

$$\Gamma_1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \mid \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} * & * \\ 0 & 1 \end{pmatrix} \mod N \right\}.$$

Definition 2.1.1. A *modular form of weight k and level N* is a function on $\mathfrak{h}$ which is holomorphic everywhere (including at the cusps) and which satisfies

$$f(z) = (cz + d)^{-k} f(g(z)),$$

for all $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ in Γ, where Γ is a congruence subgroup of level N.

The modular forms of weight k for a congruence subgroup Γ form a finite dimensional complex vector space which we denote by $M_k(\Gamma)$.

For $\Gamma = \Gamma_0(N)$ or $\Gamma = \Gamma_1(N)$, we have $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \Gamma$, so that a modular form f for such a congruence subgroup satisfies

$$f(z) = f(z + 1).$$

This, together with the holomorphicity condition, implies that f has a Fourier expansion of the form

$$f(z) = \sum_{n=0}^{\infty} a_n q^n, \qquad q = e^{2\pi i z}.$$

(For any congruence subgroup Γ, we at least have $\begin{pmatrix} 1 & N \\ 0 & 1 \end{pmatrix} \in \Gamma$, giving a similar expansion but with $q = e^{2\pi i z/N}$.) If $a_0 = 0$ in the Fourier expansion of $(cz+d)^{-k} f(g(z))$ for all $g \in \mathrm{SL}_2(\mathbb{Z})$, we call f a *cusp form*. We denote the space of cusp forms by $S_k(\Gamma)$.

For $\Gamma = \Gamma_1(N)$, one can define certain operators T_n for $n \geq 1$, called Hecke operators, and $\langle d \rangle$ for $d \in (\mathbb{Z}/N\mathbb{Z})^*$, called diamond bracket operators, which act on the space $M_k(\Gamma_1(N))$ and on the space $S_k(\Gamma_1(N))$. Together these operators form a commutative algebra called the Hecke algebra $\mathcal{H} = \mathbb{Z}[T_n, \langle d \rangle]$.

A non-zero cusp form $f \in S_k(\Gamma_1(N))$ is called an *eigenform* if it is a simultaneous eigenvector for all operators in the Hecke algebra.

If $f \in S_k(\Gamma_1(N))$ is an eigenform, we define the *character* of f to be the Dirichlet character $\varepsilon : (\mathbb{Z}/N\mathbb{Z})^* \to \mathbb{C}^*$ such that $f|\langle d \rangle = \varepsilon(d) f$. We denote the space of forms with a given character ε by $S_k(\Gamma_1(N), \varepsilon)$.

We define a *system of eigenvalues* in $S_k(\Gamma_1(N), \varepsilon)$ to be a set of eigenvalues (a_n) of the Hecke operators T_n for $n \geq 1$ acting on an eigenform $f \in S_k(\Gamma_1(N), \varepsilon)$. One can show that the following relationships hold for Hecke operators:

1. $T_{mn} = T_m T_n \qquad$ if $\gcd(m, n) = 1$, and
2. $T_{p^n} = T_{p^{n-1}} T_p - p^{k-1} \varepsilon(p) T_{p^{n-2}} \qquad$ for p prime.

Thus to determine a given system of eigenvalues one need only compute the eigenvalues a_p for p prime.

2.2 Galois Representations

The Galois representations of Serre's Conjecture (and, consequently, those that will be of concern to us) are the $\bmod \ell$ Galois representations. Recall the definition:

Definition 2.2.1. A mod ℓ *Galois representation* is a continuous homomorphism

$$\rho : G_{\mathbb{Q}} \longrightarrow GL_n(\bar{\mathbb{F}}_\ell).$$

In this thesis, the representations that we will be interested in will be continuous homomorphisms

$$\rho : G_K \longrightarrow GL_2(\bar{\mathbb{F}}_\ell)$$

where K is an imaginary quadratic field and $G_K = \mathrm{Gal}(\bar{\mathbb{Q}}/K)$.

Since we are interested in the refined version of Serre's conjecture, we will also need the definitions of level, weight and character. In the following two subsections we define the level and character associated to ρ. The definition of the weight k_ρ is more complicated. Instead of defining it specifically for the classical case, we will discuss the BDJ generalization of the weight recipe in Chapter 3.

2.2.1 Level of ρ

To define the level of ρ, we follow Serre's exposition in his seminal 1987 paper on the subject ([Ser87]). The level is defined to be the Artin conductor of ρ, defined as it is in characteristic 0, except that in this case we take the prime to ℓ part of the conductor. We will now give the precise definition.

First write the Galois representation as

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

where V is a 2-dimensional vector space over $\bar{\mathbb{F}}_\ell$. Let $p \neq \ell$ be a rational prime. The representation ρ will factor through some finite extension L over $\mathbb{Q}$, so we may write

$$\rho : \mathrm{Gal}(L/\mathbb{Q}) \longrightarrow \mathrm{GL}(V).$$

Let G be the Galois group $\mathrm{Gal}(L/\mathbb{Q})$. Let

$$D_0 \supset D_1 \supset \cdots \supset D_i \supset \cdots$$

be the higher ramification groups of G corresponding to the prime p. For each i, denote by V_i the subspace of V fixed by D_i. Define the integer $n(p,\rho)$ by

$$n(p,\rho) = \sum_{i=0}^{\infty} \frac{1}{(D_0 : D_i)} \dim(V/V_i).$$

We have the following properties regarding $n(p,\rho)$.

1. $n(p,\rho) = 0$ if and only if D_0 is trivial, which is if and only if ρ is unramified at p;

2. $n(p,\rho) \geq 1$ if ρ is ramified at p;

3. $n(p,\rho) = \dim(V/V_0)$ if and only if D_1 is trivial, which is if and only if ρ is tamely ramified at p.

We define the level $N(\rho)$ by

$$N(\rho) = \prod_{p \neq \ell} p^{n(p,\rho)}.$$

This thesis is concerned with representations over an imaginary quadratic field K, i.e.

$$\rho_K : G_K \to \mathrm{GL}(V).$$

Now ρ_K will factor through some Galois extension L over K, so the Galois group in question will be $G = \mathrm{Gal}(L/K)$. From there on, we can define the level the same way, except that we will take primes $\mathfrak{p} \in \mathcal{O}_K$, so that the level

$$\mathfrak{n}(\rho_K) = \prod_{\mathfrak{p} \nmid \ell \cdot \mathcal{O}_K} \mathfrak{p}^{n(\mathfrak{p},\rho)}$$

will be an ideal of $\mathcal{O}_K$. The level will still, by definition, be prime to ℓ.

2.2.2 Character of ρ

In this section, we will define a generalization to imaginary quadratic fields K of the character ε_ρ that Serre associated to ρ in [Ser87]. This character ε_ρ will be obtained from the character

$$\det \rho : G_K = \mathrm{Gal}(\bar{\mathbb{Q}}/K) \to \mathrm{GL}_2(\bar{\mathbb{F}}_\ell)$$

by removing the ℓ part. We will now make this more precise.

Since the conductor of $\det \rho$ must divide $\ell\mathfrak{n}(\rho)$ (see, e.g., [Fig95, p 7]), we can identify $\det \rho$ with a homomorphism

$$\det \rho : (\mathcal{O}_K/\ell\mathfrak{n}(\rho))^* \to \bar{\mathbb{F}}_\ell^*,$$

or, equivalently, to a pair of homomorphisms

$$\varphi_\rho : (\mathcal{O}_K/\ell\mathcal{O}_K)^* \to \bar{\mathbb{F}}_\ell^*$$

and

$$\varepsilon_\rho : (\mathcal{O}_K/\mathfrak{n}(\rho))^* \to \bar{\mathbb{F}}_\ell^*.$$

We define the *character of* ρ to be the character ε_ρ.

2.3 Serre's Conjecture

In a 1987 paper [Ser87], Serre gave a conjecture prescribing a relationship between modular forms and mod ℓ Galois representations.

Conjecture 2.3.1. *(Serre, 1987) Suppose*

$$\rho : G_{\mathbb{Q}} \to GL_2(\bar{\mathbb{F}}_\ell),$$

is a mod ℓ Galois representation which is continuous, odd and irreducible. Then there is a modular form $f = \sum a_n q^n$ such that $tr(\rho(Frob_p)) = a_p$ and $\det(\rho(Frob_p)) = \varepsilon(p)p^{k-1}$ for all $p \nmid N\ell$. Here N is the level, k the weight and ε the character of f.

Whenever such an f does exist for a given ρ, we say that ρ is *modular*. Furthermore, Serre gave a refinement of his conjecture, in which he prescribed the minimum weight and level of such an eigenform f, assuming $k \geq 2$ and $\ell \nmid N$, using the definitions given in the preceding section (though we have omitted the definition of the weight k_ρ).

Conjecture 2.3.2. *(Serre, refined) Suppose*

$$\rho : G_{\mathbb{Q}} \to GL_2(\bar{\mathbb{F}}_\ell)$$

is a $\bmod \ell$ *Galois representation which is continuous, odd and irreducible. Then* ρ *is modular and one can take the corresponding modular form* f *to be in* $S_{k_\rho}(\Gamma, \varepsilon_\rho)$ *with* Γ *of level* $N(\rho)$*. Furthermore, the level* $N(\rho)$ *and the weight* k_ρ *are minimal among levels prime to* ℓ *and weights* $k \geq 2$*.*

Serre's conjecture is now a theorem. First, work by Ribet, Gross, Coleman-Voloch and others showed that the original conjecture and the refined conjecture are equivalent (see, e.g., [Dia97]). Recently Khare and Wintenberger ([KWa], [KWb]) proved the conjecture itself using work of Dieulefait, Taylor, Wiles and Kisin.

This thesis is concerned with a generalization of Serre's conjecture. There are two natural avenues to explore. One is to consider representations of higher dimension, i.e. representations

$$\rho : G_{\mathbb{Q}} \to \mathrm{GL}_n(\bar{\mathbb{F}}_\ell),$$

for $n > 2$. Progress has been made in developing conjectures and providing evidence for these conjectures by Ash, Doud, Pollack and Sinnott (see [ADP02] and [AS00]) and also by Herzig ([Her]). In Chapter 4 we will look at some examples of 2-dimensional representations considered in the papers by Ash et al. They use these examples to construct reducible 3-dimensional representations, but we will consider irreducible 2-dimensional representations they compute in the process.

A second natural generalization of Serre's conjecture is to consider more general number fields, i.e. representations

$$\rho : G_F = \mathrm{Gal}(\bar{\mathbb{Q}}/F) \to \mathrm{GL}_2(\bar{\mathbb{F}}_\ell),$$

for an extension F of $\mathbb{Q}$. This type of generalization is the focus of this thesis.

In a forthcoming paper, Buzzard, Diamond and Jarvis (BDJ) [BDJ] consider the case of totally real fields F. They formulate a version of Serre's refined conjecture in this context, which we will review in Section 3.3. Totally real fields are a natural starting place as there is already a complete map in the other direction, i.e. one can associate a Galois representation to a Hilbert modular cusp form.

In this situation, it no longer makes sense to talk about minimal weights. Instead Buzzard, Diamond and Jarvis define *Serre weights* to be irreducible $\bar{\mathbb{F}}_\ell$ representations σ of $\mathrm{GL}_2(\mathcal{O}/\ell\mathcal{O})$ and explain what it means for a representation to be modular of weight σ. Their conjecture then, instead of giving a minimal weight, describes all the possible Serre weights and level structures of modular forms giving rise to a given representation ρ. They show that their conjectural weight recipe is correct for $K = \mathbb{Q}$. They also cite both theoretical and computational evidence supporting the conjecture. This includes calculations by Dembélé, Diamond and Roberts [DDR] of Hilbert modular forms with these weights and level structures and their corresponding Galois representations.

The BDJ conjecture covers mod ℓ representations for unramified primes ℓ. Schein [Sch] has subsequently extended this conjecture to ramified primes $\ell > 2$. In [Gee07] and [Gee], Gee made some progress towards proving the regular and refined versions of Serre's conjecture are equivalent in the totally real case.

In a 1998 paper [Fig99], Figueiredo investigated the possibility of generalizing Serre's Conjecture to imaginary quadratic fields. He computed mod ℓ cusp forms and corresponding Galois representations, providing evidence that an analogous correspondence would also hold in this situation. His computations are limited to weight 2 and he did not formulate a refined version of Serre's Conjecture.

In this thesis we explore the refined version of Serre's conjecture over imaginary quadratic fields.

Generalized Serre's Conjecture

In this chapter, we discuss the generalization of Serre's conjecture to number fields. We define Serre weights, a generalization of the classical notion of weights. We review some basics about fundamental characters, which will be used in subsequent sections. We discuss the BDJ conjecture for totally real fields. Finally we define cohomological mod ℓ forms for imaginary quadratic fields and ask whether the BDJ conjecture will hold in this case as well.

3.1 Serre Weights

Let K be a number field and denote by $\mathcal{O}$ its ring of integers. Fix a prime ℓ which is unramified in K.

Definition 3.1.1. Define a *Serre weight* to be an irreducible $\bar{\mathbb{F}}_\ell$-representation V of $G = GL_2(\mathcal{O}/\ell\mathcal{O})$.

In this section we describe what these Serre weights look like and describe the form in which we work with them computationally.

Denote by S_K the set of embeddings $\tau : K \hookrightarrow \mathbb{C}$. Set

$$G = GL_2(\mathcal{O}/\ell\mathcal{O}) \cong \prod_{\mathfrak{p}|\ell} GL_2(\mathcal{O}/\mathfrak{p}).$$

For each prime $\mathfrak{p}$ of K such that $\mathfrak{p}|\ell$, set $k_\mathfrak{p} = \mathcal{O}/\mathfrak{p}$ and $f_\mathfrak{p} = [k_\mathfrak{p} : \mathbb{F}_\ell]$. We may identify S_K with $\prod_{\mathfrak{p}|\ell} S_\mathfrak{p}$, where $S_\mathfrak{p}$ is the set of embeddings $k_\mathfrak{p} \hookrightarrow \bar{\mathbb{F}}_\ell$. We will see that the irreducible $\bar{\mathbb{F}}_\ell$-representations of G are of the form

$$V = \bigotimes_{\mathfrak{p}|\ell} V_\mathfrak{p} \qquad \text{(the tensor product is taken over } \bar{\mathbb{F}}_\ell)$$

where

$$V_{\mathfrak{p}} = \bigotimes_{\tau \in S_{\mathfrak{p}}} \left(\det^{a_\tau} \otimes_{k_{\mathfrak{p}}} \mathrm{Sym}^{b_\tau - 1} k_{\mathfrak{p}}^2\right) \otimes_\tau \bar{\mathbb{F}}_\ell.$$

Note that the $\bar{\mathbb{F}}_\ell$-representation V is a tensor product over primes $\mathfrak{p}$ dividing ℓ; each factor $V_{\mathfrak{p}}$ will act on the corresponding factor $GL_2(\mathcal{O}/\mathfrak{p})$ of $GL_2(\mathcal{O}/\ell\mathcal{O})$.

For each of these factors $V_{\mathfrak{p}}$, we take the tensor product over all $\tau \in S_{\mathfrak{p}}$, so we will take a closer look at these embeddings τ. Fix some $\tau_0 \in S_{\mathfrak{p}}$:

$$\tau_0 : k_{\mathfrak{p}} = \mathcal{O}/\mathfrak{p} \hookrightarrow \bar{\mathbb{F}}_\ell.$$

Then for each i such that $1 \leq i < f$ where $f = [k_{\mathfrak{p}} : \mathbb{F}_\ell]$, set

$$\tau_i = \tau_0 \circ \mathrm{Frob}_\ell^i.$$

We then have $S_{\mathfrak{p}} = \{\tau_i \,:\, 0 \leq i < f\}$.

For computational purposes, we will think of $\mathrm{Sym}^{b_\tau - 1}(k_{\mathfrak{p}}^2)$ as the space of homogeneous polynomials of degree $b_\tau - 1$ in two variables with coefficients in $k_{\mathfrak{p}}$. We define the left action of $\mathrm{GL}_2(\mathcal{O}_K)$ on this space as follows: for $g \in \mathrm{GL}_2(\mathcal{O}_K)$, we reduce g modulo $\mathfrak{p}$ and then the action is given by

$$\bar{g} \cdot P(X, Y) = P(dX - bY, -cX + aY),$$

for $\bar{g} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathcal{O}_K/\mathfrak{p})$. We will also need a right action, for which we take the inverse, i.e.,

$$P(X, Y) \cdot \bar{g} = (\bar{g})^{-1} \cdot P(X, Y).$$

Since the Serre weights are irreducible representations, we may assume $1 \leq b_\tau \leq \ell$. If $b_\tau > \ell$, the ideal I generated by X^ℓ and Y^ℓ is stable under the action of G since $g(X^\ell) \in I$ and $g(Y^\ell) \in I$ so $g(I) \subseteq I$. In this case, we get a G-stable subspace of $\mathrm{Sym}^{b_\tau - 1}(\bar{\mathbb{F}}_\ell^2)$, so this is a reducible representation of G.

The determinant map is simply multiplication by the determinant (or some power of the determinant) of g for $g \in G$. This is sometimes denoted $\det^{a_\tau} k_{\mathfrak{p}}^2$. We can view the representation

$$\bigotimes_{\tau \in S_\mathfrak{p}} (\det^{a_\tau} \otimes_\tau \bar{\mathbb{F}}_\ell)$$

(where the inner tensor product is taken over the image of $k_\mathfrak{p}$ in $\bar{\mathbb{F}}_\ell$ via the embedding by that particular τ) as the tensor product of characters

$$(\tau \circ \det)^{a_\tau} : GL_2(k_\mathfrak{p}) \longrightarrow \bar{\mathbb{F}}_\ell^\times$$

for integers a_τ. That is, for each embedding τ, we have the diagram

$$\begin{array}{ccc} GL_2(k_\mathfrak{p}) & \longrightarrow & \bar{\mathbb{F}}_\ell^\times \\ \det \downarrow & & \cup \\ k_\mathfrak{p}^\times & \stackrel{\tau}{\longrightarrow} & \mathbb{F}_{\ell^f}^\times \end{array}.$$

So now we can write

$$\bigotimes_\tau (\det^{a_\tau} \otimes_\tau \bar{\mathbb{F}}_\ell) = \bigotimes_\tau (\tau \circ \det)^{a_\tau}.$$

Furthermore, writing the various $\tau \in S_\mathfrak{p}$ as τ_i (as defined above), we can express this as

$$\bigotimes_\tau (\tau \circ \det)^{a_\tau} = \bigotimes_{i=0}^{f-1} (\tau_i \circ \det)^{a_i},$$

where $a_i = a_{\tau_i}$ and both tensor products are taken over $\bar{\mathbb{F}}_\ell$. Then

$$\bigotimes_{i=0}^{f-1} (\tau_i \circ \det)^{a_i} = \prod_{i=0}^{f-1} (\tau_0 \circ \det)^{a_i \ell^i} = (\tau_0 \circ \det)^{\sum_{i=0}^{f-1} a_i \ell^i}.$$

Summarizing, we get that

$$\bigotimes_\tau (\det^{a_\tau} \otimes_\tau \bar{\mathbb{F}}_\ell) = (\tau_0 \circ \det)^{\sum_{i=0}^{f-1} a_i \ell^i}.$$

Thus the representation $\bigotimes_\tau (\det^{a_\tau} \otimes_\tau \bar{\mathbb{F}}_\ell)$ is determined by the exponents $\sum_{i=0}^{f-1} a_i \ell^i$ mod $(\ell^f - 1)$, so we can now see that to get all of these representations, it suffices to allow the a_i to run from 0 to $\ell - 1$. Taking all the $f_\mathfrak{p}$-tuples of a_i where $0 \le a_i \le \ell - 1$, we get all the distinct representations of this type, with one redundancy: if all the a_i are 0 we get the same representation as when all the a_i are $\ell - 1$. Thus we make the additional assumption that in each $f_{\mathfrak{p}}$-tuple of a_i, one of the a_i is strictly less than $\ell - 1$.

3.2 Fundamental Characters

In this section we review the concept of fundamental characters, as we will need this in the subsequent section where we define the conjectural weight recipe.

Let K be a local field of characterstic 0, so K is a finite extension of $\mathbb{Q}_p$ for some rational prime p. Let L be a finite Galois extension of K and let l and k be the residue fields of L and K respectively. There is a natural surjection of Galois groups

$$\mathrm{Gal}(L/K) \to \mathrm{Gal}(l/k).$$

We define the *inertia group of L over K, denoted $I(L/K)$,* to be the kernel of this map. For an extension L' over L we have a surjection $I(L'/K) \to I(L/K)$ and so we can define the *inertia group I_K* to be the inverse limit of the $I(L/K)$ as L ranges over all finite Galois extensions of K in $\bar{K}$.

