Modular Elliptic Curves over Quartic CM Fields

Andrew James Jones

School of Mathematics and Statistics

Submitted for the degree of Doctor of Philosophy (Mathematics)
at the University of Sheffield

October 2014

Acknowledgements

I would like to express my gratitude to my supervisor, Dr. Tobias Berger, whose knowledge, expertise and support have proved invaluable throughout the course of my doctorate, and without whose careful guidance I would not be even half the mathematician I am today.

I thank the EPSRC and the University of Sheffield, for providing the financial and administrative support to allow me to perform my research, and to the staff in the School of Mathematics and Statistics for creating a most wonderful atmosphere in which to study mathematics. I am particularly in debt to Dr. Jayanta Manoharmayum, for introducing me to modular forms, and to Mr. David Robson, whose excellent I.T. support was key to my computations.

While countless people have had a hand in this thesis, whether directly or indirectly, I would like to extend special thanks to Drs. Paul Gunnells and Dan Yasaki, for some enlightening conversations in Greensboro, North Carolina; to Professor John Cremona and Dr. Neil Dummigan, whose insightful comments helped to improve this piece of work; to Alexander Rahm, for his generous offer of assistance with my computations; and to Daniel Fretwell and David O'Sullivan, for the countless enjoyable hours spent discussing mathematics over lunch.

Last, but by no means least, I would like to thank my family for their love, patience and understanding. In particular I thank my parents, Trefor and Christine, for making me the man I am today; my brother, Philip, for always watching out for me; and most of all my wife Jessica, whose unwavering love and faith has kept me going, and without whom I would be lost.

Contents

Chapter 1

Introduction

First conjectured in the late 1950s, the *Taniyama-Shimura Conjecture* (now the *Modularity Theorem*) posited a connection between rational elliptic curves and classical modular forms. The combined efforts of Breuil, Conrad, Diamond, Taylor and Wiles at the turn of the 21^{st} century confirmed this connection, by proving that the Galois representation attached to a rational elliptic curve is equivalent to a representation attached to a rational weight 2 Hecke eigenform.

Viewed within the framework of the Langlands program, this is one of many conjectured results linking Galois representations to automorphic forms and representations of reductive algebraic groups, and as such readily lends itself to generalisation. Indeed, it is well-known that classical modular forms correspond to automorphic forms for $\mathrm{GL}_2(\mathbb{Q})$ (exploiting the fact that the complex upper half-plane $\mathfrak{h}$ is the globally symmetric space for the $\mathbb{Q}$-group GL_2) and so, even restricting our attention to general linear groups, there are two clear paths to choose from: we can change the dimension, or we can change the base field.

Both approaches have their merits, but, in keeping with the spirit of the Taniyama-Shimura Conjecture, the focus of this thesis is the latter case, which allows one to consider the modularity of elliptic curves defined over a number field. The question of modularity has already been extensively studied for both totally real and imaginary quadratic fields. In the former case, work by Kisin and Taylor shows that all elliptic curves over totally real fields are *potentially modular*, in the sense that any such curve becomes modular over some totally real field extension (and it has recently been shown by Freitas, Hung and Siksek that any elliptic curve defined over a real quadratic field is truly modular). Modular forms over imaginary quadratic fields have been studied in great depth computationally, with a substantial body of work produced by Cremona and a number of his students.

As such, we consider perhaps the next logical case: that of a quartic CM field (a totally imaginary quartic field which is a quadratic extension of a real quadratic field). This is inspired by a recent result due to C.P. Mok, which shows how one can attach Galois representations to automorphic forms defined over such fields (two recent papers; one by Harris, Lan, Taylor and Thorne, and another by Scholze, study this question in greater generality, but Mok's result suffices for forms that we expect to correspond to elliptic curves). The representations are in fact attached to classes in the group cohomology $H^*(\Gamma, \mathbb{C})$, where Γ is an arithmetic subgroup of the $\mathbb{Q}$-group $G = \mathrm{Res}_{F/\mathbb{Q}}(\mathrm{GL}_2)$ (here F denotes our CM field). By a generalization of the Eichler-Shimura isomorphism, it is known that certain automorphic forms for G can be realized as such cohomology classes, and moreover that the Hecke action translates to this new setting.