From field theory, we know that for each n there is an extension of k of degree n, which we will denote by k_n. This extension is the splitting field of $X^{q^n} - X$ and it is unique up to k-isomorphism. The Galois group of this extension, $\mathrm{Gal}(k_n/k)$, is cyclic of order n, with canonical generator the Frobenius element $x \mapsto x^q$. Milne's Proposition 7.50 [Mil08, p.121] says the following:

Proposition 3.2.1. *Let L be an algebraic extension of K. There is a one-to-one inclusion reversing correspondence of sets*

$$\{K' \subset L,\ \textit{finite and unramified over } K\} \leftrightarrow \{k' \subset l,\ \textit{finite over } k\},$$

where k' is the residue field of K'. Furthermore, there is a canonical isomorphism

$$\mathit{Gal}(K'/K) \to \mathit{Gal}(k'/k).$$

From this proposition and the preceding discussion, we see that for each n there is a degree n unramified extension K_n of K. It is again the splitting field of $X^{q^n} - X$ and it is unique up to K-isomorphism. Since the Galois groups must be isomorphic, we see that $\mathrm{Gal}(K_n/K)$ is cyclic of order n. As before the Galois group has as canonical generator the Frobenius element σ which is the element of the Galois group satisfying the property

$$\sigma\beta \equiv \beta^q \mod \mathfrak{p} \text{ for all } \beta \in \mathcal{O}_{K_n}.$$

In subsequent sections, we will need something from local class field theory called a *fundamental character*. Fix an embedding $\bar{K} \hookrightarrow \bar{K}_{\mathfrak{p}}$. This gives us a corresponding inclusion of Galois groups

$$\mathrm{Gal}(\bar{K}_{\mathfrak{p}}/K_{\mathfrak{p}}) \hookrightarrow \mathrm{Gal}(\bar{K}/K), \qquad \sigma \mapsto \sigma|_{\bar{K}}.$$

Via this inclusion, we may regard the inertia subgroup $I_{K_{\mathfrak{p}}}$ as a subgroup of $G_K = \mathrm{Gal}(\bar{K}/K)$. Letting f denote the degree of the extension $K_{\mathfrak{p}}$ over $\mathbb{Q}_\ell$, we have that the residue field $k_{\mathfrak{p}}$ of $K_{\mathfrak{p}}$ is isomorphic to $\mathbb{F}_{\ell^f}$. Let $K'_{\mathfrak{p}} = K_{\mathfrak{p}}((-\ell)^{\frac{1}{\ell^f-1}})$. The field $K_{\mathfrak{p}}$ contains all the $(\ell^f - 1)$st roots of unity, so the extension $K'_{\mathfrak{p}}$ is Galois over $K_{\mathfrak{p}}$. We also know, from Kummer theory, that

$$\mathrm{Gal}(K'_{\mathfrak{p}}/K_{\mathfrak{p}}) = k_{\mathfrak{p}}^\times = \mathbb{F}_{\ell^f}^\times.$$

Since $K_{\mathfrak{p}}$ is unramified over $\mathbb{Q}_\ell$, the inertia group $I_{K_{\mathfrak{p}}}$ injects into the Galois group $\mathrm{Gal}(\bar{\mathbb{Q}}_\ell/K_{\mathfrak{p}})$ which, in turn, injects into $\mathrm{Gal}(\bar{\mathbb{Q}}_\ell/\mathbb{Q}_\ell)$. We thus get a map

$$I_{K_{\mathfrak{p}}} \hookrightarrow \mathrm{Gal}(\bar{\mathbb{Q}}_\ell/K_{\mathfrak{p}}) \to \mathrm{Gal}(K'_{\mathfrak{p}}/K_{\mathfrak{p}}) \to \mathbb{F}_{\ell^f}^\times,$$

where the map $\mathrm{Gal}(\bar{\mathbb{Q}}_\ell/K_{\mathfrak{p}}) \to \mathrm{Gal}(K'_{\mathfrak{p}}/K_{\mathfrak{p}})$ is simply restriction to $K'_{\mathfrak{p}}$. The map $I_{K_{\mathfrak{p}}} \to \mathbb{F}_{\ell^f}^\times$ given above is called the *fundamental character*.

3.3 The Weight Conjecture for Totally Real Fields

In this section, we will describe, at least in part, the conjectural weight recipe given by Buzzard, Diamond and Jarvis in [BDJ] for the generalization to totally real fields of the refined version of Serre's conjecture.

Let K be a totally real field and fix a prime ℓ which is unramified in K. Let $\rho : G_K \to GL_2(\bar{\mathbb{F}}_\ell)$ be a continuous, irreducible and totally odd representation.

As described in Section 3.1, each Serre weight V is of the form $V = \otimes_{\bar{\mathbb{F}}_\ell} V_\mathfrak{p}$ where each $V_\mathfrak{p}$ is an irreducible representation of $GL_2(k_\mathfrak{p})$ and the $\mathfrak{p}$ run over all the primes of K which divide ℓ. We will describe a set $W_\mathfrak{p}(\rho)$ of $GL_2(k_\mathfrak{p})$-representations; the conjectural weight set $W(\rho)$ will then consist of Serre weights of the form $V = \otimes_{\bar{\mathbb{F}}_\ell} V_\mathfrak{p}$ where each $V_\mathfrak{p} \in W_\mathfrak{p}(\rho)$.

First, we will need some more notation. For the moment, we will be working with a fixed prime $\mathfrak{p}$ dividing ℓ, so we will suppress the $\mathfrak{p}$ from the notation, i.e., instead of $k_\mathfrak{p}$, $f_\mathfrak{p}$ and $S_\mathfrak{p}$, we will simply write k, f and S, respectively. We fix an embedding $\bar{K} \hookrightarrow \bar{K}_\mathfrak{p}$ and identify $G_{K_\mathfrak{p}}$ and $I_{K_\mathfrak{p}}$ with subgroups of G_K. Denote by $K'_\mathfrak{p}$ the unramified quadratic extension of $K_\mathfrak{p}$ in $\bar{K}_\mathfrak{p}$, and extend this prime notation to its associated entities, i.e., we have k', f' and S'. (We only need to consider the quadratic extension because we are only looking at 2-dimensional representations.) Write $D = G_{K_\mathfrak{p}}$ and $D' = G_{K'_\mathfrak{p}}$. Define a projection map $\pi : S' \to S$ by $\tau' \mapsto \tau'|_k$. For an embedding $\sigma \in S$ or $\sigma \in S'$, let ω_σ denote the fundamental character of I_L defined by composing σ with the homomorphism from local class field theory $I_L \to (\mathcal{O}/\ell\mathcal{O})^\times$ (here L is either $K_\mathfrak{p}$ or $K'_\mathfrak{p}$ depending on whether σ is in S or S').

The sets $W_\mathfrak{p}(\rho)$ will only depend on the local behaviour of ρ at ℓ and we will split the definition into two cases: when $\rho|_D$ is reducible and when it is irreducible. First we consider the case where $\rho|_D$ is irreducible. For a subset J of S' such that $\pi : J \xrightarrow{\sim} S$, we define a matrix

$$M_{\vec{b},J} = \begin{pmatrix} \prod_{\tau' \in J} \omega_{\tau'}^{b_{\pi(\tau')}} & 0 \\ 0 & \prod_{\tau' \notin J} \omega_{\tau'}^{b_{\pi(\tau')}} \end{pmatrix}.$$

Then we define $W_{\mathfrak{p}}(\rho)$ by

$$W_{\mathfrak{p}}(\rho) = \left\{ V_{\vec{a},\vec{b}} \ : \ \rho|_I \sim \prod_{\tau \in S} \omega_\tau^{a_\tau} M_{\vec{b},J} \text{ for some } J \subset S' \text{ such that } \pi : J \xrightarrow{\sim} S \right\}.$$

In this case, when $\rho|_D$ is irreducible, we can write $\rho|_D$ as the induction of a character, i.e., $\rho|_D \sim \mathrm{Ind}_{D'}^D \xi$ for some character $\xi : D' \to \bar{\mathbb{F}}_\ell^\times$. We use this to define a set $W'(\xi)$ which is very close to $W_{\mathfrak{p}}(\rho)$:

$$W'(\xi) = \left\{ (V_{\vec{a},\vec{b}}, J) \ : \ J \subset S',\ \pi : J \xrightarrow{\sim} S,\ \xi|_I = \prod_{\tau \in S} \omega_\tau^{a_\tau} \prod_{\tau' \in J} \omega_{\tau'}^{b_{\pi(\tau')}} \right\}.$$

We have $W_{\mathfrak{p}}(\rho) = \{V | (V, J) \in W'(\xi) \text{ for some } J\}$ and so we have a projection map $W'(\xi) \to W_{\mathfrak{p}}(\rho)$. We have another projection $W'(\xi) \to \{J \subset S' | \pi : J \xrightarrow{\sim} S\}$. Both of these projections are usually bijections, so that $|W_{\mathfrak{p}}(\rho)| \sim 2^f$. (Note that, in the above, if we replace the character ξ by its conjugate under D/D', this simply replaces J by its complement in S'.)

Choose some $\tau_0' \in S'$ and set $\tau_i' = \tau_0' \circ \mathrm{Frob}_\ell^i$ and $\tau_i = \pi(\tau_i')$. Then we have $S = \{\tau_i \mid i \in \mathbb{Z}/f\mathbb{Z}\}$ and $S' = \{\tau_i' \mid i \in \mathbb{Z}/2f\mathbb{Z}\}$. Denote the fundamental characters for our fixed τ_0 and τ_0' by $\omega = \omega_{\tau_0}$ and $\omega' = \omega_{\tau_0'}$. Then we can write the other fundamental characters in terms of these two, namely, $\omega_{\tau_i} = \omega^{\ell^i}$ and $\omega_{\tau_i'} = (\omega')^{\ell^i}$. We also have $\omega = (\omega')^{\ell^f+1}$. Note that $\xi|_I = (\omega')^n$ for some $n \mod \ell^{2f} - 1$ and $\rho|_D$ irreducible implies that $(\ell^f + 1)$ does not divide n.

The following proposition, which is a combination of Propositions 3.1 and 3.2 in [BDJ], analyzes the combinatorics of the situation to make more precise the notion that $|W_{\mathfrak{p}}(\rho)|$ is close to 2^f.

Proposition 3.3.1. *Suppose ℓ is an odd prime and ξ, $W'(\xi)$ and n are defined as above. Define A to be the set of congruence classes* $\mod \ell^f + 1$ *of the form*

$$\begin{cases} -1 + (\ell+1) \sum_{i \in B^*} (-1)^i \ell^i & \text{if } f \text{ is even} \\ (\ell+1) \sum_{i \in B^*} (-1)^i \ell^i & \text{if } f \text{ is odd,} \end{cases}$$

where, in both cases, B^* *runs over all non-empty proper subsets of* $\{0, 1, \ldots, f-1\}$*. The conjugacy classes of* A *are distinct and non-zero. Furthermore, we have*

$$|W'(\xi)| = \begin{cases} 2^f & n \notin A \\ 2^f - 1 & n \in A. \end{cases}$$

On the other hand, suppose $\ell = 2$*. Then*

$$|W'(\xi)| = \begin{cases} 2^f - 1 & \text{if } f \text{ is even} \\ 2^f & \text{if } f \text{ is odd and } 3 \nmid n \\ 2^f - 3 & \text{if } f \text{ is odd and } 3 \mid n. \end{cases}$$

We review part of the proof as it will be useful in computing the predicted weights. Define

$$n'_{a,\vec{b},B} = a(\ell^f + 1) + \sum_{i \in B} b_i \ell^i + \sum_{i \notin B} b_i \ell^{f+i} \mod \ell^{2f} - 1,$$

where

$$\begin{aligned} &a \in \mathbb{Z}/(\ell^f - 1)\mathbb{Z}, \\ &\vec{b} = (b_0, \ldots, b_{f-1}) \text{ with } 1 \le b_i \le \ell \text{ and} \\ &B \subset \{0, \ldots, f-1\}. \end{aligned}$$

We then have a bijection of sets

$$W'(\xi) \leftrightarrow \{(a, \vec{b}, B) \mid n \equiv n'_{a,\vec{b},B} \mod \ell^{2f} - 1\}.$$

For each subset B of $\{0, \ldots, f-1\}$, there is a bijection between such triples $(a, \vec{b}, B)$ and solutions of the congruences

$$n \equiv \sum_{i \in B} b_i \ell^i - \sum_{i \notin B} b_i \ell^i \mod \ell^f + 1, \tag{3.1}$$

with all the b_i in $\{1, \ldots, \ell\}$. But the values of the expression on the right hand side, $\sum_{i \in B} b_i \ell^i - \sum_{i \notin B} b_i \ell^i$, consist of the ℓ^f consecutive integers from $n'_B - \ell^f$ to $n'_B - 1$,

where

$$n'_B = \sum_{i \in B} \ell^{i+1} - \sum_{i \notin B} \ell^i + 1.$$

So long as $n \not\equiv n'_B \mod \ell^f + 1$, we get a unique solution to the congruence (3.1) and so we have a bijection of sets

$$W'(\xi) \leftrightarrow \{B \mid n \not\equiv n'_B \mod \ell^f + 1\}.$$

Also, the projection $W'(\xi) \to \{J \subset S' \mid \pi : J \xrightarrow{\sim} S\}$ is injective.

Buzzard, Diamond and Jarvis also give the following proposition, which gives criteria for determining when multiple B occur with the same $(a, \vec{b})$.

Proposition 3.3.2. *(Proposition 3.3 in [BDJ]) The projection map from $W'(\xi)$ to $W_{\mathfrak{p}}(\rho)$ fails to be injective if and only if $\ell^r n \equiv m \mod \ell^f + 1$ for some integers r, m with $|m| \leq \ell(\ell^{f-2} - 1)/(\ell - 1)$.*

Now consider the case where $\rho|_{G_{K_{\mathfrak{p}}}}$ is reducible. We write

$$\rho|_{G_{K_{\mathfrak{p}}}} \sim \begin{pmatrix} \chi_1 & * \\ 0 & \chi_2 \end{pmatrix}.$$

We define a set $W'(\chi_1, \chi_2)$, depending on these two characters, as follows:

$$W'(\chi_1, \chi_2) = \left\{ (V_{\vec{a},\vec{b}}, J) \ : \ J \subset S,\ \chi_1|_{I_{K_{\mathfrak{p}}}} = \prod_{\tau \in S} \omega_\tau^{a_\tau} \prod_{\tau \in J} \omega_\tau^{b_\tau},\ \chi_2|_{I_{K_{\mathfrak{p}}}} = \prod_{\tau \in S} \omega_\tau^{a_\tau} \prod_{\tau \notin J} \omega_\tau^{b_\tau} \right\}.$$

The weight set $W_{\mathfrak{p}}(\rho)$ will be defined as a subset of the projection $\pi_1(W'(\chi_1, \chi_2))$ onto the first component. Writing $\rho|_D \sim \begin{pmatrix} \chi_1 & * \\ 0 & \chi_2 \end{pmatrix}$, let c_ρ be the corresponding class in $H^1(K_{\mathfrak{p}}, \chi_1 \chi_2^{-1})$. To a given pair $\alpha = (V_{\vec{a},\vec{b}}, J) \in W'(\chi_1, \chi_2)$, Buzzard, Diamond and Jarvis associate a certain subspace $L_\alpha \subset H^1(K_{\mathfrak{p}}, \bar{\mathbb{F}}_\ell(\chi_1 \chi_2^{-1}))$ and then define the weight set by:

$$W_{\mathfrak{p}}(\rho) = \{V_{\vec{a},\vec{b}} \ : \ c_\rho \in L_\alpha \text{ for some } \alpha = (V_{\vec{a},\vec{b}}, J) \in W'(\chi_1, \chi_2)\}.$$

See [BDJ] for the definition of the subspace L_α.

We analyze the set $W'(\chi_1, \chi_2)$ combinatorally, similar to the analysis in the irreducible case above. We will see that the projection $\pi_2 : W'(\chi_1, \chi_2) \to \{J \subset S\}$ is usually a bijection (and otherwise not far off) so that $|W'(\chi_1, \chi_2)| \sim 2^f$. Note also that interchanging χ_1 and χ_2 in $W'(\chi_1, \chi_2)$ replaces J by its complement.

Find n_1 and n_2 in $\mathbb{Z}/(\ell^f - 1)\mathbb{Z}$ such that

$$\begin{aligned} \chi_1 &= \omega^{n_1}, \text{ and} \\ \chi_2 &= \omega^{n_2}, \end{aligned}$$

and set $n = n_1 - n_2$.

The following three propositions are Propositions 3.4, 3.5 and 3.6 in [BDJ].

Proposition 3.3.3. *Suppose that $\ell > 3$. Define A to be the set of congruence classes* mod $\ell^f - 1$ *of the form*

$$\begin{cases} -1 + (\ell+1)\sum_{i \in B^*} (-1)^i \ell^i & \textit{if } f \textit{ is odd} \\ (\ell+1)\sum_{i \in B^*} (-1)^i \ell^i & \textit{if } f \textit{ is even,} \end{cases}$$

where, in the first case B^* runs over all subsets of $\{0, 1, \dots, f-1\}$, and in the second case B^* runs over all non-empty proper subsets of $\{0, 1, \dots, f-1\}$. The elements of A are distinct and non-zero. Furthermore, we have

$$|W'(\chi_1, \chi_2)| = \begin{cases} 2^f + 2 & \textit{if } n = 0 \textit{ and } f \textit{ is even,} \\ 2^f + 1 & \textit{if } n \in A, \\ 2^f & \textit{otherwise.} \end{cases}$$

Proposition 3.3.4. *Suppose that $\ell = 3$. Define A to be the set of congruence classes* mod $(3^f - 1)/2$ *of the form*

$$\begin{cases} -1 + 4\sum_{i \in B^*} (-1)^i 3^i & \textit{if } f \textit{ is odd} \\ 4\sum_{i \in B^*} (-1)^i 3^i & \textit{if } f \textit{ is even,} \end{cases}$$

where, in the first case B^* *runs over all subsets of* $\{0,1,\ldots,f-1\}$ *other than* $\{0,2,\ldots,f-1\}$ *and* $\{1,3,\ldots,f-2\}$*, and in the second case* B^* *runs over all non-empty proper subsets of* $\{0,1,\ldots,f-1\}$ *other than* $\{0,2,\ldots,f-2\}$ *and* $\{1,3,\ldots,f-1\}$*. The elements of* A *are distinct and non-zero. Furthermore, we have*

$$|W'(\chi_1,\chi_2)| = \begin{cases} 2^f+2 & \text{if } n=0 \text{ and } f \text{ is even, or } n=(3^f-1)/2 \\ 2^f+1 & \text{if } n \in A, \\ 2^f & \text{otherwise.} \end{cases}$$

Proposition 3.3.5. *Suppose* $\ell = 2$*. Then*

$$|W'(\chi_1,\chi_2)| = \begin{cases} 2^f+4 & \text{if } n=0 \text{ and } f \text{ is even,} \\ 2^f+3 & \text{if } n\neq 0,\ 3\mid n \text{ and } f \text{ is even,} \\ 2^f+2 & \text{if } n=0 \text{ and } f \text{ is odd,} \\ 2^f+1 & \text{if } n\neq 0 \text{ and } f \text{ is odd,} \\ 2^f & \text{if } 3\nmid n \text{ and } f \text{ is even.} \end{cases}$$

We recall part of the proof of the above propositions, as we will use the techniques to compute the weights in the reducible case. Define

$$n'_{a,\vec{b},B} = a + \sum_{i\in B} b_i \ell^i \mod \ell^f - 1$$

for

$$\begin{aligned} &a \in \mathbb{Z}/(\ell^f-1)\mathbb{Z}, \\ &\vec{b} = (b_0,\ldots,b_{f-1}), \text{ with } 1 \le b_i \le \ell, \text{ and} \\ &B \subset \{0,\ldots,f-1\}. \end{aligned}$$

Let $\bar{B}$ denote the complement of B in $\{0,\ldots,f-1\}$. We look for triples $(a,\vec{b},B)$ as above such that

$$\begin{aligned} n_1 &\equiv n'_{a,\vec{b},B} \mod (\ell^f-1) \text{ and} \\ n_2 &\equiv n'_{a,\vec{b},\bar{B}} \mod (\ell^f-1). \end{aligned}$$

Such triples are in bijection with $W'(\chi_1, \chi_2)$.

We can instead look for solutions of

$$n \equiv \sum_{i \in B} b_i \ell^i - \sum_{i \notin B} b_i \ell^i \mod \ell^f - 1.$$

For a particular subset $B \subset \{0, \dots f-1\}$, there is a unique triple $(a, \vec{b}, B)$ for each solution of the above. We can use

$$n_B = \sum_{i \in B} \ell^{i+1} - \sum_{i \notin B} \ell^i$$

to determine the number of solutions. In particular the values of $\sum_{i \in B} b_i \ell^i - \sum_{i \notin B} b_i \ell^i$ are precisely the ℓ^f consecutive integers from $n_B + 1 - \ell^f$ to n_B. Thus if $n \not\equiv n_B \mod \ell^f - 1$, then we have a unique solution but if $n \equiv n_B \mod \ell^f - 1$, then we have two solutions.

Buzzard, Diamond and Jarvis also give the following proposition, which gives a criterion for determining when multiple B occur with the same $(a, \vec{b})$.

Proposition 3.3.6. *(Proposition 3.7 in [BDJ]) The projection map from $W'(\chi_1, \chi_2)$ onto its first component fails to be injective if and only if $\ell^r n \equiv m \mod \ell^f - 1$ for some integers r, m with $|m| \le \max\{0,\ \ell(\ell^{f-2} - 1)/(\ell - 1)\}$.*

Note in particular that if $n = 0$ (e.g., in the case where ρ restricted to the decomposition group is trivial), then the projection map in the above proposition is not injective.

3.4 Cohomological mod ℓ Forms Over K

For the purposes of this thesis, we will define modular forms over an imaginary quadratic field K cohomologically.

Let $\mathcal{O}_K$ denote the ring of integers of K. Analogous to the classical case, we define the group $\Gamma(\mathfrak{n})$ for an ideal $\mathfrak{n} \subset \mathcal{O}_K$ by

$$\Gamma(\mathfrak{n}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathcal{O}_K) \;\middle|\; \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \mod \mathfrak{n} \right\}.$$

A *congruence subgroup* Γ is a subgroup of $\mathrm{GL}_2(\mathcal{O}_K)$ which contains $\Gamma(\mathfrak{n})$ for some ideal $\mathfrak{n}$. The following two congruence subgroups are of particular importance:

$$\Gamma_0(\mathfrak{n}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathcal{O}_K) \;\middle|\; \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \mod \mathfrak{n} \right\}$$

and

$$\Gamma_1(\mathfrak{n}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathcal{O}_K) \;\middle|\; \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} * & * \\ 0 & 1 \end{pmatrix} \mod \mathfrak{n} \right\}.$$

Our definition of modular forms involves certain operators $T_\mathfrak{p}$ called Hecke operators, which we will define in Section 5.5.

Definition 3.4.1. We define a *cohomological* mod ℓ *form of level* $\mathfrak{n}$ *and Serre weight* V to be a non-trivial cohomology class $v \in H^2(\Gamma, V)$ which is a simultaneous eigenvector for the Hecke operators $T_\mathfrak{p}$ for all primes $\mathfrak{p}$ such that $\mathfrak{p} \nmid \ell\mathfrak{n}$. Here, Γ is a congruence subgroup of level $\mathfrak{n}$.

3.5 Serre's Conjecture for Imaginary Quadratic Fields

We need to define what it means for a representation ρ to be modular of weight V. Here, V is a Serre weight, i.e., V is an irreducible $\bar{\mathbb{F}}_\ell$-representation of $G = \mathrm{GL}_2(\mathcal{O}/\ell\mathcal{O})$. We have seen that such representations are of the form

$$V = \bigotimes_{\mathfrak{p}|\ell} V_\mathfrak{p}$$

where

$$V_{\mathfrak{p}} = \bigotimes_{\tau \in S_{\mathfrak{p}}} \left(\det^{a_\tau} \otimes_{k_{\mathfrak{p}}} \mathrm{Sym}^{b_\tau - 1} k_{\mathfrak{p}}^2\right) \otimes_\tau \bar{\mathbb{F}}_\ell.$$

To a modular form f we associate a homomorphism, which we will again denote by f, as follows. We first define the Hecke algebra, $\mathbb{T} = \bar{\mathbb{F}}_\ell[T_r : r \nmid \ell\mathfrak{n}]$, where T_r is the Hecke operator for r prime. Then we can consider a modular form f to be a homomorphism

$$\begin{aligned} f : \mathbb{T} &\to \bar{\mathbb{F}}_\ell[a_r : r \nmid \ell\mathfrak{n}] \\ T_r &\mapsto a_r, \end{aligned}$$

where a_r is the eigenvalue of the form f for the Hecke operator T_r.

To a Galois representation $\rho : G_K \to \mathrm{GL}_2(\bar{\mathbb{F}}_\ell)$, we can associate a maximal ideal in the Hecke algebra $\mathbb{T}$ as follows. From ρ, we get a map

$$\begin{aligned} \mathbb{T} &\to \bar{\mathbb{F}}_\ell \\ T_r &\mapsto \mathrm{tr}(\rho(\mathrm{Frob}_r)). \end{aligned}$$

We then get an exact sequence

$$0 \to \mathfrak{m}_\rho \to \mathbb{T} \to \bar{\mathbb{F}}_\ell,$$

with $\mathfrak{m}_\rho = \langle T_r - \mathrm{tr}(\rho(\mathrm{Frob}_r))\rangle \subset \mathbb{T}$ the maximal ideal we associate to ρ. We also define $M_{\Gamma,V} = H^2(\Gamma, V)$.

Definition 3.5.1. Let $\rho : G_K \to \mathrm{GL}_2(\bar{\mathbb{F}}_\ell)$ be a continuous, irreducible representation and V a Serre weight. We say that ρ is *modular of weight V* if $M_{\Gamma,V}[\mathfrak{m}_\rho] \neq 0$.

Note that this is equivalent to requiring that there be a non-zero modular form $f \in M_{\Gamma,V}$ such that the eigenvalue a_r of $T_r(f)$ is equal to $\mathrm{tr}(\rho(\mathrm{Frob}_r))$ in $\bar{\mathbb{F}}_\ell$ for all primes $r \nmid \ell\mathfrak{n}$.

The main question concerning this thesis is the following.

Question 3.5.2. *Let K be an imaginary quadratic field and suppose*

$$\rho : G_K \to GL_2(\bar{\mathbb{F}}_\ell)$$

is a continuous, irreducible representation. Is it true that ρ is modular of weight V for every Serre weight V in the BDJ conjectural weight set $W(\rho)$?

Remark 3.5.3. *In Serre's original conjecture, he requires that the representation ρ be odd. For a representation of G_K where K is an imaginary quadratic field, there is no odd/even distinction.*

Examples of Galois Representations

In this chapter, we compute examples of Galois representations. The examples we compute come from three sources: elliptic curves, class field theory and representations arising from polynomials.

Much of the data in this chapter was computed with a variety of mathematical software systems, including KANT/KASH [DF+97], Magma [BCP97], PARI/GP [The05] and Sage [Ste].

4.1 Examples from Elliptic Curves

Fix a prime ℓ and let E be an elliptic curve over $K = \mathbb{Q}(i)$ which is supersingular at ℓ and which has good reduction at ℓ. To such an elliptic curve E one can associate a mod ℓ Galois representation ρ_E such that

1. the level of ρ_E is equal to the conductor of the elliptic curve E;
2. the character of ρ_E is trivial; and
3. the traces $a_\mathfrak{p}$ of $\rho_E(\mathrm{Frob}_\mathfrak{p})$ are given by the sequence $\{a_p\}_E$ associated to the elliptic curve, reduced $\mod \ell$.

Furthermore, with the above assumptions, we know the local behaviour of ρ_E at ℓ. In particular, we will look at the case $\ell = 7$. Letting I_7 denote the inertia group at 7, we have

$$\rho_E|_{I_7} \sim \begin{pmatrix} \omega & 0 \\ 0 & \omega^7 \end{pmatrix},$$

where ω denotes the level 2 fundamental character. Using the BDJ recipe, we have

$$\chi_1 = \omega^1$$
$$\chi_2 = \omega^7,$$

so $n_1 = 1$ and $n_2 = 7$. The inertia degree for 7 in $K = \mathbb{Q}(i)$ is $f = 2$, so we will have

$$a \in \mathbb{Z}/(\ell^f - 1)\mathbb{Z} = \mathbb{Z}/48\mathbb{Z}$$
$$\vec{b} = (b_0, b_1) \text{ and}$$
$$B \subset \{0,\ 1\}.$$

We need to find triples $(a, \vec{b}, B)$ such that

$$n_1 \equiv n_{a,\vec{b},B} = a + \sum_{i \in B} 7^i b_i \mod 48, \qquad \text{and}$$
$$n_2 \equiv n_{a,\vec{b},\bar{B}} = a + \sum_{i \in \bar{B}} 7^i b_i \mod 48.$$

For each of the four subsets B, we get one solution $(a, \vec{b})$. We then compute $\vec{a} = (a_0, a_1)$ by computing $a \equiv a_0 + 7a_1 \mod 48$. We list the predicted weights in Table 4.2.

Table 4.1: Weights for elliptic curves mod 7

ℓ	char	$\vec{a} = (a_0, a_1)$	$\vec{b} = (b_0, b_1)$
7	1	$(0, 0)$	$(1, 1)$
7	1	$(0, 0)$	$(7, 7)$
7	1	$(1, 0)$	$(5, 7)$
7	1	$(0, 1)$	$(7, 5)$

The examples we compute in this section come from elliptic curves over $\mathbb{Q}(i)$ computed by Cremona in [Cre84]. Cremona computed modular forms (with coefficients in $\mathbb{Q}$, i.e. with trivial weight) corresponding to these elliptic curves, so we already know that the representations associated to these elliptic curves are modular. Here we compute all the weights in which we expect to find modular forms giving rise to these representations. By computing the modular forms for those weights and levels, we provide computational evidence for the BDJ conjecture in this setting.

In his tables, Cremona lists elliptic curves by giving their a_i coefficients for the Weierstrass equation

$$E \;:\; y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

In order to determine whether these elliptic curves are supersingular and have good reduction at ℓ, we first complete the square to get an equation of the form

$$E \;:\; y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6$$

where

$$\begin{aligned} b_2 &= a_1^2 + 4a_2 \\ b_4 &= 2a_4 + a_1a_3 \\ b_6 &= a_3^2 + 4a_6. \end{aligned}$$

We will also need

$$\begin{aligned} b_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2, \text{ and} \\ \Delta &= -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6. \end{aligned}$$

This last quantity Δ is called the *discriminant* of the Weierstrass equation. Considering Δ modulo ℓ tells us whether E has good reduction modulo ℓ, i.e., whether the reduction of E modulo ℓ is non-singular.

To test whether E is supersingular at ℓ, we use the following theorem. (See, e.g., [Sil86, p. 140].)

Theorem 4.1.1. *Suppose K is a finite field of characteristic $\ell \neq 2$. Let E be an elliptic curve over K given by Weierstrass equation*

$$E \;:\; y^2 = f(x),$$

where $f(x) \in K[x]$ has degree 3 and has distinct roots in $\bar{K}$. The curve E is supersingular if and only if the $x^{\ell-1}$ term in $f(x)^{(\ell-1)/2}$ has coefficient equal to zero.

Of the curves listed in Cremona's table, we found several which are both supersingular and have good reduction at $\ell = 7$. We list the a_i coefficients for these curves in the following table, along with their conductors $\mathfrak{f}$ and the norms of the conductors $N\mathfrak{f}$. We indicate those curves whose sequences $\{a_\mathfrak{p}\}$ suggest that the corresponding modular form is actually Galois over $\mathbb{Q}$ (judging by whether $a_\mathfrak{p}$ equals $a_{\bar{\mathfrak{p}}}$ for split primes $p\mathcal{O}_K = \mathfrak{p}\bar{\mathfrak{p}}$). We are, of course, more interested in those which are *not* Galois over $\mathbb{Q}$. In the rightmost column, we indicate whether the corresponding modular form was found for all of the predicted weights (listed above in Table 4.1).

Table 4.2: Elliptic curves over $\mathbb{Q}(i)$ mod 7 with several levels

a_1	a_2	a_3	a_4	a_6	$\mathfrak{f}$	$N\mathfrak{f}$	Gal/$\mathbb{Q}$	f
$1+i$	0	$1+i$	$1-i$	0	$(6+6i)$	72	✓	✓
i	$1-i$	i	$-i$	0	$(9+7i)$	130		✓
1	1	1	0	0	(15)	225	✓	✓
i	-1	0	$2-i$	i	$(19+9i)$	442		✓

In Section 6.3, we give the $\{a_\mathfrak{p}\}_E$ sequence for some small primes $\mathfrak{p}$ and the $\{a_\mathfrak{p}\}$ coefficients computed for the corresponding modular forms.

4.2 Examples from Polynomials

In this section we will examine examples of Galois representations arising from polynomials. We will determine the level, character and predicted weights for each representation.

4.2.1 Techniques & Background

Here we will review some background, stating basic theorems and describing general techniques, which will be used in the subsequent sections to analyze the various examples of Galois representations.

Let $p(x)$ be an irreducible polynomial in $\mathbb{Q}[x]$, and denote by L the Galois closure of the field generated by $p(x)$ over $\mathbb{Q}$. We will look at 2-dimensional mod ℓ

representations of the Galois group $\mathrm{Gal}(L/\mathbb{Q})$. Taking the image of $\mathrm{Gal}(\bar{\mathbb{Q}}/L)$ to be trivial, we get a representation

$$\rho_{\mathbb{Q}} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\bar{\mathbb{F}}_\ell),$$

which factors through $\mathrm{Gal}(L/\mathbb{Q})$. We are interested in representations of G_K for imaginary quadratic fields K, so we take the restriction to K of the above representation, giving us

$$\rho_K : G_K \to \mathrm{GL}_2(\bar{\mathbb{F}}_\ell),$$

which factors through $\mathrm{Gal}(M/K)$, where M is the composite field LK.

If we start with a representation $\rho_{\mathbb{Q}}$ over $\mathbb{Q}$ which is *odd*, i.e. $\det \rho(\sigma_\infty) = -1$, then we already know $\rho_{\mathbb{Q}}$ is modular by Serre's conjecture. Instead, we will start with *even* representations $\rho_{\mathbb{Q}}$, and look at the base change to K.

Once we have a representation

$$\rho_K : G_K \to \mathrm{GL}_2(\bar{\mathbb{F}}_\ell),$$

we need to compute the level, weight and character of ρ_K in order to figure out where to look for corresponding modular forms. We will of course also have to compute the coefficients $\{a_{\mathfrak{p}}\}$ for primes $\mathfrak{p}$.

To compute the level of ρ_K, we will look at all primes dividing the discriminant of the polynomial, except ℓ. For each such prime p, we compute $n(p, \rho|_{\mathbb{Q}})$. In the examples we compute we will have p unramified in K for all primes p dividing the level N of the representation $\rho|_{\mathbb{Q}}$. When this is the case, we have $n(\mathfrak{p}, \rho|_K) = n(p, \rho|_{\mathbb{Q}})$ for primes $\mathfrak{p}$ lying above p. The corresponding level to check will be

$$\mathfrak{n} = \prod \mathfrak{p}^{n(\mathfrak{p},\rho)}.$$

As discussed earlier, we know that for any prime p which is tamely ramified in L, we have $n(p, \rho) = \dim(V/V_0)$, where V_0 is the subspace of V fixed by the inertia group $I_{\mathfrak{P}}$ for some prime $\mathfrak{P}$ of L lying above p. We often make use of the basic fact that $|I_{\mathfrak{P}}|$

is equal to the ramification index $e_{\mathfrak{P}/p}$. If p is wildly ramified in L, the determination of $n(p, \rho)$ requires further analysis.

To determine the possible Serre weights $V_{\vec{a},\vec{b}}$, we consider the primes $\mathfrak{p}$ lying above ℓ. For each such prime $\mathfrak{p}$, we need to consider the local behaviour of ρ_K at $\mathfrak{p}$. We then apply the weight recipe in [BDJ] to compute the possible weights $V_{\mathfrak{p}}$. There are two cases: when the restriction of ρ_K to the decomposition group $D_{\mathfrak{p}}$ is irreducible and when it is reducible. In either case, we will examine the restriction of ρ_K to the inertia group $I_{\mathfrak{p}}$. We make use of the combinatorial analysis in [BDJ], which provides formulas for the number of different weights $V_{\mathfrak{p}}$ for each prime $\mathfrak{p}$ above ℓ, to check that we have found all possible weights.

In those cases where we compute the base change from a representation over $\mathbb{Q}$, we make use of some basic facts regarding base change to compute the coefficients $\{a_{\mathfrak{p}}\}$. Recall that we want to compute the restriction of the representation ρ to the imaginary quadratic field $K = \mathbb{Q}(i)$,

$$\rho_K = \rho|_K : G_K \to \mathrm{GL}_2(\bar{\mathbb{F}}_\ell).$$

Let $M = KL$ be the composite of K and L. Since both K and L are Galois over $\mathbb{Q}$, we know that M is Galois over $\mathbb{Q}$ and M is Galois over K. In our examples, we will consider totally real extensions L, so we have $K \cap L = \mathbb{Q}$, and thus

$$G = \mathrm{Gal}(M/K) \cong \mathrm{Gal}(L/\mathbb{Q})$$

and

$$\begin{gathered}\mathrm{Gal}(M/\mathbb{Q}) \cong \mathrm{Gal}(K/\mathbb{Q}) \times \mathrm{Gal}(L/\mathbb{Q}) \\ \sigma \mapsto (\sigma|_K,\ \sigma|_L).\end{gathered}$$

Suppose p is a rational prime which is unramified in M, and let $\mathfrak{P}$ be a prime of M lying above p. Let $\mathfrak{p}_K = \mathfrak{P} \cap K$ and, likewise, $\mathfrak{p}_L = \mathfrak{P} \cap L$. We need to compute $a_{\mathfrak{p}_K}$ for M over K from a_p for L over $\mathbb{Q}$.

We examine the two cases: p splits in K and p is inert in K.

Case 1 (p splits in K): We have $p = \mathfrak{p}_K \bar{\mathfrak{p}}_K$. Suppose for some prime $\mathfrak{P}$ of M

lying over p, we have $\mathfrak{p}_K = \mathfrak{P} \cap K$. The inertia degree $f(\mathfrak{p}_K/p)$ is equal to 1. Thus we have

$$\left[\frac{M/K}{\mathfrak{P}}\right] = \left(\left[\frac{K/\mathbb{Q}}{\mathfrak{p}_K}\right] \times \left[\frac{L/\mathbb{Q}}{\mathfrak{p}_L}\right]\right).$$

The decomposition group $D_{\mathfrak{p}_K}$ is trivial. Then, since $\mathrm{Frob}_{\mathfrak{p}_K} \in D_{\mathfrak{p}_K}$, we must have

$$\left[\frac{K/\mathbb{Q}}{\mathfrak{p}_K}\right] = \mathrm{Frob}_{\mathfrak{p}_K} = 1.$$

We now have

$$\rho_K\left(\left[\frac{M/K}{\mathfrak{P}}\right]\right) = \rho\left(\left[\frac{L/\mathbb{Q}}{\mathfrak{p}_L}\right]\right)$$

and so, of course, the traces will be the same as well, i.e., $a_{\mathfrak{p}_K} = a_{\bar{\mathfrak{p}}_K} = a_p$.

Case 2 (p is inert in K): We have $p = \mathfrak{p}_K^2$. The inertia degree $f(\mathfrak{p}_K/p)$ is equal to 2. Thus we have

$$\begin{aligned}\left[\frac{M/K}{\mathfrak{P}}\right] &= \left(\left[\frac{K/\mathbb{Q}}{\mathfrak{p}_K}\right] \times \left[\frac{L/\mathbb{Q}}{\mathfrak{p}_L}\right]\right)^2 \\ &= \left(\left[\frac{K/\mathbb{Q}}{\mathfrak{p}_K}\right]^2 \times \left[\frac{L/\mathbb{Q}}{\mathfrak{p}_L}\right]^2\right) \\ &= \left(\mathrm{id} \times \left[\frac{L/\mathbb{Q}}{\mathfrak{p}_L}\right]^2\right),\end{aligned}$$

and so

$$\rho_K\left(\left[\frac{M/K}{\mathfrak{P}}\right]\right) = \rho\left(\left[\frac{L/\mathbb{Q}}{\mathfrak{p}_L}\right]^2\right) = \rho^2\left(\left[\frac{L/\mathbb{Q}}{\mathfrak{p}_L}\right]\right).$$

We can use this relationship to compute $a_{\mathfrak{p}}$ from a_p. Alternatively, we could use the following method.

Denote by a_p the trace of $\rho_{\mathbb{Q}}(\mathrm{Frob}_p)$ and denote by $b_{\mathfrak{p}}$ the trace of $\rho_K(\mathrm{Frob}_{\mathfrak{p}_K})$. Suppose $a_p = \alpha + \beta$, for some $\alpha, \beta \in \bar{\mathbb{F}}_\ell$ with $\alpha\beta = \det(\rho_{\mathbb{Q}}(\mathrm{Frob}_p))$. Then we have

$$\begin{aligned}b_{\mathfrak{p}} &= \alpha^2 + \beta^2 \\ &= (\alpha+\beta)^2 - 2\det(\rho_{\mathbb{Q}}(\mathrm{Frob}_p)) \\ &= a_p^2 - 2\det(\rho_{\mathbb{Q}}(\mathrm{Frob}_p)).\end{aligned}$$

We want to compute the sequence $\{a_{\mathfrak{p}}\}$ associated to the representation ρ, i.e.

we want to compute $\mathrm{tr}(\rho(\mathrm{Frob}_{\mathfrak{p}}))$ for each prime $\mathfrak{p}$ of $\mathcal{O}_K$ where $\mathfrak{p}$ is unramified in $M = LK$. Let $\mathfrak{P}$ be a prime of M lying over $\mathfrak{p}$. Denote by $\bar{\mathcal{O}}_K$ the residue field of $\mathcal{O}_K$ and likewise for M.

Since $\mathfrak{p}$ is unramified in M, the Frobenius automorphism $\mathrm{Frob}_{\mathfrak{p}}$ is uniquely defined ([Jan96, p 125]). Also, $\mathrm{Frob}_{\mathfrak{p}}$ generates the Galois group $\mathrm{Gal}(\bar{\mathcal{O}}_M/\bar{\mathcal{O}}_K)$ of the residue field extension corresponding to the field extension M over K. We know that

$$\mathrm{Gal}(\bar{\mathcal{O}}_M/\bar{\mathcal{O}}_K) \cong \mathrm{Gal}(\mathbb{F}_{q^f}/\mathbb{F}_q),$$

where $q = |\bar{\mathcal{O}}_K|$ and $f = f(\mathfrak{P}/\mathfrak{p})$ is the inertia degree of $\mathfrak{P}$ over $\mathfrak{p}$. Thus the order of the element $\mathrm{Frob}_{\mathfrak{p}}$ is equal to the inertia degree f. When the image $\rho(\mathrm{Gal}(M/K))$ is isomorphic to $\mathrm{Gal}(M/K)$, we know that the order of $\rho(\mathrm{Frob}_{\mathfrak{p}})$ is equal to the order of the $\mathrm{Frob}_{\mathfrak{p}}$. Often, the order of $\rho(\mathrm{Frob}_{\mathfrak{p}})$ is sufficient to determine the trace of $\rho(\mathrm{Frob}_{\mathfrak{p}})$.

4.2.2 Dihedral Group D_4

In this section, we compute an example with dihedral group D_4, which appears in Ash, Doud and Pollack [ADP02].

Example 4.2.1. *Representation* $\bmod 5$ *with level* $\mathfrak{n} = 29$

The totally real polynomial

$$x^4 - x^3 - 3x^2 + x + 1, \qquad \mathrm{disc} = 5^2 \times 29,$$

has Galois closure L defined by the polynomial

$$x^8 - 6x^7 - 13x^6 + 102x^5 + 27x^4 - 438x^3 + 25x^2 + 252x + 49.$$

The Galois group $G = \mathrm{Gal}(L/\mathbb{Q})$ is isomorphic to the dihedral group D_4. We will take $\ell = 5$. There is one irreducible 2-dimensional $\bmod 5$ representation of D_4. Since the extension L over $\mathbb{Q}$ is totally real, this representation is necessarily even and hence not covered by Serre's conjecture. (However, since it has solvable image, it is known to be modular by proven cases of Artin's conjecture.) We consider the base change ρ_K from $\mathbb{Q}$ to $K = \mathbb{Q}(i)$ of this representation.

In the following table we give, for each conjugacy class in the image of ρ, a representative element along with its order, length (of conjugacy class), determinant, $a_\mathfrak{p}$ = trace, and $b_\mathfrak{p} = \mathrm{tr}^2 - 2\det$. For a split prime $p\mathcal{O}_K = \mathfrak{p}\bar{\mathfrak{p}}$ we have $\mathrm{tr}(\rho(\mathrm{Frob}_\mathfrak{p})) = a_\mathfrak{p} = a_{\bar{\mathfrak{p}}}$ and for an inert prime $p\mathcal{O}_K = \mathfrak{p}$ we have $\mathrm{tr}(\rho(\mathrm{Frob}_\mathfrak{p})) = b_\mathfrak{p}$.

rep	order	length	det	$a_\mathfrak{p}$	$b_\mathfrak{p}$
$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	1	1	1	2	2
$\begin{pmatrix} 4 & 0 \\ 0 & 4 \end{pmatrix}$	2	1	1	3	2
$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$	2	2	4	0	2
$\begin{pmatrix} 4 & 0 \\ 0 & 1 \end{pmatrix}$	2	2	4	0	2
$\begin{pmatrix} 0 & 4 \\ 1 & 0 \end{pmatrix}$	4	2	1	0	3

From the above table, we see that $\det(\rho)$ is a quadratic character, and so we get a nontrivial character for ρ, which is a quadratic character on $(\mathcal{O}_K/29\mathcal{O}_K)^*$. We will denote this character by ε_{29}.