The Galois representations thus obtained satisfy certain local-to-global compatibility conditions. Indeed, let $\rho : \mathrm{Gal}(\overline{F}/F) \to \mathrm{GL}_2(\overline{\mathbb{Q}}_\ell)$ denote the representation attached to the automorphic representation $\pi = \otimes_v \pi_v$, where v runs through the places of F. Then, for each finite place v at which π_v is unramified, the representation ρ_v obtained by restriction to the local absolute Galois group $\mathrm{Gal}(\overline{F}_v/F_v)$, and the local component π_v are connected as described by the local Langlands correspondence for GL_2. In particular, the characteristic polynomial of ρ on a Frobenius element at such places is described by the Langlands class of π_v, which can be determined through knowledge of the Hecke action on those vectors which are fixed by certain compact subgroups of $G(\mathbb{A})$ under the action of π.

We therefore follow in the footsteps of Cremona et al by working with automorphic forms computationally, in a setting that allows us to compute the Hecke action. As is standard in the field, rather than work with the forms directly, we exploit the connection between automorphic forms and group cohomology, which is more amenable to computation. Given an arithmetic subgroup Γ of the $\mathbb{Q}$-group G, we identify $H^*(\Gamma, \mathbb{C})$ with the cohomology of the *locally symmetric space* $X_\Gamma := \Gamma\backslash G(\mathbb{R})/A_G^0(\mathbb{R})K_\infty$, where K_∞ denotes a maximal compact subgroup of $G(\mathbb{R})$, and $A_G^0(\mathbb{R})$ the *split component* lying in the centre of G (these are the analogues of the modular curves of classical theory).

The *globally symmetric space* $X := G(\mathbb{R})/A_G^0(\mathbb{R})K_\infty$ can be identified with the space of binary Hermitian forms over our field F. Work by Voronoï, which was later generalized by Koecher, shows that such spaces admit a decomposition into convex polytopes which is stable under the action of any arithmetic subgroup of G, and that, moreover, there are only finitely many equivalence classes of polytopes under this Γ-action. We can therefore compute the cohomology of X_Γ by working with a *finite* polytopic cell complex, known as the *Koecher complex*.

To compute the Hecke action, however, we need a new approach. While the spaces X_Γ *are* acted on by Hecke operators, the cells in the corresponding complex are not preserved, making computation impossible. We therefore follow the approach of Gunnells in his paper **[Gun99]**, which is expanded upon in the papers **[AGM02]**, **[GY08]**, **[GHY13]** and **[GY13]**, by looking at a larger combinatorial cell complex $\mathscr{S}$, known as the *sharbly complex*, whose Γ-equivariant homology is known to compute the group cohomology $H^*(\Gamma, \mathbb{C})$, and which also admits a Hecke action. In these papers, the authors describe how one can construct a finite subcomplex of $\mathscr{S}$ using cells of the Koecher complex, which moreover computes the homology of the whole complex.

The Hecke action on $\mathscr{S}$ does *not* preserve this subcomplex, but the authors describe a theoretical algorithm which, given a homology class in $H_*^\Gamma(\mathscr{S})$, produces an equivalent class whose support lies wholly in this subcomplex. In particular, they show how to implement this algorithm practically for certain number fields, including a quartic CM field, giving us a means for computing the Hecke action for such fields.

The paper **[GHY13]** describes this procedure for the quartic CM field $\mathbb{Q}(\zeta_5)$, where ζ_5 denotes a fifth root of unity. In particular, they consider arithmetic subgroups of the form $\Gamma_0(\mathfrak{n})$ comprising matrices whose lower left entry vanishes modulo some ideal $\mathfrak{n}$, and compute the action of several Hecke operators on such forms for a large range of levels $\mathfrak{n}$. I transfer this approach to three different quartic CM fields of small discriminant (the fields $\mathbb{Q}(\zeta_8)$ and $\mathbb{Q}(\zeta_{12})$ of eighth and twelfth roots of unity, and the field generated by the roots of the quartic polynomial $x^4-x^3+2x^2+x+1$), finding examples of rational Hecke eigenclasses, and computing the Hecke action on them, using my own adaptation of the authors' algorithm in MAGMA. I also study the symmetric spaces X for such fields, identifying certain phenomena which were not apparent in **[GHY13]**, as well as providing data for the polytopic decomposition of Koecher for such spaces.

Having computed the action of the Hecke operators on the group cohomology $H^*(\Gamma_0(\mathfrak{n}), \mathbb{C})$, Gunnells et al seek to pair the corresponding eigenclasses with elliptic curves over the field F. In my analysis I do the same, but seek to go one step further and *prove* the Galois representation attached to an elliptic curve is equivalent to that of the corresponding automorphic form.