To compute the level, we find the ramification index at $p = 29$ is $e_{29} = 2$. Since $p = 29$ is tamely ramified, we have $n(29, \rho) = \dim(V/V_0)$. The inertia group I_{29} has order 2 and is not central. The representation ρ restricted to such a subgroup of D_4 fixes a space of dimension 1, so $n(29, \rho) = 1$ and the level of this representation is $\mathfrak{n} = 29$.

We use the BDJ recipe to compute the weights for $\ell = 5$. We compute the ramification index $e_5 = 2$ and the inertia degree $f_5 = 2$. Furthermore, we compute that $\rho|_{I_5}$ fixes a one dimensional subspace and so is of the form

$$\rho|_{I_5} \sim \begin{pmatrix} \omega^2 & 0 \\ 0 & 1 \end{pmatrix},$$

where ω is the mod 5 cyclotomic character. We use the reducible case of BDJ, and we have

$$\chi_1 = \omega^2$$
$$\chi_2 = \omega^0,$$

so $n_1 = 2$ and $n_2 = 0$. The inertia degree for 5 in $K = \mathbb{Q}(i)$ is $f = 1$, so we will have

$$a \in \mathbb{Z}/(\ell^f - 1)\mathbb{Z} = \mathbb{Z}/4\mathbb{Z}$$
$$\vec{b} = (b_0) \text{ and}$$
$$B \subset \{0\}.$$

We need to find triples (a, b_0, B) such that

$$n_1 \equiv n_{a,b_0,B} = a + \sum_{i \in B} 5^i b_i \mod 4, \qquad \text{and}$$
$$n_2 \equiv n_{a,b_0,\bar{B}} = a + \sum_{i \in \bar{B}} 5^i b_i \mod 4.$$

For each of the two subsets B, we get one solution (a, b_0). In particular, for $B = \{0\}$, we get $a = 0$, $b_0 = 2$ and for $B = \emptyset$, we get $a = 2$, $b_0 = 2$. The analysis is the same regardless of which prime we choose above $\ell = 5$, and so, for $K = \mathbb{Q}(i)$, we combine the results to get the various possible weights, which we list in Table 4.3.

Table 4.3: D_4 representation mod 5 with level $\mathfrak{n} = 29$

ℓ	level	char	$\vec{a} = (a_0, a_1)$	$\vec{b} = (b_0, b_1)$	f
5	29	ε_{29}	$(0, 0)$	$(2, 2)$	✓
5	29	ε_{29}	$(0, 2)$	$(2, 2)$	
5	29	ε_{29}	$(2, 0)$	$(2, 2)$	
5	29	ε_{29}	$(2, 2)$	$(2, 2)$	✓

For two of the four weights in the above table, we did not find the form as expected. There was a form found in those weights that looks as though it might be a twist of the expected form. Further investigation is required to determine what is happening here.

In Section 6.4.1 we provide a table with the orders of $\mathrm{Frob}_{\mathfrak{p}}$ along with the coefficients $a_\mathfrak{p}$ of the corresponding system of eigenvalues for some small primes $\mathfrak{p}$ for this representation.

4.2.3 Alternating Group A_4

Example 4.2.2. *Representation* mod 3 *with level* $\mathfrak{n} = 61$

In [Fig99, p 117], Figueiredo gives three examples of A_4 representations. The first of these examples comes from the polynomial

$$x^4 - 7x^2 - 3x + 1 \qquad \text{disc } = 3^2 \times 61^2.$$

Figueiredo considers the mod 3 representation arising from this polynomial using the isomorphism $A_4 \cong \mathrm{PSL}_2(\mathbb{F}_3)$. He shows that there must be a lift of this representation to $\mathrm{GL}_2(\bar{\mathbb{F}}_3)$. I will instead compute representations directly from the $\hat{A}_4$ extension, where $\hat{A}_4$ is a double cover of A_4, isomorphic to $\mathrm{SL}_2(\mathbb{F}_3)$. From the database of Klüners and Malle [KM], we find the polynomial giving the $\hat{A}_4$ extension of Figueiredo's polynomial:

$$x^8 + 3x^7 - 11x^6 - 9x^5 + 21x^4 + 9x^3 - 11x^2 - 3x + 1$$

which has Galois closure given by the following degree 24 polynomial:

$$\begin{aligned} x^{24} &- 9x^{23} - 206x^{22} + 1680x^{21} + 16053x^{20} - 112863x^{19} - 585638x^{18} \\ &+ 3495552x^{17} + 9763561x^{16} - 57615780x^{15} - 68523951x^{14} \\ &+ 519956256x^{13} + 95882805x^{12} - 2594932704x^{11} + 1213595253x^{10} \\ &+ 6932798424x^9 - 6682968027x^8 - 8573027148x^7 + 13459018536x^6 \\ &+ 1679228685x^5 - 10467091917x^4 + 4152416400x^3 + 1245998376x^2 \\ &- 1023909417x + 155570139 \end{aligned}$$

We denote this Galois closure by L.

We take $\ell = 3$. There is only one irreducible 2-dimensional mod 3 representation

$$\rho : G_K \to \mathrm{GL}_2(\bar{\mathbb{F}}_3)$$

factoring through $\mathrm{Gal}(LK/K)$. We get this representation by taking the base change to $K = \mathbb{Q}(i)$ from the representation $\rho_{\mathbb{Q}}$ of $G_{\mathbb{Q}}$, which we get simply by restricting $G_{\mathbb{Q}}$ to $\mathrm{Gal}(L/\mathbb{Q})$ and then applying the following isomorphisms and inclusion:

$$\mathrm{Gal}(L/\mathbb{Q}) \cong \hat{A}_4 \cong \mathrm{SL}_2(\mathbb{F}_3) \hookrightarrow \mathrm{GL}_2(\mathbb{F}_3).$$

For the level, we need only compute $n(61, \rho)$. We have the ramification index $e_{61} = 3$ in L, and so 61 is tamely ramified and $n(61, \rho) = \dim(V/V_0)$. We check that ρ restricted to the subgroup of order 3 fixes a 1-dimensional subspace of V, so $n(61, \rho) = 1$ and the level of ρ is $\mathfrak{n} = 61$.

Since the image of ρ is $\mathrm{SL}_2(\mathbb{F}_3)$, we see that $\det(\rho)$ is trivial, and so the character of ρ is trivial as well.

To compute the weights, we look at the representation locally at $\ell = 3$ and apply the BDJ recipe. We compute the ramification index $e_3 = 4$ and the inertia degree $f_3 = 2$, and we note that the inertia degree of 3 in $K = \mathbb{Q}(i)$ is $f = 2$. The decomposition group at 3 for L over $\mathbb{Q}$ has order 8, and the only order 8 subgroup is the quaternion group Q_8. If we consider the restriction of $\rho_{\mathbb{Q}}$ to the decomposition group, we would be in the irreducible case of BDJ. However, we want to consider the restriction of $\rho_{\mathbb{Q}}$ first to $K = \mathbb{Q}(i)$, which we denote by ρ, and then to the decomposition group at 3. Then we have ρ restricted to D_3 is reducible, and we can write

$$\rho|_{D_3} \sim \begin{pmatrix} \omega^{(\ell^2-1)/4} & 0 \\ 0 & \omega^{-(\ell^2-1)/4} \end{pmatrix}$$

and so we have

$$\chi_1 = \omega^{(\ell^2-1)/4} = \omega^2$$
$$\chi_2 = \omega^{-(\ell^2-1)/4} = \omega^{-2}.$$

Thus $n_1 = 2$ and $n_2 = 6$. (Recall that $n_\nu \in \mathbb{Z}/(\ell^f - 1)\mathbb{Z} = \mathbb{Z}/8\mathbb{Z}$.) We need to find triples $(a, \vec{b}, B)$ with

$$\begin{aligned} &a \in \mathbb{Z}/8\mathbb{Z} \\ &B \subset \{0, \dots, f-1\} \text{ and} \\ &\vec{b} = (b_0, b_1), \text{ with } 1 \le b_i \le \ell = 3 \end{aligned}$$

such that

$$\begin{aligned} n_1 \equiv n_{a,\vec{b},B} &= a + \sum_{i \in B} 3^i b_i \mod 8, \qquad \text{and} \\ n_2 \equiv n_{a,\vec{b},\bar{B}} &= a + \sum_{i \in \bar{B}} 3^i b_i \mod 8. \end{aligned}$$

For two of the four subsets B (namely, $B = \{0\}$ and $B = \{1\}$) we get one solution $(a, \vec{b})$, while for the other two ($B = \{0, 1\}$ and $B = \emptyset$) we get two solutions $(a, \vec{b})$. We then compute $\vec{a} = (a_0, a_1)$ by writing $a = a_0 + 3a_1 \mod 8$. In Table 4.4 we list the possible weights.

Table 4.4: A_4 representation mod 3 with level $\mathfrak{n} = 61$

ℓ	level	B	$\vec{a} = (a_0, a_1)$	$\vec{b} = (b_0, b_1)$	f
3	61	$\{0, 1\}$	$(0, 2)$	$(1, 1)$	✓
3	61	$\{0, 1\}$	$(0, 2)$	$(3, 3)$	✓
3	61	$\{1\}$	$(1, 1)$	$(2, 2)$	✓
3	61	$\{0\}$	$(0, 0)$	$(2, 2)$	✓
3	61	$\emptyset$	$(2, 0)$	$(1, 1)$	✓
3	61	$\emptyset$	$(2, 0)$	$(3, 3)$	✓

We need to compute the coefficients $\{a_\mathfrak{p}\}$. When p splits in K, say $p \cdot \mathcal{O}_K = \mathfrak{p}\bar{\mathfrak{p}}$, we have

$$a_\mathfrak{p} = a_{\bar{\mathfrak{p}}} = a_p.$$

The image of our representation is $\mathrm{SL}_2(\mathbb{F}_3)$, so we have $\det = 1$. Therefore if $p = \mathfrak{p}$ is inert in K, we get

$$\begin{aligned} b_\mathfrak{p} &= \mathrm{tr}(\rho(\mathrm{Frob}_p))^2 - 2 \cdot \det(\rho(\mathrm{Frob}_p)) \\ &= b_p^2 - 2 \\ &\equiv b_p^2 + 1 \mod 3. \end{aligned}$$

In the following table we give representatives for each conjugacy class in $\mathrm{SL}_2(\mathbb{F}_3)$, the order of those elements, the trace (equal to $a_\mathfrak{p}$ when p splits in K) and $b_\mathfrak{p}$ when p is inert in K.

Rep	Order	$\mathrm{tr} = a_\mathfrak{p}$	$b_\mathfrak{p}$
$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	1	-1	-1
$\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$	2	1	-1
$\begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$	3	-1	-1
$\begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$	3	-1	-1
$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$	4	0	1
$\begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$	6	1	-1
$\begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix}$	6	1	-1

In Section 6.4.2 we provide a table with the orders of $\mathrm{Frob}_\mathfrak{p}$ along with the coefficients of the corresponding systems of eigenvalues for some small primes $\mathfrak{p}$ for this representation.

Example 4.2.3. *Representation* mod 3*, level* $\mathfrak{n} = 79$

Figueiredo's second example in [Fig99] comes from the polynomial

$$P = x^4 - x^3 - 24x^2 + x + 11 \qquad \text{disc } = 3^4 \times 79^2.$$

This is a totally real A_4 extension of $\mathbb{Q}$. It is a subfield of an $\hat{A}_4$ extension generated by the following polynomial

$$x^8 - 17x^6 + 60x^4 - 29x^2 + 1,$$

which has as its Galois closure the field defined by the following degree 24 polynomial

$$x^{24} - 255x^{22} + 27807x^{20} - 1706560x^{18} + 65353749x^{16} - 1637285385x^{14} \\ + 27343876078x^{12} - 303898414365x^{10} + 2196602852661x^{8} - 9790619278320x^{6} \\ + 24093731990727x^{4} - 25093789540875x^{2} + 2600398130625.$$

Let L denote the field generated by this degree 24 extension.

We take $\ell = 3$, so we will be considering $\mod 3$ representations of $\mathrm{Gal}(L/\mathbb{Q}) \cong \hat{A}_4 \cong \mathrm{SL}_2(\mathbb{F}_3)$. There is only one such irreducible degree 2 representation.

We need to compute the level of this representation. Since we are considering this representation $\mod 3$ and the only primes ramifying in this extension are 3 and 79, we need only consider $p = 79$ for the level. The ramification at $p = 79$ is tame and so $n(79, \rho) = \dim(V/V_0)$. We compute the ramification index $e_{79} = 3$ and denote the inertia group at 79 by I_{79}. We find that $\rho|_{I_{79}}$ fixes a 1-dimensional subspace of V, so $n(79, \rho) = 1$ and the level of this representation is $\mathfrak{n} = 79$.

Since the image of this representation is isomorphic to $\mathrm{SL}_2(\mathbb{F}_3)$, the character will be trivial.

We now use the BDJ recipe to compute the weights. For $\ell = 3$ we find the ramification index $e_3 = 3$ and the inertia degree $f_3 = 2$. Globally, the decomposition group at 3 would then have order 6. However, as in the previous example, we consider the restriction of the representation to $K = \mathbb{Q}(i)$, and so the decomposition group D_3 in this case will have order 3. We are thus in the reducible case of BDJ. We can write

$$\rho|_{D_3} \sim \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix},$$

and so we have

$$\chi_1 = \omega^0$$
$$\chi_2 = \omega^0,$$

with $n_1 = n_2 = 0$ (and so also $n = 0$). We need to find triples $(a, \vec{b}, B)$ with

$$a \in \mathbb{Z}/8\mathbb{Z},$$
$$\vec{b} = (b_0, b_1) \text{ with } 1 \le b_i \le \ell = 3 \text{ and}$$
$$B \subset \{0, 1\}$$

such that

$$0 \equiv n_{a,\vec{b},B} = a + \sum_{i \in B} 3^i b_i \mod 8, \qquad \text{and}$$
$$0 \equiv n_{a,\vec{b},\bar{B}} = a + \sum_{i \in \bar{B}} 3^i b_i \mod 8.$$

For two of the four subsets B (namely, $B = \{0, 1\}$ and $B = \emptyset$) we get one solution $\vec{b}$ (but two solutions for $(\vec{a}, \vec{b})$), while for the other two ($B = \{0\}$ and $B = \{1\}$) we get two solutions $(a, \vec{b})$ each. However there is some symmetry here: we get the same solutions for $B = \{0\}$ as for $B = \{1\}$, and we get the same solutions for $B = \emptyset$ as for $B = \{0, 1\}$. This symmetry is expected by Proposition 3.3.6, since $n = 0$. We compute $\vec{a} = (a_0, a_1)$ by writing $a = a_0 + 3a_1 \mod 8$. In Table 4.5 we list the possible weights.

Table 4.5: A_4 representation mod 3 with level $\mathfrak{n} = 79$

ℓ	level	char	B	$\vec{a} = (a_0, a_1)$	$\vec{b} = (b_0, b_1)$	f
3	79	1	$\{0,1\}$, $\emptyset$	$(0, 0)$	$(2, 2)$	✓
3	79	1	$\{1\}$, $\{0\}$	$(1, 2)$	$(1, 3)$	
3	79	1	$\{1\}$, $\{0\}$	$(2, 1)$	$(3, 1)$	

The weights in Table 4.5 are the weights in $W'(\chi_1, \chi_2)$ in the BDJ notation for the reducible case. Recall that, for these weights to be in the predicted weight set $W_{\mathfrak{p}}(\rho)$, they must satisfy the additional condition that the corresponding cohomology class c_ρ be contained in a certain subspace $L_\alpha \subset H^1(K_{\mathfrak{p}}, \bar{\mathbb{F}}_\ell(\chi_1\chi_2^{-1}))$. In this case, one can show that this condition is not met for the latter weights (those with $\vec{b} = (1, 3)$ and $\vec{b} = (3, 1)$). Thus we only expect this form to show up in the former weight (with $\vec{b} = (2, 2)$) and, as indicated in the final column, that is indeed what we found.

In Section 6.4.2 we provide a table with the orders of $\mathrm{Frob}_{\mathfrak{p}}$ along with the coefficients of the corresponding systems of eigenvalues for some small primes $\mathfrak{p}$ for this representation.

4.3 Examples from Class Field Theory

4.3.1 Dihedral Group D_3

For this section, we assume $\ell \neq 3$. Write the elements of D_3 as rotations r^k and reflections sr^k for $0 \leq k \leq 2$. If w is a third root of unity in $\bar{\mathbb{F}}_\ell^*$, we get one irreducible 2-dimensional representation ρ of D_3. We can write the action of ρ on the elements of D_3 as follows (see, e.g., [Ser77, p.36])

$$\rho(r^k) = \begin{pmatrix} w^k & 0 \\ 0 & w^{-k} \end{pmatrix}, \qquad \rho(sr^k) = \begin{pmatrix} 0 & w^{-k} \\ w^k & 0 \end{pmatrix}.$$

In the following table, we give the trace, determinant and order of the images of ρ on the elements of D_3.

	r^0	r^1	r^2	sr^0	sr^1	sr^2
trace	2	-1	-1	0	0	0
det	1	1	1	-1	-1	-1
order	1	3	3	2	2	2

To compute the coefficients $b_\mathfrak{p}$ in the base change to $K = \mathbb{Q}(i)$ when $\mathfrak{p}$ is inert, we use the formula

$$b_\mathfrak{p} = \mathrm{tr}(\rho_\mathbb{Q}(\mathrm{Frob}_p))^2 - 2 \cdot \det(\rho_\mathbb{Q}(\mathrm{Frob}_p)),$$

where p is the rational prime below $\mathfrak{p}$. We get the following values for $b_\mathfrak{p}$ when $\mathfrak{p}$ is inert in $\mathbb{Q}(i)$.

	r^0	r^1	r^2	sr^0	sr^1	sr^2
$b_\mathfrak{p}$	2	-1	-1	2	2	2

Example 4.3.1. *Representations* mod 5 *and* mod 7 *with levels* $\mathfrak{n} = 8 + 17i$, $\mathfrak{n} = 13 + 28i$ *and* $\mathfrak{n} = 8 + 35i$

The following examples are not arising as base change of even representations over $\mathbb{Q}$, but are representations directly over $K = \mathbb{Q}(i)$. We get these examples by considering quadratic extensions of $\mathbb{Q}(i)$ which are ramified only at a single prime $\mathfrak{p}$, split over $\mathbb{Q}$, and which have class group isomorphic to the cyclic group of order 3. I would like to thank Gabor Wiese for showing me this source of examples. At the time, we had been considering these examples mod 2, but as 2 is ramified in $\mathbb{Q}(i)$, it is not covered by the BDJ recipe. Schein's extension of the BDJ recipe to the ramified case ([Sch]) does not cover $\ell = 2$. In the following we will consider these representations mod 5 and mod 7. This allows us to see the different behaviour in the weights modulo an inert prime as compared to a split prime.

The representation ρ will factor through an extension L of $K = \mathbb{Q}(i)$ where $G = \mathrm{Gal}(L/K)$ is isomorphic to D_3. In all cases the representation will have a quadratic character $\varepsilon : (\mathcal{O}_K/\mathfrak{p})^* \to \bar{\mathbb{F}}_\ell^*$.

For the level, we need only consider this single ramified prime $\mathfrak{p}$, which will have ramification index $e_\mathfrak{p} = 2$ in the extension L over K. The representation ρ restricted to the order 2 subgroup of D_3 fixes a one-dimensional subspace, so that the level in each case will be precisely equal to this prime, i.e., $\mathfrak{n} = \mathfrak{p}$.

In all three examples, the primes above 5 and 7 in $\mathbb{Q}(i)$ will be unramified in the dihedral extension L over K. Thus, in all cases, the representation ρ restricted to the inertia group I at ℓ will be trivial and so we have

$$\chi_1 = \omega^0$$
$$\chi_2 = \omega^0,$$

and $n = n_1 = n_2 = 0$. The difference in the weight computations arises from the prime ℓ being split or inert. Note that for both cases $n = 0$ implies, according to Proposition 3.3.6, that we will have multiple subsets B with the same $(a, \vec{b})$.

For $\ell = 5$ (exemplifying the split case), we need to find triples (a, b_0, B) with

$$\begin{aligned} &a \in \mathbb{Z}/4\mathbb{Z}, \\ &1 \le b_0 \le 5 \text{ and} \\ &B \subset \{0\} \end{aligned}$$

such that

$$\begin{aligned} 0 &\equiv n_{a,b_0,B} = a + \sum_{i \in B} 5^i b_i \mod 4, \qquad \text{and} \\ 0 &\equiv n_{a,b_0,\bar{B}} = a + \sum_{i \in \bar{B}} 5^i b_i \mod 4. \end{aligned}$$

If we take either $B = \{0\}$ or $B = \emptyset$, we have the congruences

$$\begin{aligned} &0 \equiv a + b_0 \mod 4, \qquad \text{and} \\ &0 \equiv a \mod 4. \end{aligned}$$

Thus a is 0 and $b_0 = 4$.

For $\ell = 7$ (exemplifying the inert case), we look for triples $(a, \vec{b}, B)$ with

$$\begin{aligned} &a \in \mathbb{Z}/48\mathbb{Z}, \\ &\vec{b} = (b_0, b_1) \text{ with } 1 \le b_i \le 7 \text{ and} \\ &B \subset \{0, 1\} \end{aligned}$$

such that

$$\begin{aligned} 0 &\equiv n_{a,b_0,B} = a + \sum_{i \in B} 7^i b_i \mod 48, \qquad \text{and} \\ 0 &\equiv n_{a,b_0,\bar{B}} = a + \sum_{i \in \bar{B}} 7^i b_i \mod 48. \end{aligned}$$

We again have some symmetry: the cases $B = \{0, 1\}$ and $B = \emptyset$ will yield the same system of congruences and the cases $B = \{1\}$ and $B = \{0\}$ will yield the same system of congruences. For the former, we have

$$\begin{aligned} &0 \equiv a + b_0 + 7b_1 \mod 48, \qquad \text{and} \\ &0 \equiv a \mod 48, \end{aligned}$$

giving $\vec{b} = (6,6)$ and $a = 0$ so $\vec{a} = (0,0)$. In the latter case, we have

$$0 \equiv a + b_0 \mod 48, \qquad \text{and}$$
$$0 \equiv a + 7b_1 \mod 48,$$

giving $\vec{a} = (5,6)$ with $\vec{b} = (1,7)$ and $\vec{a} = (6,5)$ with $\vec{b} = (7,1)$.

The primes for which we found such dihedral extensions are

$$\mathfrak{n} = (8 + 17i) \text{ (lying over } p = 353\text{)},$$
$$\mathfrak{n} = (13 + 28i) \text{ (lying over } p = 953\text{) and}$$
$$\mathfrak{n} = (8 + 35i) \text{ (lying over } p = 1289\text{)}.$$

In Table 4.6, we list all the combinations of weights, level, character and prime ℓ for the above examples, and indicate in the final column (under f) whether a corresponding modular form was found.

Table 4.6: D_3 representations mod 5 and mod 7 with several levels

ℓ	level	char	$\vec{a} = (a_0, a_1)$	$\vec{b} = (b_0, b_1)$	f
5	$8 + 17i$	ε_{8+17i}	$(0,0)$	$(4,4)$	✓
7	$8 + 17i$	ε_{8+17i}	$(0,0)$	$(6,6)$	✓
7	$8 + 17i$	ε_{8+17i}	$(5,6)$	$(1,7)$	✓
7	$8 + 17i$	ε_{8+17i}	$(6,5)$	$(7,1)$	✓
5	$13 + 28i$	ε_{13+28i}	$(0,0)$	$(4,4)$	✓
7	$13 + 28i$	ε_{13+28i}	$(0,0)$	$(6,6)$	✓
7	$13 + 28i$	ε_{13+28i}	$(5,6)$	$(1,7)$	✓
7	$13 + 28i$	ε_{13+28i}	$(6,5)$	$(7,1)$	✓
5	$8 + 35i$	ε_{8+35i}	$(0,0)$	$(4,4)$	✓
7	$8 + 35i$	ε_{8+35i}	$(0,0)$	$(6,6)$	✓
7	$8 + 35i$	ε_{8+35i}	$(5,6)$	$(1,7)$	✓
7	$8 + 35i$	ε_{8+35i}	$(6,5)$	$(7,1)$	✓

In Section 6.5.1 we provide tables with the orders of $\mathrm{Frob}_{\mathfrak{p}}$ along with the coefficients $a_{\mathfrak{p}}$ of the corresponding system of eigenvalues for some small primes $\mathfrak{p}$ for each of the three levels $\mathfrak{n}$ above.

4.3.2 Dihedral Group D_5

Example 4.3.2. *Representation* mod 11 *with level* $\mathfrak{n} = 19 + 20i$

In this section we look at another example which is a representation directly over $K = \mathbb{Q}(i)$, not a base change from a representation over $\mathbb{Q}$. This one was constructed in the same way as the D_3 examples of this sort in Section 4.3.1. For the prime $19 + 20i$ (lying over $p = 761$), we get a quadratic extension of $\mathbb{Q}(i)$ which is ramified only at $19 + 20i$ and which has class group isomorphic to the cyclic group of order 5. Thus we get an extension L of $K = \mathbb{Q}(i)$ such that the Galois group $G = \mathrm{Gal}(L/K)$ is isomorphic to D_5.

We will consider this representation modulo $\ell = 11$, for which prime we have an irreducible 2-dimensional representation of D_5. The image of $\det(\rho)$ is ± 1, so the character of ρ will be a quadratic character $\varepsilon_{19+20i} : (\mathcal{O}_K/(19 + 20i)\mathcal{O}_K)^* \to \bar{\mathbb{F}}_\ell^*$.

In the following table we give, for each conjugacy class in the image of ρ, a representative element along with its order, length (of conjugacy class), determinant and trace.

rep	order	length	det	trace
$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	1	1	1	2
$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$	2	5	10	0
$\begin{pmatrix} 4 & 0 \\ 0 & 3 \end{pmatrix}$	5	2	1	7
$\begin{pmatrix} 5 & 0 \\ 0 & 9 \end{pmatrix}$	5	2	1	3

The ramification index of $\mathfrak{p} = 19 + 20i$ in L over K is $e_\mathfrak{p} = 2$. The fixed space of ρ restricted to the order 2 subgroup of D_5 has dimension 1 so the level of ρ is $\mathfrak{n} = 19 + 20i$.

To compute the weights, we apply the BDJ recipe in the reducible case. The prime above 11 is unramified in the extension L over K, so the restriction of ρ to the inertia group I for $\ell = 11$ is trivial. Thus we have

$$\chi_1 = \omega^0$$
$$\chi_2 = \omega^0,$$

so $n_1 = n_2 = 0$. Note that $n = 0$ implies, according to Proposition 3.3.6, that we will have multiple subsets B with the same $(a, \vec{b})$. We look for triples $(a, \vec{b}, B)$ with

$$a \in \mathbb{Z}/120\mathbb{Z},$$
$$\vec{b} = (b_0, b_1) \text{ with } 1 \leq b_i \leq 11 \text{ and}$$
$$B \subset \{0, 1\}$$

such that

$$0 \equiv n_{a,b_0,B} = a + \sum_{i \in B} 11^i b_i \mod 120, \qquad \text{and}$$
$$0 \equiv n_{a,b_0,\bar{B}} = a + \sum_{i \in \bar{B}} 11^i b_i \mod 120.$$

For the subsets $B = \{0, 1\}$ and $B = \emptyset$ we get the same system of congruences, namely:

$$0 \equiv a + b_0 + 11b_1 \mod 120, \qquad \text{and}$$
$$0 \equiv a \mod 120,$$

giving $\vec{b} = (10, 10)$ and $a = 0$ so $\vec{a} = (0, 0)$.

For the subsets $B = \{1\}$ and $B = \{0\}$ we get the same system of congruences, namely:

$$0 \equiv a + b_0 \mod 120, \qquad \text{and}$$
$$0 \equiv a + 11b_1 \mod 120,$$

giving $\vec{a} = (9, 10)$ with $\vec{b} = (1, 11)$ and $\vec{a} = (10, 9)$ with $\vec{b} = (11, 1)$.

In Table 4.7, we list the possible weights with the level and character for this example and indicate in the final column whether a corresponding form was found. The case for which it has not yet been found has not been checked due to size limitations in the computations.

Table 4.7: D_5 representation mod 11 with level $\mathfrak{n} = 19 + 20i$

ℓ	level	char	$\vec{a} = (a_0, a_1)$	$\vec{b} = (b_0, b_1)$	f
11	$19 + 20i$	ε_{19+20i}	$(0, 0)$	$(10, 10)$	
11	$19 + 20i$	ε_{19+20i}	$(9, 10)$	$(1, 11)$	✓
11	$19 + 20i$	ε_{19+20i}	$(10, 9)$	$(11, 1)$	✓

In Section 6.5.2 we provide a table with the orders of $\mathrm{Frob}_{\mathfrak{p}}$ along with the coefficients of the corresponding systems of eigenvalues for some small primes $\mathfrak{p}$ for this representation.

Computing Modular Forms over $\mathbb{Q}(i)$

5.1 Borel-Serre Duality

Recall that the space we want to compute is $H^2(\Gamma, V)$ for some congruence subgroup Γ and some Serre weight V. Instead of computing this cohomology group directly, we use Borel-Serre duality to compute a homology group with coefficients in the Steinberg module. The homology group is computationally friendly because we can express the Steinberg module (and a free resolution of it) in terms of modular symbols.

Let K be a number field with ring of integers $\mathcal{O}$ and let Γ be a subgroup of finite index in $GL_2(\mathcal{O})$. We will assume that K has class number 1 so that $\mathcal{O}$ is a PID. Denote by ν the virtual cohomological dimension of Γ. Applying the formula in Ash [Ash94, p.330], we see that

$$\nu = 2r_1 + 3r_2 - 1,$$

where r_1 is the number of real and $2r_2$ the number of complex embeddings of K.

Let R be a commutative ring with identity such that the torsion in Γ is invertible in R. We define the *Steinberg module* to be the $R[\Gamma]$-module $H^\nu(\Gamma, R[\Gamma])$ and denote it by St. Suppose M is an $R[\Gamma]$-module. Borel-Serre duality [BS73, p.482-483] gives an isomorphism

$$H^\alpha(\Gamma, M) \xrightarrow{\sim} H_{\nu-\alpha}(\Gamma, St \otimes M)$$

for any integer α.

For imaginary quadratic fields K, we have $\nu = 2$. In our case, we want to compute $H^2(\Gamma, V)$ for a Serre weight V, so via Borel-Serre duality, we will instead be computing $H_0(\Gamma, St \otimes V)$. We will need to know how to compute the Steinberg module. Ash gives a description, which we recall here, of the Steinberg module in terms of "universal minimal modular symbols". In [Ash94], Ash defines this space for arbitrary dimension n. Here, we restrict to the case $n = 2$.

The space of universal minimal modular symbols is canonically isomorphic to the

Steinberg module as we have defined it above; from now on we will take the modular symbols description as our definition. Consider the set of formal R-linear sums of symbols $[v] = [v_1, v_2]$ where the v_i are unimodular columns in $\mathcal{O}^2$, i.e., $v_i = [a\ b]^T$ with $\gcd(a, b) = 1$. Mod out by the R-module generated by the following elements:

1. $[v_2, v_1] + [v_1, v_2]$;

2. $[v] = [v_1, v_2]$ whenever $\det(v) = 0$; and

3. $[v_1, v_3] - [v_1, v_2] - [v_2, v_3]$,

where the v_i again run over all unimodular columns in $\mathcal{O}^2$. This quotient module is now our definition of the Steinberg module St. We denote the image of $[v]$ in St by $[v]^*$.

In order to compute the homology of Γ with coefficients in $St \otimes M$, we will first give a free resolution of St

$$\cdots \to S_2 \to S_1 \to S_0 \to St$$

and then tensor with the $R[\Gamma]$-module M

$$\cdots \to S_2 \otimes M \to S_1 \otimes M \to S_0 \otimes M \to St \otimes M.$$

We will then take Γ coinvariants:

$$\cdots \to (S_2 \otimes M)_\Gamma \to (S_1 \otimes M)_\Gamma \to (S_0 \otimes M)_\Gamma \to (St \otimes M)_\Gamma$$

and, finally, take the homology of this chain complex.

The first thing we need is an $R[\Gamma]$-free resolution of St. We now describe the resolution given by Ash in [Ash94], which is based on the resolution in Lee and Szczarba [LS76]. The $R[\Gamma]$-modules S_k of this resolution are described in a manner similar to that of the Steinberg module. Consider the set of formal R-linear sums of symbols $[v] = [v_1, v_2, \cdots, v_{2+k}]$, where each v_i is a unimodular column in $\mathcal{O}^2$. Mod out by the $R[\Gamma]$-module generated by the following elements:

1. $[v_{\sigma(1)}, \ldots, v_{\sigma(2+k)}] - sgn(\sigma)[v_1, \ldots, v_{2+k}]$; and

2. $[v]$ if $v_1, \ldots, v_{2+k}$ are all contained in a hyperplane in K^2.

Here, the v_i again run over all unimodular columns in $\mathcal{O}^2$ and σ runs over all permutations of $\{1, \ldots, 2+k\}$. We take this quotient module to be S_k in our free resolution of St:

$$\cdots \to S_2 \to S_1 \to S_0 \to St$$

and denote the image of $[v]$ in S_k by $[v]$ again.

We define the boundary operator $S_k \to S_{k-1}$ to be

$$\partial[v] = \sum(-1)^i[v_1, \ldots, \hat{v_i}, \ldots, v_{2+k}]$$

and the map $S_0 \to St$ is simply $[v] \mapsto [v]^*$. Ash [Ash94, p.332] notes that the proof that the S_k chain complex is an $R[\Gamma]$-free resolution of St is similar to the proof given in [LS76].

We are interested in computing $H^2(\Gamma, M)$, so (recalling that, for us, $\nu = 2$) we apply the Borel-Serre isomorphism

$$H^2(\Gamma, M) \xrightarrow{\sim} H_0(\Gamma, St \otimes M)$$

to see that we will instead be computing $H_0(\Gamma, St \otimes M)$. Thus we will only be concerned with the following part of the chain complex:

$$S_1 \longrightarrow S_0 \longrightarrow St.$$

We tensor with M and then take coinvariants by Γ to get

$$(S_1 \otimes M)_\Gamma \xrightarrow{\partial} (S_0 \otimes M)_\Gamma \longrightarrow (St \otimes M)_\Gamma.$$

We will compute the homology of degree 0 of this, i.e.,

$$H_0(\Gamma, St \otimes M) = \ker \varepsilon / \mathrm{im} \partial,$$

where

$$(S_1 \otimes M)_\Gamma \xrightarrow{\partial} (S_0 \otimes M)_\Gamma \xrightarrow{\varepsilon} 0.$$

So we will compute

$$(S_0 \otimes M)_\Gamma / \partial((S_1 \otimes M)_\Gamma),$$

which amounts to computing $(S_0 \otimes M)_\Gamma$ modulo the relations $[v_1, v_3] - [v_1, v_2] - [v_2, v_3]$, where the v_i run over all unimodular columns in $\mathcal{O}^2$.

Note that, in our case, for both St and S_0, we are looking at a space of ordered pairs of unimodular columns in $\mathcal{O}^2$, which is the same as paths between cusps ($K \cup \{\infty\}$) in the modular symbols methods of Cremona et al.

5.2 An Algebraic Proposition

The following proposition is analogous to Proposition 4.3 in the doctoral thesis of Martin [Mar01, p.69]. It will be used in Section 5.3 below to relate Manin symbols to modular symbols. First, we will need some notation. For now, let R be a ring and $K = \mathbb{Q}(i)$. Define the following matrices in $\mathrm{GL}_2(\mathcal{O}_K)$:

$$J = \begin{pmatrix} i & 0 \\ 0 & 1 \end{pmatrix} \qquad S = \begin{pmatrix} 0 & i \\ 1 & 0 \end{pmatrix} \qquad T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \qquad T' = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$

Proposition 5.2.1. *Consider the following homomorphism of left $R[GL_2(\mathcal{O}_K)]$-modules*

$$\begin{aligned} \Psi : R[GL_2(\mathcal{O}_K)] &\longrightarrow R[\mathbb{P}^1(K)] \\ \sum_M u_M[M] &\longmapsto \sum_M u_M([M(\infty)] - [M(0)]). \end{aligned}$$

The kernel of Ψ is equal to the left $R[GL_2(\mathcal{O}_K)]$ ideal

$$\mathcal{J} = \langle [I] - [T] - [T'],\ [I] + [S],\ [I] - [J] \rangle.$$

Proof. First, we will show $\mathcal{J} \subseteq \ker(\Psi)$. For this we simply evaluate Ψ on $[I] - [T] - [T']$, on $[I]+[S]$ and on $[I]-[J]$. We have

$$\begin{aligned}\Psi([I]-[T]-[T']) &= [I(\infty)]-[I(0)]-[T(\infty)]+[T(0)]-[T'(\infty)]+[T'(0)]\\ &= [\infty]-[0]-[\infty]+[1]-[1]+[0]\\ &= 0\end{aligned}$$

and

$$\begin{aligned}\Psi([I]+[S]) &= [I(\infty)]-[I(0)]+[S(\infty)]-[S(0)]\\ &= [\infty]-[0]+[0]-[\infty]\\ &= 0\end{aligned}$$

and

$$\begin{aligned}\Psi([I]-[J]) &= [I(\infty)]-[I(0)]-[J(\infty)]+[J(0)]\\ &= [\infty]-[0]-[\infty]+[0]\\ &= 0.\end{aligned}$$

The other direction, proving that $\ker(\Psi) \subseteq \mathcal{J}$, requires more work. Let $W = \sum_M u_M[M]$ be a non-zero element of $\ker(\Psi)$. Let $\mathcal{L}(W) \subseteq \mathbb{P}^1(K)$ be the union of supports of $\sum_M u_M[M(\infty)]$ and $\sum_M u_M[M(0)]$. Furthermore, we define

$$L(W) = \max_{\frac{\alpha}{\beta}\in\mathcal{L}(W)} (|\alpha|^2+|\beta|^2)$$

and

$$m(W) = \left|\left\{\frac{\alpha}{\beta} \in \mathcal{L}(W) : |\alpha|^2+|\beta|^2 = L(W)\right\}\right|$$

where we assume $(\alpha,\beta)=1$. We will use elements of the ideal $\mathcal{J}$ to write down a W' congruent to W modulo $\mathcal{J}$, but such that $L(W') \le L(W)$. Futhermore, if $L(W')=L(W)$ then we will have $m(W') < m(W)$. Iterating this process, we will see that $W \in \mathcal{J}$.

Let $\frac{\alpha}{\beta} \in \mathcal{L}(W)$ be such that $|\alpha|^2+|\beta|^2 = L(W)$. Let δ, γ be elements of $\mathcal{O}_K$ such that $\alpha\gamma-\beta\delta=1$ and such that $|\gamma| \le |\beta|$ and $|\delta| \le |\alpha|$. Then the matrices of

$\mathrm{GL}_2(\mathcal{O}_K)$ satisfying $M(\infty) = \alpha/\beta$ are of the form

$$M = \begin{pmatrix} i^m\alpha & i^n(\delta + k\alpha) \\ i^m\beta & i^n(\gamma + k\beta) \end{pmatrix}$$

for $k \in \mathcal{O}_K$ and $m, n \in \{0, 1, 2, 3\}$. As $L(W) = |\alpha|^2 + |\beta|^2$, we see that for such a matrix M to be in the support of W, we must have

$$|\delta + k\alpha|^2 + |\gamma + k\beta|^2 \leq |\alpha|^2 + |\beta|^2.$$

We will show first that for this to be true, we must have $|k| < 2$. First, suppose $|k| \geq 2$. Then

$$\begin{aligned} |\delta + k\alpha|^2 + |\gamma + k\beta|^2 &\geq (|k\alpha| - |\delta|)^2 + (|k\beta| - |\gamma|)^2 \\ &\geq (2|\alpha| - |\delta|)^2 + (2|\beta| - |\gamma|)^2 \\ &= (|\alpha| + (|\alpha| - |\delta|))^2 + (|\beta| + (|\beta| - |\gamma|))^2 \\ &\geq |\alpha|^2 + |\beta|^2. \end{aligned}$$

Note, furthermore, that equality is only possible if $|\alpha| = |\delta|$ and $|\beta| = |\gamma|$, but this contradicts the fact that $\alpha\gamma - \beta\delta = 1$. Thus we must have $|k| < 2$. Since $k \in \mathcal{O}_K$, the only possibilities are

1. $k = 0$;
2. $k \in \mathcal{O}_K^*$; or
3. $|k|^2 = 2$, i.e., $k \in \{1 + i,\ 1 - i,\ -1 + i,\ -1 - i\}$.

Aside: We show why $|\alpha| = |\delta|$ and $|\beta| = |\gamma|$ implies that M cannot have determinant in $\mathcal{O}_K^*$. We have $\det(M) = i^{m+n}(\alpha\gamma - \beta\delta)$. Under our assumption, we have $|\alpha\gamma| = |\beta\delta|$, so we need to show that we cannot have $x - y \in \mathcal{O}_K^*$ if $|x| = |y|$. Suppose this is the case and let $x = a + bi$ and $y = c + di$, so that $x - y = (a - c) + (b - d)i$. Then either $a = c$ and $b = d \pm 1$ or $b = d$ and $a = c \pm 1$. Without loss of generality, assume $a = c$ and $b = d \pm 1$. Then

$$\begin{aligned} |x|^2 &= |y|^2 \\ \Rightarrow \qquad a^2 + b^2 &= c^2 + d^2 \\ \Rightarrow \qquad (d \pm 1)^2 &= d^2, \end{aligned}$$

giving a contradiction.

Note that the action of J is

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} J = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} i & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} ia & b \\ ic & d \end{pmatrix},$$

so, with (possibly repeated) applications of $I - J$, we may assume the matrix M has the form

$$M = \begin{pmatrix} \alpha & i^n(\delta + k\alpha) \\ \beta & i^n(\gamma + k\beta) \end{pmatrix}.$$

Also, the action of S is given by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} S = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 0 & i \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} b & ia \\ d & ic \end{pmatrix},$$

so, with (possibly repeated) applications of $I - J$ and $I + S$, we may further assume the matrix M has the form

$$M_k = \begin{pmatrix} \alpha & \delta + k\alpha \\ \beta & \gamma + k\beta \end{pmatrix}.$$

Using the same techniques, we may assume that the only matrices N in the support of W such that $N(0) = \alpha/\beta$ are those of the form

$$N_j = \begin{pmatrix} j\alpha - \delta & \alpha \\ j\beta - \gamma & \beta \end{pmatrix},$$

where $|j|^2 \in \{0,\ 1,\ 2\}$ and $|j\alpha - \delta|^2 + |j\beta - \gamma|^2 \leq |\alpha|^2 + |\beta|^2$. Each of the N_j

can be replaced, using S and J, by $-M_{-j}$ as follows. Note that $I + JS \in \mathcal{J}$ since $I + JS = (I - J) + J(I + S)$. Then

$$N_j - N_j(I + JS) = -N_j JS = -M_{-j}.$$

Let W' denote the element $W \in \ker(\Psi)$ with the above modifications. So now all matrices M in the support of W' with $M(\infty) = \alpha/\beta$ are of the form

$$M_k = \begin{pmatrix} \alpha & \delta + k\alpha \\ \beta & \gamma + k\beta \end{pmatrix},$$

with

$$|\delta + k\alpha|^2 + |\gamma + k\beta|^2 \leq |\alpha|^2 + |\beta|^2.$$

Furthermore, we have no matrices N in the support of W' with $N(0) = \alpha/\beta$.

The strategy from here is as follows. We will first consider the case where $|k|^2 = 2$, and we will replace such matrices M by two matrices M' and M'', where M' will have the same form as M above but with $|k| = 1$ and M'' will be such that $M''(\infty) \neq \alpha/\beta \neq M''(0)$. These matrices will also satisfy $m(M) = m(M' - M'')$, so that the number of $\alpha/\beta \in \mathcal{L}(W)$ will not increase. The next step is to work with the case $|k| = 1$. We will replace each M of this sort again with two matrices M' and M''. One of these will be in the form of M_k but with $k = 0$. The other will again be such that $M''(\infty) \neq \alpha/\beta \neq M''(0)$. As in the $|k|^2 = 2$ case, these matrices will satisfy $m(M) = m(M' - M'')$. After these steps, the only matrix M left in W' with $M(\infty) = \alpha/\beta$ is M_0, and there are no matrices left in W' with $M(0) = \alpha/\beta$. Since $W' \in \ker(\Psi)$, we must have the coefficient u_{M_0} of M_0 in W' equal to 0. We thus decrease $m(W')$ by at least one.