To prove equivalence of the two Galois representations, I adapt an idea presented in **[DGP10]**, in which the authors use the Faltings-Serre-Livnè method to prove modularity of elliptic curves over imaginary quadratic fields. I show that these methods extend to CM fields, using the Galois representations established by Mok's result. I have implemented my own version of the algorithm described in **[DGP10]** using PARI, which, given an elliptic curve, provides a *finite* list of primes of the quartic field F. If $[\phi]$ is a Hecke eigenclass whose eigenvalues equate to the local data of our chosen elliptic curve at each such prime, then the associated Galois representations are provably equivalent.

Using this algorithm, it is possible to prove modularity of all but one of the elliptic curves over F that have appeared during my previous analysis. For each such curve, I compute the required Hecke eigenvalues and establish modularity of the curves. In practice, the number of Hecke eigenvalues to compute varies depending on the residual image of the 2-adic Galois representations - if the residual image is degenerate, a significant number of eigenvalues must be computed - and so I also discuss some of the practical issues which arise during the course of our computations.

Chapter 2

Classical Theory

We begin with a discussion of the classical theory behind the Modularity Theorem for rational elliptic curves, which lays the groundwork for our study.

In **Section 2.1**, we discuss classical modular forms, and discuss some of their properties. This is followed by a discussion of the action of Hecke operators on spaces of modular forms in **Section 2.2**. Such Hecke actions will be a recurring theme throughout our discussion, as one can define these actions on a variety of objects, several of which we shall see in time.

Section 2.3 discusses rational elliptic curves, and gives the simplest statement of modularity - an equivalence between the local data of an elliptic curve and the eigenvalues of a certain cusp form under the action of the Hecke operators. **Section 2.4** follows this up with a second statement of modularity, which states a correspondence between representations of the absolute Galois group of the rationals attached to both elliptic curves and modular forms.

In **Section 2.5**, we discuss L-functions, which are complex analytic functions that we can attach to a variety of objects. In particular, we can attach them to elliptic curves, modular forms and Galois representations, and can once again rephrase modularity in terms of equality of the corresponding L-functions. Finally, in **Section 2.6** we provide an alternative realization of modular forms as certain cohomology classes, an idea which will be exploited later in our study.

2.1 Classical Modular Forms

Modular forms can loosely be described as complex-valued functions which satisfy a number of functional equations, derived from an action of a finite-index subgroup of the *modular group* $\mathrm{SL}(\mathbb{Z})$. More precisely, for a positive integer N, define the group

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

(we call $\Gamma_0(N)$ a *congruence subgroup* of level N). Fix a positive integer k, let $f : \mathfrak{h} \to \mathbb{C}$ be holomorphic (where $\mathfrak{h}$ denotes the complex upper half-plane), and let $\gamma \in \mathrm{SL}_2(\mathbb{Z})$. We denote by $f|_\gamma$ the function

$$f|_\gamma(z) = (cz + d)^{-k} f(\gamma z),$$

where $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ and $\mathrm{SL}_2(\mathbb{Z})$ acts on $\mathfrak{h}$ via fractional linear transformations. For future reference, we note that the action of $\mathrm{SL}_2(\mathbb{Z})$ on $\mathfrak{h}$ extends naturally to an action of the group $\mathrm{GL}_2^+(\mathbb{R})$ of 2×2 real matrices with positive determinant, and that we can similarly define the function $f|_\gamma$ for $\gamma \in \mathrm{GL}_2^+(\mathbb{R})$ by

$$f|_\gamma(z) = \det(\gamma)^{\frac{k}{2}} (cz + d)^{-k} f(\gamma z).$$

We define a *modular form of weight k and level N* to be a function f as above which satisfies the functional equation

$$f|_\gamma = f \text{ for all } \gamma \in \Gamma_0(N),$$

and which is *holomorphic at the cusps* of $\mathfrak{h}$.

We explain this last notion by considering the *open* and *closed modular curves* $Y_0(N) = \Gamma_0(N)\backslash\mathfrak{h}$ and $X_0(N) = \Gamma_0(N)\backslash\mathfrak{h}^*$, where we obtain $\mathfrak{h}^*$ by adjoining the *cusps* $\mathbb{P}^1(\mathbb{Q})$ to $\mathfrak{h}$. These are Riemann surfaces, and any holomorphic function $f : \mathfrak{h} \to \mathbb{C}$ extends to a meromorphic function in the local coordinate systems around each cusp. If in fact f extends to a holomorphic function at every cusp, then we say that f is *holomorphic at the cusps*. If, moreover, f vanishes at every cusp, we call f a *cusp form*.