To aid in our analysis, we write

$$\begin{aligned}
\alpha &= a_1 + a_2 i \\
\beta &= b_1 + b_2 i \\
\delta &= c_1 + c_2 i \\
\gamma &= d_1 + d_2 i.
\end{aligned}$$

To deal with the case $|k|^2 = 2$, we start by proving the following claim.

Claim 5.2.2. *Suppose $k \in \mathcal{O}_K$ is such that $|k|^2 = 2$, i.e., $k \in \{1+i,\, 1-i,\, -1+i,\, -1-i\}$ and write $k = k_1 + k_2 i$. If*

$$|\delta + k\alpha|^2 + |\gamma + k\beta|^2 \le |\alpha|^2 + |\beta|^2,$$

then either $|\delta + k_1\alpha|^2 + |\gamma + k_1\beta|^2$ or $|\delta + k_2 i\alpha|^2 + |\gamma + k_2 i\beta|^2$ is strictly less than $|\alpha|^2 + |\beta|^2$.

Proof. Consider $k = 1 + i$. Our assumption then becomes

$$\begin{aligned}
&|c_1 + c_2 i + (1+i)(a_1 + a_2 i)|^2 + |d_1 + d_2 i + (1+i)(b_1 + b_2 i)|^2 \\
&\quad = |(a_1 - a_2 + c_1) + (a_1 + a_2 + c_2)i|^2 + |(b_1 - b_2 + d_1) + (b_1 + b_2 + d_2)i|^2 \\
&\quad = 2(a_1^2 + a_2^2) + 2a_1c_1 - 2a_2c_1 + 2a_1c_2 + 2a_2c_2 + c_1^2 + c_2^2 \\
&\qquad\quad + 2(b_1^2 + b_2^2) + 2b_1d_1 - 2b_2d_1 + 2b_1d_2 + 2b_2d_2 + d_1^2 + d_2^2 \\
&\quad \le a_1^2 + a_2^2 + b_1^2 + b_2^2,
\end{aligned}$$

i.e.,

$$\begin{aligned}
&a_1^2 + a_2^2 + 2a_1c_1 - 2a_2c_1 + 2a_1c_2 + 2a_2c_2 + c_1^2 + c_2^2 \\
&\qquad + b_1^2 + b_2^2 + 2b_1d_1 - 2b_2d_1 + 2b_1d_2 + 2b_2d_2 + d_1^2 + d_2^2 \\
&\le 0.
\end{aligned} \tag{5.1}$$

Suppose, by way of contradiction, that the claim is false for $k = 1 + i$. Then we have

$$\begin{aligned}
&|\alpha + \delta|^2 + |\beta + \gamma|^2 \\
&\quad = a_1^2 + a_2^2 + 2a_1c_1 + 2a_2c_2 + c_1^2 + c_2^2 + b_1^2 + b_2^2 + 2b_1d_1 + 2b_2d_2 + d_1^2 + d_2^2 \\
&\quad \geq a_1^2 + a_2^2 + b_1^2 + b_2^2,
\end{aligned}$$

that is,

$$2a_1c_1 + 2a_2c_2 + c_1^2 + c_2^2 + 2b_1d_1 + 2b_2d_2 + d_1^2 + d_2^2 \geq 0. \tag{5.2}$$

We also have

$$\begin{aligned}
&|i\alpha + \delta|^2 + |i\beta + \gamma|^2 \\
&\quad = a_1^2 + a_2^2 - 2a_2c_1 + 2a_1c_2 + c_1^2 + c_2^2 + b_1^2 + b_2^2 - 2b_2d_1 + 2b_1d_2 + d_1^2 + d_2^2 \\
&\quad \geq a_1^2 + a_2^2 + b_1^2 + b_2^2,
\end{aligned}$$

that is,

$$-2a_2c_1 + 2a_1c_2 + c_1^2 + c_2^2 - 2b_2d_1 + 2b_1d_2 + d_1^2 + d_2^2 \geq 0. \tag{5.3}$$

Adding together 5.2 and 5.3, we see that

$$\begin{aligned}
&2a_1c_1 + 2a_2c_2 + c_1^2 + c_2^2 + 2b_1d_1 + 2b_2d_2 + d_1^2 + d_2^2 \\
&\qquad - 2a_2c_1 + 2a_1c_2 + c_1^2 + c_2^2 - 2b_2d_1 + 2b_1d_2 + d_1^2 + d_2^2 \\
&\geq 0,
\end{aligned} \tag{5.4}$$

but, as $|\delta|^2 + |\gamma|^2 \leq |\alpha|^2 + |\beta|^2$, the left hand side of 5.4 is less than or equal to

$$\begin{aligned}
&a_1^2 + a_2^2 + b_1^2 + b_2^2 + 2a_1c_1 + 2a_2c_2 + 2b_1d_1 + 2b_2d_2 \\
&\qquad - 2a_2c_1 + 2a_1c_2 + c_1^2 + c_2^2 - 2b_2d_1 + 2b_1d_2 + d_1^2 + d_2^2,
\end{aligned}$$

i.e.,

$$\begin{aligned}
&a_1^2 + a_2^2 + b_1^2 + b_2^2 + 2a_1c_1 + 2a_2c_2 + 2b_1d_1 + 2b_2d_2 \\
&\qquad - 2a_2c_1 + 2a_1c_2 + c_1^2 + c_2^2 - 2b_2d_1 + 2b_1d_2 + d_1^2 + d_2^2 \\
&\geq 0.
\end{aligned}$$

If we have "strictly greater than" in the above, we get a contradiction with (5.1). Equality requires that $|\delta|^2 + |\gamma|^2 = |\alpha|^2 + |\beta|^2$. Since $|\delta|^2 \leq |\alpha|^2$ and $|\gamma|^2 \leq |\beta|^2$, equality can only happen if $|\delta|^2 = |\alpha|^2$ and $|\gamma|^2 = |\beta|^2$, which contradicts the fact that $\alpha\gamma - \beta\delta = 1$. Thus we must have either $|\alpha+\delta|^2 + |\beta+\gamma|^2$ or $|i\alpha+\delta|^2 + |i\beta+\gamma|^2$ is less than $|\alpha|^2 + |\beta|^2$.

The other cases are treated similarly. $\square$

For the first step, i.e. $|k|^2 = 2$, we can apply Claim 5.2.2 above as follows: Let $t_1 \in \{k_1, k_2 i\}$ be such that $|\delta + t_1\alpha|^2 + |\gamma + t_1\beta| < |\alpha|^2 + |\beta|^2$ and let t_2 be the other element of $\{k_1, k_2 i\}$. Then

$$\begin{pmatrix} t_2\alpha & \delta + t_1\alpha \\ t_2\beta & \gamma + t_1\beta \end{pmatrix} T = \begin{pmatrix} t_2\alpha & \delta + t_1\alpha \\ t_2\beta & \gamma + t_1\beta \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} t_2\alpha & \delta + k\alpha \\ t_2\beta & \gamma + k\beta \end{pmatrix}$$

and

$$\begin{pmatrix} t_2\alpha & \delta + t_1\alpha \\ t_2\beta & \gamma + t_1\beta \end{pmatrix} T' = \begin{pmatrix} t_2\alpha & \delta + t_1\alpha \\ t_2\beta & \gamma + t_1\beta \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} \delta + k\alpha & \delta + t_1\alpha \\ \gamma + k\beta & \gamma + t_1\beta \end{pmatrix}.$$

Since $t_2 = i^m$ for some integer m, we can apply $I - J$ to M until we have

$$M = \begin{pmatrix} t_2\alpha & \delta + k\alpha \\ t_2\beta & \gamma + k\beta \end{pmatrix}.$$

Defining

$$M' = \begin{pmatrix} t_2\alpha & \delta + t_1\alpha \\ t_2\beta & \gamma + t_1\beta \end{pmatrix}$$

and

$$M'' = \begin{pmatrix} \delta + k\alpha & \delta + t_1\alpha \\ \gamma + k\beta & \gamma + t_1\beta \end{pmatrix},$$

we then have

$$\begin{aligned}
M'(I-T-T') &= \begin{pmatrix} t_2\alpha & \delta+t_1\alpha \\ t_2\beta & \gamma+t_1\beta \end{pmatrix}(I-T-T') \\
&= \begin{pmatrix} t_2\alpha & \delta+t_1\alpha \\ t_2\beta & \gamma+t_1\beta \end{pmatrix} - \begin{pmatrix} t_2\alpha & \delta+k\alpha \\ t_2\beta & \gamma+k\beta \end{pmatrix} - \begin{pmatrix} \delta+k\alpha & \delta+t_1\alpha \\ \gamma+k\beta & \gamma+t_1\beta \end{pmatrix} \\
&= M' - M - M'',
\end{aligned}$$

so, modulo $\mathcal{J}$, we may replace M by $M' - M''$. Note that M' can be replaced by

$$M_{k'} = \begin{pmatrix} \alpha & \delta+k'\alpha \\ \beta & \gamma+k'\beta \end{pmatrix},$$

with $|k'|^2 = 1$, a case we will treat shortly. Also, we have $L(M'') \le L(M)$ and $M''(\infty) \ne \alpha/\beta \ne M''(0)$. Recall that when $L(W') = L(W)$, we need $m(W') < m(W)$. In this step, we are replacing one matrix M with two, M' and M'', but since $|\delta+t_1\alpha|^2 + |\gamma+t_1\beta| < |\alpha|^2 + |\beta|^2$, we have $m(M) = m(M' - M'')$. (Note that $M''(\infty) = (\delta+k\alpha)/(\gamma+k\beta)$ was already in $\mathcal{L}(W')$ as $M''(\infty) = M(0)$.) We are not decreasing $m(W)$ in this step, but we are not increasing it either. In later steps we will obtain a decrease in either $L(W')$ or $m(W')$.

So now the only matrices M remaining in the support of W with $M(\infty) = \alpha/\beta$ are those of the form

$$M_k = \begin{pmatrix} \alpha & \delta+k\alpha \\ \beta & \gamma+k\beta \end{pmatrix}, \tag{5.5}$$

where either $k = 0$ or $|k|^2 = 1$ and $|\delta+k\alpha|^2 + |\gamma+k\beta|^2 \le |\alpha|^2 + |\beta|^2$ (by assumption for those starting out with $|k|^2 = 1$ and by design for those coming initially from matrices with $|k|^2 = 2$).

Now we will use elements of $\mathcal{J}$ to eliminate the M_k for $|k| = 1$. In particular, we will use $I - T - T'$. We can first use repeated applications of $I - J$ to replace M_k by

$\tilde{M}_k$ with left hand column given by the transpose of $(-k\alpha \ \ -k\beta)$, i.e.,

$$\tilde{M}_k = \begin{pmatrix} -k\alpha & \delta + k\alpha \\ -k\beta & \gamma + k\beta \end{pmatrix}.$$

Defining

$$M' = \begin{pmatrix} -k\alpha & \delta \\ -k\beta & \gamma \end{pmatrix} \quad \text{and} \quad M'' = \begin{pmatrix} \delta & \delta + k\alpha \\ \gamma & \gamma + k\beta \end{pmatrix},$$

we then have

$$\begin{aligned} \tilde{M}_k(I - T - T') &= \begin{pmatrix} -k\alpha & \delta + k\alpha \\ -k\beta & \gamma + k\beta \end{pmatrix} (I - T - T') \\ &= \begin{pmatrix} -k\alpha & \delta + k\alpha \\ -k\beta & \gamma + k\beta \end{pmatrix} - \begin{pmatrix} -k\alpha & \delta \\ -k\beta & \gamma \end{pmatrix} - \begin{pmatrix} \delta & \delta + k\alpha \\ \gamma & \gamma + k\beta \end{pmatrix} \\ &= \tilde{M}_k - M' - M''. \end{aligned}$$

Thus we can replace $\tilde{M}_k$ by $M' + M''$, where M' can be replaced by M_0 and M'' will satisfy:

1. $M''(\infty) \neq \frac{\alpha}{\beta} \neq M''(0)$ and
2. $L(M'') \leq L(W)$.

Furthermore we have $m(\tilde{M}_k) = m(M' + M'')$. (Note that $M''(0) = (\delta + k\alpha)/(\gamma + k\beta)$ was already in $\mathcal{L}(W')$ as $M''(0) = \tilde{M}_k(0)$.)

Finally the only matrix in the support of W' with either $M(\infty)$ or $M(0)$ equal to α/β is M_0. Thus we must have $u_{M_0} = 0$ and so $m(W')$ is decreased by at least one.

□

5.3 Manin Symbols

Recall that in Section 5.1, we showed that we wish to compute

$$H_0(\Gamma, St \otimes M) = (S_0 \otimes M)_\Gamma / \partial((S_1 \otimes M)_\Gamma),$$

where

$$\partial : (S_1 \otimes M)_\Gamma \longrightarrow (S_0 \otimes M)_\Gamma$$

is the boundary map defined by

$$\partial([v_1, v_2, v_3]) = [v_1, v_3] - [v_1, v_2] - [v_2, v_3].$$

If $M = R$, we are computing the set of formal R-linear sums of symbols $[v] = [v_1, v_2]$, where each v_i is a unimodular column in $\mathcal{O}^2$ modulo the $R[\Gamma]$-module generated by the following elements:

1. $[v_2, v_1] + [v_1, v_2]$;

2. $[v]$ if $\det(v) = 0$;

3. $[v_1, v_3] - [v_1, v_2] - [v_2, v_3]$; and

4. $[v] - \gamma[v]$ for all $\gamma \in \Gamma$,

where the v_i run over all unimodular columns in $\mathcal{O}^2$. We call the $[v] = [v_1, v_2]$ *modular symbols*. Note that if we compute the same thing but without the $[v] - \gamma[v]$ relations, then we are just computing the Steinberg module St.

We will follow the approach of Wiese [Wie05, p.25-29] in using Proposition 5.2.1 from Section 5.2 to relate Manin symbols to modular symbols. Manin symbols provide us with an explicit, computationally friendly description of the homology we wish to compute. Proposition 5.3.1 below gives us the first step in the transition from modular symbols to Manin symbols. We define another matrix:

$$L := \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}.$$

We will also use

$$L^2 = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}.$$

In the following we will use the notation α/β for the unimodular column $[\alpha \;\; \beta]^T$. In particular, we will use 0 to denote $[0 \;\; 1]^T$ and ∞ to denote $[1 \;\; 0]^T$.

Proposition 5.3.1. *The following homomorphism of R-modules is an isomorphism:*

$$\Phi : R[GL_2(\mathcal{O}_K)]/\mathcal{I} \longrightarrow St$$
$$M \longmapsto [M(0), M(\infty)]$$

where

$$\mathcal{I} = R[GL_2(\mathcal{O}_K)](I - J) + R[GL_2(\mathcal{O}_K)](I + S) + R[GL_2(\mathcal{O}_K)](I + L + L^2).$$

Proof. To prove that Φ is surjective, first note that, in the Steinberg module St, we have

$$\begin{aligned}[v_1, v_2] &= [v_1, 0] + [0, v_2] \\ &= -[0, v_1] + [0, v_2],\end{aligned}$$

so it suffices to show $[0, v']$ is in the image of Φ, where v' is any unimodular column in $\mathcal{O}_2$. To see this, we use continued fractions to write down a sum of matrices in $\mathrm{SL}_2(\mathcal{O}_K)$ which, under Φ, will be mapped to $[0, v']$. For this algorithm, we rely on the fact that our fields K are Euclidean.

We use continued fractions to write a given modular symbol of the form $[0, \alpha]$ as a finite sum of symbols of the form $[\gamma(0), \gamma(\infty)]$ with $\gamma \in \mathrm{SL}_2(\mathcal{O}_K)$. We set $r_0 = \alpha$ and $r_n = 1/(r_{n-1} - a_{n-1})$ and define $a_n = \mathrm{floor}(r_n)$. Here we define the floor function on $\mathbb{Q}(i)$ as follows: $\mathrm{floor}(r + si)$ for $r,\ s \in \mathbb{Q}$ is equal to $a + bi$ with a and b the least integers such that $|a - r| \leq 1/2$ and $|b - s| \leq 1/2$.

We then define the convergents of the continued fractions as follows:

$$\begin{aligned} p_{-2} &= 0 & q_{-2} &= 1 \\ p_{-1} &= 1 & q_{-1} &= 0 \\ p_n &= a_n p_{n-1} + p_{n-2} & q_n &= a_n q_{n-1} + q_{n-2} \end{aligned}$$

so that

$$\frac{p_n}{q_n} = a_0 + \cfrac{1}{a_1 + \frac{1}{a_2 + \frac{1}{\cdots + \frac{1}{a_n}}}}$$

and

$$\alpha = \frac{p_k}{q_k}.$$

As in continued fractions for $\mathbb{Z}$, we have

$$p_n q_{n-1} - p_{n-1} q_n = (-1)^{n+1}.$$

We can now rewrite the modular symbol $[0, \alpha]$ as

$$[0, \alpha] = \sum_{n=-1}^{k} \left[\frac{p_{n-1}}{q_{n-1}}, \frac{p_n}{q_n}\right] = \sum_{n=-1}^{k} [\gamma_n(0), \gamma_n(\infty)] = \sum_{n=-1}^{k} \Phi(\gamma_n),$$

where

$$\gamma_n = \begin{pmatrix} (-1)^{n+1} p_n & p_{n-1} \\ (-1)^{n+1} q_n & q_{n-1} \end{pmatrix}.$$

We now show that the kernel of Φ is equal to

$$\mathcal{I} = R[\mathrm{GL}_2(\mathcal{O}_K)](I - J) + R[\mathrm{GL}_2(\mathcal{O}_K)](I + S) + R[\mathrm{GL}_2(\mathcal{O}_K)](I + L + L^2).$$

We start by showing that $\ker(\Phi) = \ker(\Psi)$ where Ψ is the map in Proposition 5.2.1. Define another map π by

$$\pi : St \longrightarrow R[\mathbb{P}^1(K)]$$
$$[v_1, v_2] \longmapsto v_2 - v_1.$$

Then we have $\Psi = \pi \circ \Phi$, so certainly $\ker(\Phi) \subseteq \ker(\Psi)$. To show the other inclusion, suppose $\sum_M u_M M \in \ker(\Psi)$, i.e.,

$$\Psi\left(\sum_M u_M M\right) = \sum_M u_M M(0) - \sum_M u_M M(\infty) = 0.$$

Applying Φ instead of Ψ to this element of $\ker(\Psi)$, we then have

$$\begin{aligned}\Phi\left(\sum_M u_M M\right) &= \sum_M u_M\,[M(0), M(\infty)] \\ &= \sum_M u_M\,[M(0), \infty] + \sum_M u_M\,[\infty, M(\infty)] \\ &= \sum_M u_M\,[M(0), \infty] - \sum_M u_M\,[M(\infty), \infty] \\ &= 0,\end{aligned}$$

and so $\ker(\Psi) \subseteq \ker(\Phi)$.

Finally, we need to show that $\ker(\Phi)$ can be written in the form claimed, i.e., that

$$\ker(\Phi) = R[\mathrm{GL}_2(\mathcal{O}_K)](I - J) + R[\mathrm{GL}_2(\mathcal{O}_K)](I + S) + R[\mathrm{GL}_2(\mathcal{O}_K)](I + L + L^2).$$

Currently, we have that

$$\ker(\Phi) = R[\mathrm{GL}_2(\mathcal{O}_K)](I - J) + R[\mathrm{GL}_2(\mathcal{O}_K)](I + S) + R[\mathrm{GL}_2(\mathcal{O}_K)](I - T - T').$$

First, note that in

$$R[\mathrm{GL}_2(\mathcal{O}_K)](I - J) + R[\mathrm{GL}_2(\mathcal{O}_K)](I + S)$$

we have both $I + \tilde{S}$ and $I - \tilde{J}$ where

$$\tilde{S} = JS = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad \text{and} \quad \tilde{J} = J^2 = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$$

as

$$I + \tilde{S} = (I - J) + J(I + S)$$

and

$$I - \tilde{J} = (I - J) + J(I - J).$$

We then also have $I + \tilde{J}\tilde{S}\tilde{J}$ as

$$I + \tilde{J}\tilde{S}\tilde{J} = (I - \tilde{J}) + \tilde{J}(I + \tilde{S}) - \tilde{J}\tilde{S}(I - \tilde{J}).$$

Now, to see that the two forms of the kernel are the same, we write

$$\begin{aligned}(I - T - T') + T(I + \tilde{S}) + T'(I + \tilde{S}) &= I + T\tilde{S} + T'\tilde{S} \\ &= I + L + L^2\end{aligned}$$

and

$$\begin{aligned}(I + L + L^2) - (L + L^2)(I + \tilde{J}\tilde{S}\tilde{J}) &= I - L\tilde{J}\tilde{S}\tilde{J} - L^2\tilde{J}\tilde{S}\tilde{J} \\ &= I - T - T'.\end{aligned}$$

□

Our discussion thus far is only sufficient for computing weight two modular forms. We now extend this so that we can compute higher weight forms and we also incorporate the Γ relations $[v] - \gamma[v]$.

Let $R = \bar{\mathbb{F}}_\ell$ and let $M = V$ be a Serre weight with left $R[\mathrm{GL}_2(\mathcal{O}_K)]$ action, as defined in Section 3.1. We consider the module ${}_\Gamma(R[\mathrm{GL}_2(\mathcal{O}_K)] \otimes_R M)$, where Γ acts diagonally on the left and we have the natural right $R[\mathrm{GL}_2(\mathcal{O}_K)]$ action, i.e., $(h \otimes v)g = (hg \otimes v)$.

In the following theorem and subsequent proposition we use Proposition 5.3.1 to write the homology group we wish to compute in terms of Manin symbols.

Theorem 5.3.2. *Let N denote the R-module ${}_\Gamma(R[GL_2(\mathcal{O}_K)] \otimes_R M)$ as described above. Then the following sequence of R-modules is exact:*

$$0 \to N(I - J) + N(I + S) + N(I + L + L^2) \to N \to H_0(\Gamma, St \otimes M) \to 0.$$

Proof. Proposition 5.3.1 gives the exact sequence

$$0 \to \mathcal{I} \to R[\mathrm{GL}_2(\mathcal{O}_K)] \to St \to 0$$

where

$$\mathcal{I} = R[\mathrm{GL}_2(\mathcal{O}_K)](I - J) + R[\mathrm{GL}_2(\mathcal{O}_K)](I + S) + R[\mathrm{GL}_2(\mathcal{O}_K)](I + L + L^2).$$

Since M is a free R-module, the following sequence of $R[\Gamma]$-modules is also exact:

$$0 \to N'(I - J) + N'(I + S) + N'(I + L + L^2) \to N' \to St \otimes M \to 0.$$

We then need only take Γ-coinvariants to achieve the desired exact sequence. $\square$

We need one more step to get to the module we will actually be computing. This is the content of the following proposition.

Proposition 5.3.3. *Let X denote the R-module $R[\Gamma\backslash GL_2(\mathcal{O}_K)] \otimes_R M$ with right $GL_2(\mathcal{O}_K)$-action given by $(\Gamma h \otimes v)g = \Gamma hg \otimes g^{-1}v$. Then there is a right $R[GL_2(\mathcal{O}_K)]$-module isomorphism between $N =_\Gamma (R[GL_2(\mathcal{O}_K)] \otimes_R M)$ and X.*

Proof. The isomorphism is simply given by $g \otimes v \mapsto g \otimes g^{-1}v$. $\square$

The R-module $X = R[\Gamma\backslash\mathrm{GL}_2(\mathcal{O}_K)] \otimes_R M$ is the module of Manin symbols and is the basic module we will use in computations. For $\Gamma = \Gamma_0(\mathfrak{n})$, the coset representatives of $\Gamma\backslash\mathrm{GL}_2(\mathcal{O}_K)$ are in one-to-one correspondence with $\mathbb{P}^1(\mathfrak{n})$, the projective line over $\mathcal{O}_K/\mathfrak{n}$. We use the notation $(c : d)$ with $c,\ d \in \mathcal{O}_K$ to denote such a coset representative.

5.4 $\Gamma_1(\mathfrak{n})$ and Characters

The treatment in Section 5.3 is sufficient for dealing with $\Gamma = \Gamma_0(\mathfrak{n})$. We will often want to compute forms for $\Gamma_1(\mathfrak{n})$, both for theoretical and computational reasons. The above method can also be used for the $\Gamma_1(\mathfrak{n})$ case (Figueiredo, in [Fig99], does in fact use this method). However, we will follow the approach used by Wiese [Wie05] for the $\Gamma_1(\mathfrak{n})$ case, as it is computationally advantageous to do so. In this section, we describe this method.

In the $\Gamma_1(\mathfrak{n})$ case, we will use a character

$$\varepsilon : \Gamma_0(\mathfrak{n}) \twoheadrightarrow \Gamma_1(\mathfrak{n})\backslash\Gamma_0(\mathfrak{n}) \xrightarrow{\sim} (\mathcal{O}_K/\mathfrak{n})^* \to \bar{\mathbb{F}}_\ell^*.$$

Remarks 5.4.1.

1. *When the modular form in question is associated to a Galois representation ρ, this character will correspond to the character ε_ρ of that representation.*

2. *We recover the $\Gamma_0(\mathfrak{n})$ case by taking $\Gamma_1(\mathfrak{n})$ with the trivial character.*

We define a slight variation on the weight module M, which takes into account the action of the character ε. This we define as

$$M^\varepsilon = M \otimes_{\bar{\mathbb{F}}_\ell} \bar{\mathbb{F}}_\ell^\varepsilon,$$

where $\bar{\mathbb{F}}_\ell^\varepsilon$ denotes a copy of $\bar{\mathbb{F}}_\ell$ with action of $\Gamma_0(\mathfrak{n})$ by ε^{-1}. In particular, for imaginary quadratic fields K we have

$$M^\varepsilon = \det{}^{a_\tau} \otimes \det{}^{a_{\tau'}} \otimes \mathrm{Sym}^{b_\tau - 1} \otimes \mathrm{Sym}^{b_{\tau'}-1} \otimes \bar{\mathbb{F}}_\ell^\varepsilon.$$

When ℓ splits in K, the embeddings τ and τ' will be the embeddings of $k_\mathfrak{p}$ and $k_{\bar{\mathfrak{p}}}$ in $\bar{\mathbb{F}}_\ell$. When ℓ is inert in K, the embedding τ' will be $\tau \circ \mathrm{Frob}_\ell$.

Computing cohomological   mod ℓ modular forms for $\Gamma_1(\mathfrak{n})$ with character ε then amounts to computing simultaneous eigenvectors for the Hecke operators on

$${}_{\Gamma_1(\mathfrak{n})\backslash\Gamma_0(\mathfrak{n})}\left({}_{\Gamma_1(\mathfrak{n})}\left(R[\mathrm{GL}_2(\mathcal{O}_K)] \otimes M^\varepsilon\right)\right),$$

modulo the relations used in Proposition 5.3.1. Here $\Gamma_1(\mathfrak{n})\backslash\Gamma_0(\mathfrak{n})$ is acting diagonally on the left on ${}_{\Gamma_1(\mathfrak{n})}\left(R[\mathrm{GL}_2(\mathcal{O}_K)] \otimes M \otimes \bar{\mathbb{F}}_\ell^\varepsilon\right)$.

Proposition 5.4.2. *Consider the R-module*

$$X = R[\Gamma_0(\mathfrak{n})\backslash GL_2(\mathcal{O}_K)] \otimes M \otimes \bar{\mathbb{F}}_\ell^\varepsilon,$$

where $GL_2(\mathcal{O}_K)$ acts on the right by $(h \otimes v \otimes r)g = (hg \otimes g^{-1}v \otimes r)$ and $\Gamma_1(\mathfrak{n})\backslash\Gamma_0(\mathfrak{n})$ acts on the left by $g(h \otimes v \otimes r) = (gh \otimes v \otimes \varepsilon(g)r)$. To compute cohomological mod ℓ *modular forms for $\Gamma_1(\mathfrak{n})$ with character ε of the form described above, we can equivalently compute simultaneous eigenvectors for the Hecke operators on the space X modulo the relations used in Proposition 5.3.1.*

Proof. First we apply the isomorphism

$$_{\Gamma_1(\mathfrak{n})\backslash\Gamma_0(\mathfrak{n})}\left(_{\Gamma_1(\mathfrak{n})}\left(R[\mathrm{GL}_2(\mathcal{O}_K)] \otimes M^{\varepsilon}\right)\right) \cong_{\Gamma_0(\mathfrak{n})}\left(R[\mathrm{GL}_2(\mathcal{O}_K)] \otimes M^{\varepsilon}\right).$$

Then we apply the isomorphism of Proposition 5.3.3. □

5.5 Hecke Operators

In this section, we define Hecke operators on the space of modular symbols $H_0(\Gamma, St \otimes M \otimes \bar{\mathbb{F}}_{\ell}^{\varepsilon})$, with $\Gamma = \Gamma_1(\mathfrak{n})$, but also with left coinvariants by $\Gamma_1(\mathfrak{n})\backslash\Gamma_0(\mathfrak{n})$ via the character ε, as described in Section 5.4. (To compute Hecke operators, we convert Manin symbols to modular symbols, compute the action of the Hecke operators there, and then convert back to Manin symbols. We use the results of Section 5.3 to convert back and forth.)

Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$ which is relatively prime to the level $\mathfrak{n}$ and let π be a generator for $\mathfrak{p}$. We define a set $\Delta_{\mathfrak{p}} \subset \mathrm{GL}_2(K)$ by

$$\Delta_{\mathfrak{p}} = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathcal{O}_K) \;:\; ad - bc = \pi, \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} u & * \\ 0 & \pi \end{pmatrix} \mod \mathfrak{n} \right\},$$

where $u \in \mathcal{O}_K^*$. Using the fact that K is Euclidean, one can easily show that

$$\Gamma_1(\mathfrak{n})\Delta_{\mathfrak{p}} = \Delta_{\mathfrak{p}}\Gamma_1(\mathfrak{n}) = \Delta_{\mathfrak{p}}$$

and $\Delta_{\mathfrak{p}}$ can be written as a disjoint union as

$$\Delta_{\mathfrak{p}} = \bigcup_{a,x} \Gamma_1(\mathfrak{n}) \cdot \sigma_a \begin{pmatrix} a & x \\ 0 & \pi/a \end{pmatrix},$$

where $\sigma_a \equiv \begin{pmatrix} 1/a & 0 \\ 0 & a \end{pmatrix}$ mod $\mathfrak{n}$, $a \in \{1, \ \pi\}$, and x runs over representatives of $\mathcal{O}_K/(\pi/a)$. Furthermore, since we take coinvariants via the character action on $\Gamma_1(\mathfrak{n})\backslash\Gamma_0(\mathfrak{n})$ and $\sigma_a \in \Gamma_0(\mathfrak{n})$, we may define the Hecke operator $T_{\mathfrak{p}}$ by

$$\begin{aligned} T_{\mathfrak{p}}\left([v_1, v_2] \otimes P \otimes Q\right) =& \varepsilon(\pi) \begin{pmatrix} \pi & 0 \\ 0 & 1 \end{pmatrix} \left([v_1, v_2] \otimes P \otimes Q\right) \\ &+ \sum_{x \mod \pi} \begin{pmatrix} 1 & x \\ 0 & \pi \end{pmatrix} \left([v_1, v_2] \otimes P \otimes Q\right). \end{aligned}$$

The Hecke operator $T_{\mathfrak{p}}$ is well-defined since $\Gamma_1(\mathfrak{n})\Delta_{\mathfrak{p}} = \Delta_{\mathfrak{p}}\Gamma_1(\mathfrak{n})$. Also, the Hecke operator $T_{\mathfrak{p}}$ is independent of the choice of generator π, since any other generator will be of the form $\epsilon\pi$ for $\epsilon \in \mathcal{O}_K^*$ and then $T_{\epsilon\pi} = JT_\pi$ where $J = \begin{pmatrix} \epsilon & 0 \\ 0 & 1 \end{pmatrix} \in \Gamma_1(\mathfrak{n})$.

Computational Evidence

6.1 Algorithm for Computing Modular Forms

To compute these higher weight mod ℓ modular forms over $\mathbb{Q}(i)$, I wrote a program in C using the PARI library [The05]. In this section, I give an outline of how the program works.

Let $\Gamma = \Gamma_1(\mathfrak{n})$ for some ideal $\mathfrak{n} \subset \mathcal{O}_K$ with character

$$\varepsilon : \Gamma\backslash\Gamma_0(\mathfrak{n}) \xrightarrow{\sim} (\mathcal{O}_K/\mathfrak{n})^* \to \bar{\mathbb{F}}_\ell^*.$$

Let V be a Serre weight for $K = \mathbb{Q}(i)$ and denote by V^ε this same Serre weight but with character action, so we have

$$V^\varepsilon = \det{}^{a_\tau} \otimes \det{}^{a_{\tau'}} \otimes \mathrm{Sym}^{b_\tau - 1} \otimes \mathrm{Sym}^{b_{\tau'} - 1} \otimes \bar{\mathbb{F}}_\ell^\varepsilon.$$

The program computes cohomological mod ℓ modular forms of level $\mathfrak{n}$, character ϵ and weight V. For notational convenience, set $R = \bar{\mathbb{F}}_\ell$. The program executes the following steps.

1. Compile a list of basic Manin symbols. The Manin symbols module, described in Section 5.3 is the R-module

$$X = R[\Gamma_0(\mathfrak{n})\backslash \mathrm{GL}_2(\mathcal{O}_K)] \otimes_R V^\varepsilon.$$

To compute generators for this module, we compute a set of coset representatives $(c : d)$ for $\Gamma_0(\mathfrak{n})\backslash\mathrm{GL}_2(\mathcal{O}_K)$, which is in one-to-one correspondence with $\mathbb{P}^1(\mathfrak{n})$, the projective line over $\mathcal{O}_K/\mathfrak{n}$ (see, e.g., [Byg98, p 29]). Recall that each Sym^b can be viewed as the space of homogeneous polynomials of degree b in two variables with coefficients in R. We can take as a set of generators elements of the form

$$(c:d) \otimes X^m Y^n \otimes Z^r W^s,$$

where $m+n = b_\tau - 1$ and $r+s = b_{\tau'} - 1$. In practice, we only store the coset representatives $(c:d)$ and then use a "column number" to indicate the weight (ordered by the exponent of Y and then the exponent of W).

2. Quotient out the above module by the two and three term relations described in Section 5.3, namely $I-J$, $I+S$ and $I+L+L^2$. For this we create a $3m \times m$ matrix, where m is the number of basic Manin symbols computed in Step 1. For each basic Manin symbol, we have three rows, one for each relation.

We have to be careful with the character action here. For each row, after computing the action of one of the relations on a basic Manin symbol, we have to write the result again in terms of the basic Manin symbols (for the particular coset representatives we chose for $R[\Gamma_0(\mathfrak{n})\backslash \mathrm{GL}_2(\mathcal{O}_K)]$). Here we use the left $\Gamma_1(\mathfrak{n})\backslash\Gamma_0(\mathfrak{n})$ action described in Proposition 5.4.2. For example, if after computing the action of one of these relations, we have some $(c':d') \otimes X^m Y^n \otimes Z^r W^s$ in the result, with $(c':d') = h(c:d)$ for $h \in \Gamma_1(\mathfrak{n})\backslash\Gamma_0(\mathfrak{n})$ and $(c:d) \otimes X^m Y^n \otimes Z^r W^s$ one of our chosen coset representatives, then we write

$$(c':d') \otimes X^m Y^n \otimes Z^r W^s = \varepsilon^{-1}(h)((c:d) \otimes X^m Y^n \otimes Z^r W^s).$$

We then row reduce this matrix to find generators for the space $H_0(\Gamma, St \otimes V)$, as well as linear combinations of these generators for each of the basic Manin symbols.

This matrix can be quite large and the reduction of it presents the biggest bottleneck for the program in terms of speed and memory.

3. Once we have the generators for the space and the linear combinations for the basic Manin symbols, we are ready to compute Hecke operators. We compute each Hecke operator $T_\mathfrak{p}$ as a matrix acting on the generators of the space.

Our method of computing Hecke operators is as follows. Take each generator, of the form

$$(c:d) \otimes X^m Y^n \otimes Z^r W^s$$

and convert it to a *modular symbol*, i.e., an element of the module

$$H_0(\Gamma, St \otimes M \otimes \bar{\mathbb{F}}_\ell^\varepsilon).$$

We convert it by first lifting the coset representative $(c:d)$ to a matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathcal{O}_K)$. (Actually, we can take the lift in $\mathrm{SL}_2(\mathcal{O}_K)$.) We then convert this to a modular symbol by the following map

$$\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix} \otimes X^m Y^n \otimes Z^r W^s\right) \mapsto$$
$$\left(\left[\frac{b}{d}, \frac{a}{c}\right] \otimes (bX - dY)^m(-cX + aY)^n \otimes (\bar{b}Z - \bar{d}W)^r(-\bar{c}Z + \bar{a}W)^s\right)$$

Note that, since the matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ has determinant 1, we do not need to account for the action via the $\det^a$ components of the weight module V.

We then compute the left action of the Hecke operator $T_\mathfrak{p}$ on this modular symbol, resulting in a sum of modular symbols. Using basic relations of the modular symbols, we write each as a sum of the form:

$$\left(\left[\frac{b}{d}, \frac{a}{c}\right] \otimes P(X,Y) \otimes Q(Z,W)\right)$$
$$= \left(\left[0, \frac{a}{c}\right] \otimes P(X,Y) \otimes Q(Z,W)\right) - \left(\left[0, \frac{b}{d}\right] \otimes P(X,Y) \otimes Q(Z,W)\right)$$

We then use the continued fractions method to convert each of these terms to a sum of basic Manin symbols which in turn can be written in terms of the generators. When converting from modular symbols back to Manin symbols, we again have to be careful with the weight action.

The result gives one row of the Hecke operator $T_\mathfrak{p}$. We repeat this process for each generator to get the full matrix for $T_{\mathfrak{p}}$.

6.2 Torsion

Early in section 5.1 we assume that the torsion in Γ is invertible in the commutative ring R. In our case, Γ is a congruence subgroup of $GL_2(\mathcal{O}_K)$ and $R = \bar{\mathbb{F}}_\ell$, though we may think of R as $\mathbb{F}_q$ where q is some power of ℓ. This assumption about torsion is not a strong assumption, since we can make sure that, as long as the level $\mathfrak{n}$ is large enough, the congruence subgroup Γ will be torsion free. In our examples, we have $K = \mathbb{Q}(i)$ and $\Gamma = \Gamma_1(\mathfrak{n})$ for some level $\mathfrak{n}$. Now suppose $A \in GL_2(K) \setminus K^*$ is a torsion element of prime power, i.e., there is some prime p such that $A^p = I$. Now consider $K[A]$. We have

$$K[A] \cong K[x]/(x^2 - Tx + D),$$

where T is the trace of A and D is the determinant of A. Since $A \notin K^*$, we may assume $x^2 - Tx + D$ is irreducible and so $K[A]$ is a field, and a quadratic extension of K. Since A is a p^{th} root of unity, we also have $K[A] \cong K[\zeta_p]$. Then we have a quadratic extension of K of the form $K[\zeta_p]$. Since $K = \mathbb{Q}(i)$, this implies that p is 2 or 3. We will not use $\ell = 2$ for any of our examples (since 2 is ramified in K and hence not covered by the BDJ conjecture), but we do have some examples with $\ell = 3$, so consider $p = 3$. Then in the polynomial above we have $T = -1$ and $D = 1$. The matrix A is in the congruence subgroup $\Gamma_1(\mathfrak{n})$, so we have

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} * & * \\ 0 & 1 \end{pmatrix} \mod \mathfrak{n}.$$

Since the determinant $D = 1$, this implies that $a \equiv 1 \mod \mathfrak{n}$. Then $T = -1$ implies $2 \equiv -1 \mod \mathfrak{n}$, which in turn implies that $\mathfrak{n} \mid 3\mathcal{O}_K$. None of our examples have $\mathfrak{n} \mid 3\mathcal{O}_K$, and so all of our examples satisfy the condition on torsion in Γ.

6.3 Modular Forms Corresponding to Elliptic Curves

In Section 4.1, we determined which elliptic curves over $\mathbb{Q}(i)$ of those in [Cre84] were supersingular and had good reduction at $\ell = 7$. For the representations corresponding to these elliptic curves we know the level (from the conductor of the elliptic curve) and we know that the character will be trivial. We computed the set of predicted weights using the BDJ conjecture. In this section we give tables for each of the levels with, for some small primes $\mathfrak{p}$, the values $a_{\mathfrak{p}}(E)$ associated to the elliptic curve and the systems of eigenvalues $a_{\mathfrak{p}}(f)$ which we found at the predicted levels and weights. Recall that the values $a_{\mathfrak{p}}(E)$ associated to the elliptic curve are given by

$$a_{\mathfrak{p}} = 1 + Nm(\mathfrak{p}) - M_{\mathfrak{p}},$$

where $Nm(\mathfrak{p})$ is the norm of $\mathfrak{p}$ and $M_{\mathfrak{p}}$ is the number of points on the curve E modulo $\mathfrak{p}$ (including the point at infinity).

For each of the four levels tested here, we found the corresponding systems of eigenvalues in all of the predicted weights.

Table 6.1: Elliptic curve, conductor $\mathfrak{n} = 6 + 6i$, considered $\mod 7$

$\mathfrak{p}$	$a_\mathfrak{p}(E)$	$a_\mathfrak{p}(f)$	$\mathfrak{p}$	$a_\mathfrak{p}(E)$	$a_\mathfrak{p}(f)$
$1-2i$	-2	5	$3-8i$	10	3
$1+2i$	-2	5	$3+8i$	10	3
$2-3i$	-2	5	$5-8i$	-6	1
$2+3i$	-2	5	$5+8i$	-6	1
$1-4i$	2	2	$4-9i$	2	2
$1+4i$	2	2	$4+9i$	2	2
$2-5i$	6	6	$1-10i$	-18	3
$2+5i$	6	6	$1+10i$	-18	3
$1-6i$	6	6	$3-10i$	-2	5
$1+6i$	6	6	$3+10i$	-2	5
$4-5i$	-6	1	$7-8i$	18	4
$4+5i$	-6	1	$7+8i$	18	4
$2-7i$	-2	5	11	-6	1
$2+7i$	-2	5	$4-11i$	-6	1
$5-6i$	-2	5	$4+11i$	-6	1
$5+6i$	-2	5			

Table 6.2: Elliptic curve, conductor $\mathfrak{n} = 9 + 7i$, considered $\mod 7$

$\mathfrak{p}$	$a_\mathfrak{p}(E)$	$a_\mathfrak{p}(f)$	$\mathfrak{p}$	$a_\mathfrak{p}(E)$	$a_\mathfrak{p}(f)$
$1+2i$	0	0	$3-8i$	2	2
3	4	4	$3+8i$	2	2
$2-3i$	-4	3	$5-8i$	12	5
$1-4i$	0	0	$5+8i$	-6	1
$1+4i$	-6	1	$4-9i$	8	1
$2-5i$	-6	1	$4+9i$	8	1
$2+5i$	0	0	$1-10i$	-6	1
$1-6i$	2	2	$1+10i$	-18	3
$1+6i$	2	2	$3-10i$	2	2
$4-5i$	-6	1	$3+10i$	2	2
$4+5i$	6	6	$7-8i$	6	6
$2-7i$	6	6	$7+8i$	18	4
$2+7i$	-6	1	11	-4	3
$5-6i$	-10	4	$4-11i$	6	6
$5+6i$	8	1	$4+11i$	-6	1

Table 6.3: Elliptic curve, conductor $\mathfrak{n} = 15$, considered $\mod 7$

$\mathfrak{p}$	$a_\mathfrak{p}(E)$	$a_\mathfrak{p}(f)$	$\mathfrak{p}$	$a_\mathfrak{p}(E)$	$a_\mathfrak{p}(f)$
$1+i$	-1	6	$3-8i$	10	3
$2-3i$	-2	5	$3+8i$	10	3
$2+3i$	-2	5	$5-8i$	-6	1
$1-4i$	2	2	$5+8i$	-6	1
$1+4i$	2	2	$4-9i$	2	2
$2-5i$	-2	5	$4+9i$	2	2
$2+5i$	-2	5	$1-10i$	6	6
$1-6i$	-10	4	$1+10i$	6	6
$1+6i$	-10	4	$3-10i$	14	0
$4-5i$	10	3	$3+10i$	14	0
$4+5i$	10	3	$7-8i$	2	2
$2-7i$	-10	4	$7+8i$	2	2
$2+7i$	-10	4	11	-6	1
$5-6i$	-2	5	$4-11i$	-6	1
$5+6i$	-2	5	$4+11i$	-6	1

Table 6.4: Elliptic curve, conductor $\mathfrak{n} = 19 + 9i$, considered mod 7

$\mathfrak{p}$	$a_\mathfrak{p}(E)$	$a_\mathfrak{p}(f)$	$\mathfrak{p}$	$a_\mathfrak{p}(E)$	$a_\mathfrak{p}(f)$
$1-2i$	3	3	$3-8i$	-16	5
$1+2i$	0	0	$3+8i$	2	2
3	-5	2	$5-8i$	12	5
$2-3i$	5	5	$5+8i$	-15	6
$1+4i$	3	3	$4-9i$	-10	4
$2-5i$	-6	1	$4+9i$	8	1
$2+5i$	0	0	$1-10i$	-15	6
$1-6i$	2	2	$1+10i$	0	0
$1+6i$	-7	0	$3-10i$	2	2
$4-5i$	3	3	$3+10i$	11	4
$4+5i$	-3	4	$7-8i$	-3	4
$2-7i$	-12	2	$7+8i$	0	0
$2+7i$	3	3	11	-4	3
$5-6i$	-1	6	$4-11i$	6	6
$5+6i$	-1	6	$4+11i$	3	3

6.4 Modular Forms Corresponding to Representations from Polynomials

6.4.1 Dihedral Group D_4

In Section 4.2.2 we computed a mod 5 representation ρ with level $\mathfrak{n} = 29$ and quadratic character ε_{29}, which factors through a Galois extension L over $K = \mathbb{Q}(i)$ with $G = \mathrm{Gal}(L/K) \cong D_4$. In the following table we recall the correspondence between orders of elements of G and the traces of the images of those elements under ρ. This representation ρ is a base change from a representation over $\mathbb{Q}$, so we give the traces for both the case where the prime $\mathfrak{p}$ of K splits over $\mathbb{Q}$ and for the case where it is inert over $\mathbb{Q}$.

order	trace (split)	trace (inert)
1	2	2
2	0, 3	2
4	0	3

Note that in the split case there is some ambiguity in the trace for order 2 elements, depending on whether the element is central. For each of those, I computed the restriction of the representation to the decomposition group at that prime to determine whether it should be 0 or 3.