We denote by $\mathcal{M}_k(N)$ and $\mathcal{S}_k(N)$ the spaces of modular (respectively cusp) forms of weight k and level N. As the name suggests, these are complex vector spaces, and are in fact finite-dimensional.

We will later want to consider modular forms that are *twisted* by the action of some character. To this end, let ψ denote a Dirichlet character modulo N, and denote by $\mathcal{M}_k(N, \psi)$ and $\mathcal{S}_k(N, \psi)$ the spaces of functions satisfying the functional equations

$$f|_\gamma = \psi(d) f$$

for all $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(N)$, and which possess all the other properties required of modular forms and cusp forms respectively.

One can define an inner-product on the space of cusp forms, the *Petersson inner product*

$$\langle\ ,\ \rangle : \mathcal{S}_k(N) \times \mathcal{S}_k(N) \to \mathbb{C}.$$

While this does not extend to a function $\mathcal{M}_k(N) \times \mathcal{M}_k(N) \to \mathbb{C}$, it does extend partially to allow us to take the inner product of a cusp form with an arbitrary modular form. Under this understanding, the space of modular forms admits a decomposition

$$\mathcal{M}_k(N) = \mathrm{Eis}_k(N) \oplus \mathcal{S}_k(N),$$

where the space $\mathrm{Eis}_k(N)$ of *Eisenstein series* is the "orthogonal complement" of $\mathcal{S}_k(N)$ in $\mathcal{M}_k(N)$.

Note that not all cusp forms of level N are unique to that level. In particular, if M is a divisor of N, then (since $\Gamma_0(N) \subseteq \Gamma_0(M)$), it is clear that any cusp form of level M is also a cusp form of level N. In addition, if d is a divisor of $\frac{N}{M}$, we can *raise the level* of an element f of $\mathcal{S}_k(M)$ by considering the function g defined by

$$g(z) = d^{k-1} f(dz).$$

We define the space of *newforms*, $\mathcal{S}_k(N)^{\mathrm{new}}$ to be the orthogonal complement in $\mathcal{S}_k(N)$ under the Petersson inner product of the space of forms arising from lower levels in this manner.

2.2 Hecke Operators

A common idea throughout our study of modular forms (and their generalizations) is that of a *Hecke correspondence*. In the classical situation, such correspondences are manifested through certain operators on spaces of modular forms, which we refer to as *Hecke operators*. Since these correspondences are central to our study, we shall spend some time discussing them now.

Let Γ denote a subgroup of $\mathrm{SL}_2(\mathbb{Z})$ of finite index (typically we shall consider the congruence subgroup $\Gamma_0(N)$) and let $g \in \mathrm{GL}_2^+(\mathbb{R})$ satisfy the condition that the subgroups $\Gamma_1 := \Gamma \cap g^{-1}\Gamma g$ and $\Gamma_2 := \Gamma \cap g\Gamma g^{-1}$ have finite index in Γ. One can relate the groups Γ, Γ_1 and Γ_2 by the following diagram:

$$\begin{array}{ccc} \Gamma_1 & \xrightarrow{\alpha_g} & \Gamma_2 \\ {\scriptstyle \iota_1}\downarrow & & \downarrow{\scriptstyle \iota_2} \\ \Gamma & & \Gamma \end{array}$$

where ι_i denotes the inclusion $\Gamma_i \hookrightarrow \Gamma$, and α_g is the homomorphism

$$\Gamma_1 \to \Gamma_2, \gamma \mapsto g\gamma g^{-1}.$$

Then, denoting by $X(\Gamma)$ the modular curve $\Gamma\backslash\mathfrak{h}$, one can define relations between the modular curves associated to the above groups by the diagram:

$$\begin{array}{ccc} X(\Gamma_1) & \xrightarrow{\widetilde{\alpha_g}} & X(\Gamma_2) \\ {\scriptstyle \pi_1}\downarrow & & \downarrow{\scriptstyle \pi_2} \\ X(\Gamma) & & X(\Gamma) \end{array}$$

where π_i denotes the projection map from $X(\Gamma_i)$ to $X(\Gamma)$ and $\widetilde{\alpha_g}$ the diffeomorphism from $X(\Gamma_1)$ to $X(\Gamma_2)$ induced by the map α_g, sending the orbit $\Gamma_1 x$ to the orbit $\Gamma_2 g x$.

The composition $\pi_2 \circ \widetilde{\alpha_g} \circ \pi_1^{-1}$ is our *Hecke correspondence*. This can be thought of as a multi-valued function on $X(\Gamma)$, and we can in fact provide an explicit description of this function. First, given a set $\{\gamma_i\}$ of coset representatives for the space $\Gamma_1\backslash\Gamma$, an orbit Γx is mapped to the set of preimages $\{\Gamma_1\gamma_i x\}$ via π_1^{-1}. This is subsequently mapped to the set $\{\Gamma_2 g\gamma_i x\}$ via $\widetilde{\alpha_g}$, which is finally sent to the set $\{\Gamma g\gamma_i x\}$ via the projection π_2.

For calculation purposes, we make note of the following fact (see, for example, **[DS05], Lemma 5.1.2**):

Lemma 2.2.1. *There is a natural bijection between the coset space* $\Gamma_1\backslash\Gamma$ *and the orbit space* $\Gamma\backslash\Gamma g\Gamma$ *induced by left multiplication:*

$$\Gamma \mapsto \Gamma g\Gamma, \gamma \mapsto g\gamma.$$

In particular, $\{\gamma_i\}$ *is a set of coset representatives for* $\Gamma_1\backslash\Gamma$ *if, and only if,* $\{g\gamma_i\}$ *is a set of orbit representatives for* $\Gamma g\Gamma$*.*

Thus the Hecke correspondence can be viewed as a multi-valued function

$$\Gamma x \mapsto \{\Gamma g_i x\},$$

where $\{g_i\}$ is a set of representatives of the orbit space $\Gamma\backslash\Gamma g\Gamma$ (one can easily check that this function is well-defined).

Our interest in Hecke correspondences lies in the fact that such correspondences give rise to operators on spaces of modular forms, which we refer to as *Hecke operators*. In particular, suppose we set $\Gamma = \Gamma_0(N)$ and, for a prime p not dividing N, we set $g = \left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right)$. Then, from the resulting Hecke correspondence, we obtain a Hecke operator, which we denote by T_p, which acts on the spaces $\mathcal{M}_k(N)$ and $\mathcal{S}_k(N)$ via:

$$T_p(f) = \sum_{i=1}^{p+1} f|_{g_i},$$

where $f|_{g_i}$ is as defined in the previous section, and

$$\Gamma_0(N)\left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right)\Gamma_0(N) = \coprod_{i=1}^{p+1} \Gamma_0(N) g_i.$$

One can check that the operators T_p and T_q commute for distinct primes p and q. A standard choice of representatives g_i is given by the set

$$\left\{\left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 1 \\ 0 & p \end{smallmatrix}\right), \ldots, \left(\begin{smallmatrix} 1 & p-1 \\ 0 & p \end{smallmatrix}\right), \left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right)\right\}.$$

Recall from the previous section that we have a decomposition

$$\mathcal{M}_k(N) = \mathrm{Eis}_k(N) \oplus \mathrm{S}_k(N).$$

Since the Hecke operator T_p preserves both $\mathcal{M}_k(N)$ and $\mathcal{S}_k(N)$, it also preserves the space $\mathrm{Eis}_k(N)$ of Eisenstein series. In fact, one can show (see, for example, **[DS05], Proposition 5.2.3**) that there exists a basis of Eisenstein series, each of which is a simultaneous eigenform for the operators T_p.

Eisenstein series are not the only eigenforms for the Hecke operators. Indeed, it is known (see, for example, **[DS05], Theorem 5.8.2**) that one can exhibit a basis of the space $\mathcal{S}_k(N)$ of newforms of level N which consists entirely of cusp forms that are simultaneous eigenforms for the Hecke operators T_p, with p not dividing N. Given such an eigenform f, we write $a_p(f)$ for the eigenvalue of f with respect to the operator T_p.

2.3 Elliptic Curves and Modularity

Modular forms play a key role in Wiles' proof of Fermat's Last Theorem, and as such they (and their more recent generalizations) are of great interest to modern-day number theorists. Their importance lies in the Taniyama-Shimura conjecture (now often referred to as the Modularity Theorem), which states that all rational elliptic curves are *modular* (which we shall expand upon soon, but for now it suffices to understand that modularity implies some connection to modular forms). The idea behind the proof of Fermat's Last Theorem is that a non-trivial solution to the Fermat equation

$$a^n + b^n = c^n,\ a, b, c \in \mathbb{Z},\ n \geq 3$$

can be used to construct an elliptic curve which is not modular, and the Modularity Theorem then tells us that no such solution can exist.