In the following table we list, for some small primes $\mathfrak{p}$, the order of $\mathrm{Frob}_{\mathfrak{p}}$ as discussed above along with the coefficients $a_{\mathfrak{p}}$ of the corresponding system of eigenvalues found. For this example, we found the modular form for two of the four predicted weights. Further investigation is required to understand why the form did not show up as predicted in two of the weights. Table 4.3 in Section 4.2.2 lists the predicted weights along with the level, character and ℓ for each modular form predicted by the conjecture to correspond to ρ.

Table 6.5: Galois group D_4, level $\mathfrak{n} = 29$, considered mod 5

$\mathfrak{p}$	$o(\mathrm{Frob}_{\mathfrak{p}})$	$a_{\mathfrak{p}}$	$\mathfrak{p}$	$o(\mathrm{Frob}_{\mathfrak{p}})$	$a_{\mathfrak{p}}$
$1+i$	4	0	$5-8i$	2	0
3	4	3	$5+8i$	2	0
$2-3i$	2	0	$4-9i$	4	0
$2+3i$	2	0	$4+9i$	4	0
$1-4i$	4	0	$1-10i$	2	0
$1+4i$	4	0	$1+10i$	2	0
$1-6i$	4	0	$3-10i$	1	2
$1+6i$	4	0	$3+10i$	1	2
$4-5i$	2	0	$7-8i$	4	0
$4+5i$	2	0	$7+8i$	4	0
7	2	2	11	2	2
$2-7i$	2	0	$4-11i$	4	0
$2+7i$	2	0	$4+11i$	4	0
$5-6i$	2	0	$7-10i$	1	2
$5+6i$	2	0	$7+10i$	1	2
$3-8i$	4	0			
$3+8i$	4	0			

6.4.2 Alternating Group A_4

In Section 4.2.3 we computed two mod 3 representations, one of level $\mathfrak{n} = 61$ and the other of level $\mathfrak{n} = 79$. Both have trivial character and factor through a Galois extension M over $K = \mathbb{Q}(i)$ with $G = \mathrm{Gal}(M/K) \cong \hat{A}_4$. In the following table we recall the correspondence between orders of elements of G and the traces of the images of those elements under ρ. This representation ρ is a base change from a representation over $\mathbb{Q}$, so we give the traces for both the case where the prime $\mathfrak{p}$ of K splits over $\mathbb{Q}$ and for the case where it is inert over $\mathbb{Q}$.

order	trace (split)	trace (inert)
1	2	2
2	1	2
3	2	2
4	0	1
6	1	2

In the following tables we list, for some small primes $\mathfrak{p}$, the order of $\mathrm{Frob}_\mathfrak{p}$ as discussed above along with the coefficients $a_\mathfrak{p}$ of the corresponding system of eigenvalues found. For both examples, we found the modular form for all the predicted weights. Tables 4.4 and 4.5 in Section 4.2.3 list the predicted weights along with the level, character and ℓ for each modular form predicted by the conjecture to correspond to ρ.

Table 6.6: Galois group A_4, level $\mathfrak{n} = 61$, considered mod 3

$\mathfrak{p}$	$o(\mathrm{Frob}_\mathfrak{p})$	$a_\mathfrak{p}$	$\mathfrak{p}$	$o(\mathrm{Frob}_\mathfrak{p})$	$a_\mathfrak{p}$
$1+i$	4	0	$3-8i$	3	2
$1-2i$	6	1	$3+8i$	3	2
$1+2i$	6	1	$5-8i$	4	0
$2-3i$	6	1	$5+8i$	4	0
$2+3i$	6	1	$4-9i$	3	2
$1-4i$	6	1	$4+9i$	3	2
$1+4i$	6	1	$1-10i$	6	1
$2-5i$	3	2	$1+10i$	6	1
$2+5i$	3	2	$3-10i$	6	1
$1-6i$	4	0	$3+10i$	6	1
$1+6i$	4	0	$7-8i$	4	0
$4-5i$	4	0	$7+8i$	4	0
$4+5i$	4	0	11	4	1
7	3	2	$4-11i$	6	1
$2-7i$	4	0	$4+11i$	6	1
$2+7i$	4	0	$7-10i$	4	0
			$7+10i$	4	0

Table 6.7: Galois group A_4, level $\mathfrak{n} = 79$, considered mod 3

$\mathfrak{p}$	$o(\mathrm{Frob}_\mathfrak{p})$	$a_\mathfrak{p}$	$\mathfrak{p}$	$o(\mathrm{Frob}_\mathfrak{p})$	$a_\mathfrak{p}$
$1+i$	4	0	$3-8i$	3	2
$1-2i$	4	0	$3+8i$	3	2
$1+2i$	4	0	$5-8i$	2	1
$2-3i$	3	2	$5+8i$	2	1
$2+3i$	3	2	$4-9i$	6	1
$1-4i$	4	0	$4+9i$	6	1
$1+4i$	4	0	$1-10i$	3	2
$2-5i$	6	1	$1+10i$	3	2
$2+5i$	6	1	$3-10i$	6	1
$1-6i$	6	1	$3+10i$	6	1
$1+6i$	6	1	$7-8i$	6	1
$4-5i$	3	2	$7+8i$	6	1
$4+5i$	3	2	11	3	2
7	3	2	$4-11i$	6	1
$2-7i$	6	1	$4+11i$	6	1
$2+7i$	6	1	$7-10i$	4	0
$5-6i$	3	2	$7+10i$	4	0
$5+6i$	3	2			

6.5 Modular Forms Corresponding to Representations from CFT

6.5.1 Dihedral Group D_3

For these D_3 examples over $K = \mathbb{Q}(i)$, we compute the values $\mathrm{tr}(\rho(\mathrm{Frob}_{\mathfrak{p}}))$ for each prime $\mathfrak{p}$ by computing the product of

1. the inertia degree of $\mathfrak{p} \subset \mathcal{O}_K$ in the quadratic extension L, and

2. the order of a prime $\mathfrak{P} \subset \mathcal{O}_L$ above $\mathfrak{p}$ in the class group of L.

This product gives us the order of $\mathrm{Frob}_{\mathfrak{p}}$ in the Galois group, which is isomorphic to D_3. We denote this order by $o(\mathrm{Frob}_{\mathfrak{p}})$. Recall that, from the image of ρ in $\mathrm{GL}_2(\bar{\mathbb{F}}_\ell)$, we have the following correspondence between orders of elements and the traces of the images of the elements under ρ:

order	trace
1	2
3	-1
2	0

In the following tables we list, for some small primes $\mathfrak{p}$, the order of $\mathrm{Frob}_{\mathfrak{p}}$ as discussed above along with the coefficients $a_{\mathfrak{p}}$ of the systems of eigenvalues (considered mod 5 and mod 7). There are three tables, one for each of the levels $\mathfrak{n} = 8 + 17i$, $\mathfrak{n} = 13 + 28i$ and $\mathfrak{n} = 8 + 35i$. In all cases, we found the corresponding systems of eigenvalues in all weights predicted for both $\ell = 5$ and for $\ell = 7$. Table 4.6 in Section 4.3.1 lists the predicted weights along with the level, character and ℓ for each modular form predicted by the conjecture to correspond to ρ.

Table 6.8: Galois group D_3, level $\mathfrak{n} = 8 + 17i$, considered mod 5 and mod 7

$\mathfrak{p}$	$o(\mathrm{Frob}_{\mathfrak{p}})$	$a_{\mathfrak{p}}$	$\mathfrak{p}$	$o(\mathrm{Frob}_{\mathfrak{p}})$	$a_{\mathfrak{p}}$
$1+i$	3	-1	$3-8i$	2	0
$1-2i$	2	0	$3+8i$	2	0
$1+2i$	3	-1	$5-8i$	2	0
3	2	0	$5+8i$	1	2
$2-3i$	3	-1	$4-9i$	3	-1
$2+3i$	2	0	$4+9i$	1	2
$1-4i$	3	-1	$1-10i$	3	-1
$1+4i$	3	-1	$1+10i$	2	0
$2-5i$	2	0	$3-10i$	3	-1
$2+5i$	2	0	$3+10i$	3	-1
$1-6i$	3	-1	$7-8i$	2	0
$1+6i$	2	0	$7+8i$	2	0
$4-5i$	2	0	11	3	-1
$4+5i$	2	0	$4-11i$	3	-1
7	2	0	$4+11i$	2	0
$2-7i$	2	0	$7-10i$	2	0
$2+7i$	1	2	$7+10i$	3	-1
$5-6i$	2	0			
$5+6i$	2	0			

Table 6.9: Galois group D_3, level $\mathfrak{n} = 13 + 28i$, considered $\mod 5$ and $\mod 7$

$\mathfrak{p}$	$o(\mathrm{Frob}_{\mathfrak{p}})$	$a_{\mathfrak{p}}$	$\mathfrak{p}$	$o(\mathrm{Frob}_{\mathfrak{p}})$	$a_{\mathfrak{p}}$
$1+i$	3	-1	$3-8i$	2	0
$1-2i$	2	0	$3+8i$	2	0
$1+2i$	3	-1	$5-8i$	2	0
3	2	0	$5+8i$	3	-1
$2-3i$	1	2	$4-9i$	3	-1
$2+3i$	3	-1	$4+9i$	2	0
$1-4i$	2	0	$1-10i$	1	2
$1+4i$	2	0	$1+10i$	2	0
$2-5i$	3	-1	$3-10i$	2	0
$2+5i$	3	-1	$3+10i$	2	0
$1-6i$	3	-1	$7-8i$	2	0
$1+6i$	3	-1	$7+8i$	2	0
$4-5i$	2	0	11	2	0
$4+5i$	2	0	$4-11i$	3	-1
7	3	-1	$4+11i$	2	0
$2-7i$	2	0	$7-10i$	2	0
$2+7i$	2	0	$7+10i$	1	2
$5-6i$	3	-1			
$5+6i$	2	0			

Table 6.10: Galois group D_3, level $\mathfrak{n} = 8 + 35i$, considered mod 5 and mod 7

$\mathfrak{p}$	$o(\mathrm{Frob}_\mathfrak{p})$	$a_\mathfrak{p}$	$\mathfrak{p}$	$o(\mathrm{Frob}_\mathfrak{p})$	$a_\mathfrak{p}$
$1+i$	2	0	$3-8i$	3	-1
$1-2i$	3	-1	$3+8i$	1	2
$1+2i$	3	-1	$5-8i$	2	0
3	2	0	$5+8i$	3	-1
$2-3i$	2	0	$4-9i$	3	-1
$2+3i$	3	-1	$4+9i$	2	0
$1-4i$	3	-1	$1-10i$	1	2
$1+4i$	2	0	$1+10i$	3	-1
$2-5i$	2	0	$3-10i$	2	0
$2+5i$	2	0	$3+10i$	3	-1
$1-6i$	3	-1	$7-8i$	1	2
$1+6i$	2	0	$7+8i$	2	0
$4-5i$	3	-1	11	2	0
$4+5i$	1	2	$4-11i$	2	0
7	3	-1	$4+11i$	2	0
$2-7i$	3	-1	$7-10i$	2	0
$2+7i$	1	2	$7+10i$	3	-1
$5-6i$	2	0			
$5+6i$	3	-1			

6.5.2 Dihedral Group D_5

In Section 4.3.2 we computed a mod 11 representation ρ with level $\mathfrak{n} = 19+20i$ and quadratic character ε_{19+20i}, which factors through a Galois extension L over $K = \mathbb{Q}(i)$ with $G = \mathrm{Gal}(L/K) \cong D_5$. In the following table we recall the correspondence between orders of elements of G and the traces of the images of those elements under ρ.

order	trace
1	2
2	0
5	3, 7

There are actually two representations: wherever one has a 3 or a 7, the other will have the opposite. Both forms, denoted $\{a_\mathfrak{p}\}$ and $\{\tilde{a}_\mathfrak{p}\}$ below, were found for the predicted weights for which we looked. In the following table we list, for some small primes $\mathfrak{p}$, the order of $\mathrm{Frob}_\mathfrak{p}$ as discussed above along with the coefficients $a_\mathfrak{p}$ and $\tilde{a}_\mathfrak{p}$ of the corresponding systems of eigenvalues found. So far we have only checked two of the three predicted weights, but found both forms in each. Table 4.7 in Section 4.3.2 lists the predicted weights along with the level, character and ℓ for each modular form predicted by the conjecture to correspond to ρ.

Table 6.11: Galois group D_5, level $\mathfrak{n} = 19 + 20i$, considered $\mod 11$

$\mathfrak{p}$	$o(\mathrm{Frob}_{\mathfrak{p}})$	$a_{\mathfrak{p}}$	$\tilde{a}_{\mathfrak{p}}$	$\mathfrak{p}$	$o(\mathrm{Frob}_{\mathfrak{p}})$	$a_{\mathfrak{p}}$	$\tilde{a}_{\mathfrak{p}}$
$1+i$	5	7	3	$3-8i$	2	0	0
$1-2i$	5	7	3	$3+8i$	5	7	3
$1+2i$	5	3	7	$5-8i$	2	0	0
3	2	0	0	$5+8i$	2	0	0
$2-3i$	2	0	0	$4-9i$	2	0	0
$2+3i$	5	3	7	$4+9i$	5	3	7
$1-4i$	2	0	0	$1-10i$	5	7	3
$1+4i$	2	0	0	$1+10i$	5	3	7
$2-5i$	2	0	0	$3-10i$	1	2	2
$2+5i$	2	0	0	$3+10i$	2	0	0
$1-6i$	5	7	3	$7-8i$	2	0	0
$1+6i$	5	7	3	$7+8i$	2	0	0
$4-5i$	2	0	0	$4-11i$	5	7	3
$4+5i$	2	0	0	$4+11i$	5	3	7
7	2	0	0	$7-10i$	5	3	7
$2-7i$	2	0	0	$7+10i$	5	3	7
$2+7i$	5	3	7				
$5-6i$	5	7	3				
$5+6i$	2	0	0				

6.6 Final Remarks

In summary, the computational evidence presented here supports the surmise that the BDJ conjectural weight recipe for totally real fields will hold in the case of imaginary quadratic fields as well. For the examples of Galois representations computed here, corresponding modular forms were found in almost all of the predicted weights. There were two exceptions. In one example we did not find the form in all the weights because the computations were too large for the program, so we have not yet looked for all of the predicted weights. In the other exception, we found the form in only two of the four predicted weights. It does look like we may have found a twist of the form in the remaining two weights. Further investigation is required.

The modular symbols computation method used in my program is justified here only for $K = \mathbb{Q}(i)$. I expect it will be straightforward to use the same methodology for all the other Euclidean class number one imaginary quadratic fields. Note, however, that for each field one must justify an algebraic proposition such as the one presented in Section 5.2. We already know the relations we expect to work for each of these fields, namely those relations computed by Cremona, et al. See, for example, [Cre84].

Several students of Cremona (namely Bygott [Byg98], Lingham [Lin05] and Whitley [Whi90]) have extended the modular symbols method (for trivial weights) to imaginary quadratic fields of higher class number. I expect, with some work, that the method presented in this thesis can be joined with their work to compute modular forms with arbitrary weight for imaginary quadratic fields of higher class number.

References

[ADP02] A. Ash, D. Doud, and D. Pollack, *Galois representations with conjectural connections to arithmetic cohomology*, Duke Mathematical Journal **112** (2002), 521–579.

[AS00] A. Ash and W. Sinnott, *An analogue of Serre's conjecture for Galois representations and Hecke eigenclasses in the mod p cohomology of $GL(n, \mathbb{Z})$*, Duke Mathematical Journal **105** (2000), 1–24.

[Ash94] A. Ash, *Unstable cohomology of $SL(n, \mathcal{O})$*, Journal of Algebra **167** (1994), 330–342.

[BCP97] W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system. I. The user language*, Journal of Symbolic Computation **24** (1997), no. 3-4, 235–265.

[BDJ] K. Buzzard, F. Diamond, and F. Jarvis, *On Serre's conjecture for mod ℓ Galois representations over totally real fields*, preprint.

[BS73] A. Borel and J.-P. Serre, *Corners and arithmetic groups*, Commentarii Mathematici Helvetici **48** (1973), 436–491.

[Byg98] J. Bygott, *Modular forms over imaginary quadratic number fields*, Ph.D. thesis, Exeter University, 1998.

[Cre84] J. Cremona, *Hyperbolic tessellations, modular symbols, and elliptic curves over complex quadratic fields*, Compositio Mathematica **51** (1984), 275–323.

[Ş08] M. H. Şengün, *Serre's conjecture over imaginary quadratic fields*, Ph.D. thesis, University of Wisconsin-Madison, 2008.

[DDR] L. Dembélé, F. Diamond, and D. Roberts, *Numerical examples and evidence for Serre's conjecture over totally real fields*, preprint.

[DF$^+$97] M. Daberkow, C. Fieker, et al., *Kant v4*, Journal of Symbolic Computation **24** (1997), 267–283.

[Dia97] F. Diamond, *The refined conjecture of Serre*, Elliptic Curves and Fermat's Last Theorem (J. Coates and S.-T. Yau, eds.), International Press, Hong Kong, 1997, 2nd. ed., pp. 172–186.

[Fig95] L. M. Figueiredo, *Serre's conjecture over imaginary quadratic fields*, Ph.D. thesis, University of Cambridge, 1995.

[Fig99] ———, *Serre's conjecture for imaginary quadratic fields*, Compositio Mathematica **118** (1999), 103–122.

[Gee] T. Gee, *On the weights of mod p Hilbert modular forms*, preprint.

[Gee07] ———, *Companion forms over totally real fields II*, Duke Mathematical Journal **136** (2007), 275284.

[Her] F. Herzig, *The weight in a Serre-type conjecture for tame n-dimensional Galois representations*, preprint.

[Jan96] G. Janusz, *Algebraic number fields*, 2 ed., Graduate Studies in Mathematics, vol. 7, American Mathematical Society, USA, 1996.

[KM] J. Klüners and G. Malle, *A database for number fields*, available from http://www.math.uni-duesseldorf.de/ klueners/minimum/minimum.html.

[KWa] C. Khare and J.-P. Wintenberger, *Serre's modularity conjecture (I)*, preprint.

[KWb] ———, *Serre's modularity conjecture (II)*, preprint.

[Lin05] M. Lingham, *Modular forms and elliptic curves over imaginary quadratic fields*, Ph.D. thesis, University of Nottingham, 2005.

[LS76] R. Lee and R. H. Szczarba, *On the homology and cohomology of congruence subgroups*, Inventiones Mathematicae **33** (1976), no. 1, 15–53.

[Mar01] F. Martin, *Périodes de formes modulaires de poids 1*, Ph.D. thesis, Université Paris 7, 2001.

[Mil08] J. S. Milne, *Algebraic number theory*, 2008, Version 3.00, available from http://www.jmilne.org/math/CourseNotes/ANT.pdf.

[Sch] M. Schein, *Weights in Serre's conjecture for Hilbert modular forms: the ramified case*, preprint.

[Ser77] J.-P. Serre, *Linear representations of finite groups*, Graduate Texts in Mathematics, vol. 42, Springer, New York, 1977.

[Ser87] ———, *Sur les représentations modulaires de degré 2 de Gal*$(\bar{\mathbb{Q}}/\mathbb{Q})$, Duke Mathematical Journal **54** (1987), 179–230.

[Sil86] J. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 106, Springer-Verlag, New York, 1986.

[Ste] W. Stein, *Sage mathematical software system*, available from http://modular.math.washington.edu/sage/doc/reference/.

[The05] The PARI Group, Bordeaux, *PARI/GP, version* 2.3.1, 2005, available from http://pari.math.u-bordeaux.fr/.

[Whi90] E. Whitley, *Modular forms and elliptic curves over imaginary quadratic fields*, Ph.D. thesis, Exeter University, 1990.

[Wie05] G. Wiese, *Modular forms of weight one over finite fields*, Ph.D. thesis, Universiteit Leiden, 2005.