We shall now expand on some of these concepts, beginning with the notion of an *elliptic curve*. The standard definition is that an elliptic curve E is a non-singular projective algebraic curve of genus one, together with a distinguised point $\mathcal{O}_E$, often referred to as the *point at infinity*. For our purposes, it is enough to think of an elliptic curve defined over the rationals to be the set of solutions (over an algebraic closure $\overline{\mathbb{Q}}$ of the rationals) of a *Weierstrass equation*,

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,\ a_i \in \mathbb{Q},$$

together with the point at infinity $\mathcal{O}_E$. The requirement that E be non-singular simply means that the curve has a well-defined tangent at each point.

Elliptic curves are interesting objects in their own right; for example, one can define an abelian group structure on the set of points on an elliptic curve, in which the point at infinity becomes the identity element. Since our interest is to establish a link between such curves and modular forms, we shall concentrate on the properties that are directly related to the topic at hand.

We say that two elliptic curves E_1 and E_2 are *isogenous* if there exists a surjective rational map $\varphi : E_1 \to E_2$ such that $\varphi(\mathcal{O}_{E_1}) = \varphi(\mathcal{O}_{E_2})$, and which preserves the group structure on the curves. Such a map necessarily has finite kernel, and if an isogeny with trivial kernel exists between E_1 and E_2 then we say that they are *isomorphic*. It is known that every elliptic curve over the rationals is isomorphic to one defined by a Weierstrass equation of the above form, all of whose coefficients are integral. Moreover, each isomorphism class of curves contains an integral Weierstrass model whose discriminant is minimal among all such models (see, for example, **[Sil09], Corollary 8.3**); henceforth, we shall assume without loss of generality that any rational elliptic curve is defined by such an equation.

Given a prime p, it makes sense to define the *reduction* of the curve E at p – it is simply the set of solutions over the finite field $\mathbb{F}_p$ to the Weierstrass equation obtained by reducing the coefficients a_i modulo p (together with the point at infinity). For all but finitely many primes p, this reduction in fact defines an elliptic curve over the field $\mathbb{F}_p$, and we say that E has *good reduction* at p. At all other primes, we say that E has bad reduction.

In the same way that we have Hecke eigenvalues a_p associated to a cuspidal newform f for primes p away from the level N of f, one can attach local data to a given elliptic curve at all but finitely many primes. Given an elliptic curve E, one can define an integer N_E, the *conductor* of E, which is divisible only by those primes at which E has bad reduction. At all primes not dividing N_E, we let $|\widetilde{E}(\mathbb{F}_p)|$ denote the number of points on the reduced curve $\widetilde{E}$ at p. We may then define

$$a_p = a_p(E) = p + 1 - |\widetilde{E}(\mathbb{F}_p)|.$$

The Modularity Theorem, in its most basic form, then states (see, for example, **[DS05], Theorem 8.8.1**):

Theorem 2.3.1. *Let E be an elliptic curve defined over the rationals, with conductor N. Then there exists a cuspidal newform of weight 2 and level N, which is an eigenform for the Hecke operators T_p such that, for every prime p not dividing N, we have*

$$a_p(f) = a_p(E).$$

Thus we can understand modularity, in a sense, to denote an equivalence between local data attached to elliptic curves and that attached to modular forms. To extend this idea to more general settings, we will need to consider some of the underlying machinery, which we will do in the next section.

2.4 Galois Representations

A key tool when studying modularity is the concept of a *Galois representation*, that is, a representation of the absolute Galois group $G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ of the rationals. It turns out that one can define Galois representations attached to both elliptic curves and modular forms, which encapsulate the local data a_p associated to each of these objects at all but finitely many primes. The Modularity Theorem can then be rephrased as an equivalence between these Galois representations, from which our statement in the previous section follows as an immediate consequence.

We now discuss these ideas in more detail. Given a prime ℓ, an *ℓ-adic Galois representation* is a continuous representation

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

for some $n \in \mathbb{N}$ (for our discussion, we shall consider only the case $n = 2$). Equivalently, we have a $\mathbb{Q}_\ell$-vector space V which is also a $G_{\mathbb{Q}}$-module, for which the action of $G_{\mathbb{Q}}$ is continuous. We say that ρ is *irreducible* if V contains no proper $G_{\mathbb{Q}}$-submodules, else we say it is *reducible*.

Since we require our representations to be continuous, it makes sense to briefly describe the topologies we are using: the group $G_{\mathbb{Q}}$, defined to be the profinite limit

$$G_{\mathbb{Q}} = \varprojlim_{F/\mathbb{Q} \text{ Galois}} \mathrm{Gal}(F/\mathbb{Q}),$$

is given the *Krull topology*, in which a neighbourhood basis of the identity is given by the subgroups $\mathrm{Gal}(F/K)$, where F/K is a finite Galois extension. On the other hand, the topology on $\mathrm{GL}_2(\overline{\mathbb{Q}}_\ell)$ is derived from the usual ℓ-adic topology.

As stated previously, we are interested in local data. To this end, we will define a family of elements of the absolute Galois group $G_{\mathbb{Q}}$, indexed by the rational primes. Given a prime p, let $\mathfrak{p}$ denote a maximal ideal of the integral closure $\overline{\mathbb{Z}}$ which contains p. We can then define a reduction map

$$\overline{\mathbb{Z}} \to \overline{\mathbb{Z}}/\mathfrak{p} \simeq \overline{\mathbb{F}}_p.$$

Define the *decomposition group* at p to be

$$D_p = \{\sigma \in G_{\mathbb{Q}}, \sigma(\mathfrak{p}) = \mathfrak{p}\},$$

so that elements of D_p can be viewed (under the above reduction map) as elements of the absolute Galois group $G_{\mathbb{F}_p} = \mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$. The latter group is isomorphic to the profinite group $\overline{\mathbb{Z}}$, and is known to be generated topologically

by the *geometric Frobenius element*. This is defined to be the inverse of the *arithmetic Frobenius element*, which is the standard automorphism

$$\sigma_p : \overline{\mathbb{F}}_p \to \overline{\mathbb{F}}_p, x \mapsto x^p.$$

It can be shown that the elements of D_p cover the group $G_{\mathbb{F}_p}$, and thus in particular the absolute Galois group contains a preimage of the geometric Frobenius; we call any such preimage a *Frobenius element at* p, and denote it by Frob_p.

As it stands, Frobenius elements are not well-defined: for each choice of maximal ideal $\mathfrak{p}$ above p, Frob_p is defined only up to the *inertia group*, which is defined to be the kernel

$$I_p = \ker(D_p \to G_{\mathbb{F}_p}).$$

We can sidestep this irregularity by restricting our attention to primes p at which our Galois representation ρ is *unramified*, meaning that the inertia group I_p lies in the kernel of ρ.

This still leaves one slight problem, as our definition of Frobenius elements remains dependent on our choice of maximal ideal $\mathfrak{p}$ above p. However, for the objects we are interested in, this difficulty will not prove insurmountable. It is not too difficult to see that any two maximal ideals $\mathfrak{p}$ and $\mathfrak{p}'$ above p are related by an element of $G_{\mathbb{Q}}$, and that the resulting decomposition groups must be conjugate in $G_{\mathbb{Q}}$. Thus the idea of ramification is independent of our choice of ideal, and the Frobenius elements at p form a well-defined conjugacy class in $G_{\mathbb{Q}}$. We shall mostly be interested in conjugation-invariant properties of our representation ρ (in particular, the trace), and so it is enough to choose an arbitrary representative of this class to be *the* Frobenius element at p.

It is known that the Frobenius elements Frob_p, as we range over all rational primes p, are dense in the absolute Galois group $G_{\mathbb{Q}}$. We shall therefore usually restrict our attention to evaluating our Galois representation ρ at Frobenius elements. In particular, it will turn out that the local data we are interested in can be found by evaluating the trace of our representations at Frobenius elements.

Before discussing the Galois representations associated to elliptic curves and modular forms, we would like to know how to compare two representations. Fortunately, there is a simple notion of isomorphism between Galois representations: we say that ρ_1 and ρ_2 are *isomorphic* (denoted $\rho_1 \simeq \rho_2$) if there exists some element $g \in \mathrm{GL}_2(\overline{\mathbb{Q}}_\ell)$ such that

$$\rho_2(\sigma) = g\ \rho_1(\sigma)\ g^{-1}$$

for all $\sigma \in G_{\mathbb{Q}}$.

Now, given an elliptic curve E defined over the rationals, how can we define an ℓ-adic Galois representation $\rho_{E,\ell}$ associated to it? It turns out that the group structure defined on E is key here, as we will wish to consider the ℓ-torsion of

E. More precisely, for any positive integer r, define the *ℓ^r-torsion points of E* to be the subgroup

$$E[\ell^r] = \{P \in E(\overline{\mathbb{Q}}), \ell^r P = \mathcal{O}_E\}.$$

This is known to be an abelian group, isomorphic to $(\mathbb{Z}/\ell^r\mathbb{Z})^2$. We define the *$\ell$-adic Tate module $T_\ell(E)$* of E to be the profinite limit

$$\mathrm{Ta}_\ell(E) = \varprojlim_r E[\ell^r].$$

By fixing appropriate bases for each of the torsion groups $E[\ell^r]$, we obtain an isomorphism

$$\mathrm{Ta}_\ell(E) \simeq \mathbb{Z}_\ell^2,$$

and similarly an isomorphism

$$\mathrm{Aut}(\mathrm{Ta}_\ell(E)) \simeq \mathrm{GL}_2(\mathbb{Z}_\ell).$$

We now bring the absolute Galois group into play. The coordinates of the ℓ^r torsion points are known to be algebraic integers, and so, defining $\mathbb{Q}(E[\ell^r])$ to be the number field generated by these coordinates, we obtain an action of $G_\mathbb{Q}$ on $\mathbb{Q}(E[\ell^r])$ for each r, which induces an automorphism of the torsion subgroup $E[\ell^r]$. These actions are compatible with the Tate module structure, and thus we can define a homomorphism

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

for each prime ℓ. In fact, we have the following result (see, for example, **[Wie08], Theorem 1.3.3**):

Theorem 2.4.1. *Let E be a rational elliptic curve of conductor N, and let ℓ be prime. Then there exists an irreducible Galois representation*

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

which is unramified at all primes p not dividing ℓN. For each such prime, the characteristic polynomial of $\rho_{E,\ell}(\mathrm{Frob}_p)$ is

$$X^2 - a_p(E)X + p.$$

Moreover, the determinant of $\rho_{E,\ell}$ is the ℓ-adic cyclotomic character of $\mathbb{Q}$.

We briefly recall that the ℓ-adic cyclotomic character of $\mathbb{Q}$ is the one-dimensional Galois representation χ_ℓ defined by

$$\sigma(\zeta) = \zeta^{\chi_\ell(\sigma)}$$

for all ℓ-power roots of unity $\zeta \in \overline{\mathbb{Q}}$. It is unramified at all primes apart from ℓ.

And what of modular forms? Although more complicated to define completely, the representation one attaches to a modular form turns out to bear similarities to that for an elliptic curve, in that one defines a Tate module related to modular curve $X_0(N)$, and a $G_{\mathbb{Q}}$-action on this module. Given a cuspidal newform f of level N and weight 2, which is an eigenform for the Hecke operators T_p, one can also define a Tate module $\mathrm{Ta}_\ell(f)$ for f, and the aforementioned $G_{\mathbb{Q}}$-action will descend to an action on $\mathrm{Ta}_\ell(f)$.

We now flesh out this idea (for a more detailed exposition, see **[DS05], Chapter 9.5**). For each N, define the *divisor group* $\mathrm{Div}(X_0(N))$ to be the group of formal finite $\mathbb{Z}$-linear combinations of points on $X_0(N)$,

$$\mathrm{Div}(X_0(N)) = \left\{ \sum n_P \cdot P, n_P \in \mathbb{Z},\ P \in X_0(N) \right\}.$$

We say a divisor is *principal* if it is of the form

$$D = \sum n_P \cdot P - n_Q \cdot Q,$$

where P and Q denote the zeros and poles respectively of some meromorphic function on the Riemann surface $X_0(N)$, and n_P and n_Q denote their multiplicities. We define the *Picard group* $\mathrm{Pic}^0(X_0(N))$ to be the quotient

$$\left\{ D \in \mathrm{Div}(X_0(N));\ \sum n_P = 0 \right\} / \left\{ D \in \mathrm{Div}(X_0(N)), D \text{ is principal} \right\}.$$

It is known that the Picard group is isomorphic to the *Jacobian* $\mathrm{Jac}(X_0(N))$ of $X_0(N)$, which can be thought of as a means of measuring the behaviour of complex linear maps from the space of holomorphic differentials on the modular curve. Since an in-depth discussion of the Jacobian is superfluous to our purposes, we shall simply make note of the fact that it has the structure of a g-dimensional complex torus, where g is the genus of the Riemann surface $X_0(N)$. With this in mind, it is clear that, given a prime ℓ and a positive integer r, we have an isomorphism of ℓ^r-torsion

$$\mathrm{Pic}^0(X_0(N))[\ell^r] \simeq (\mathbb{Z}/\ell^r\mathbb{Z})^{2g}.$$

We can therefore define the *ℓ-adic Tate module* of $X_0(N)$,

$$\mathrm{Ta}_\ell(\mathrm{Pic}^0(X_0(N))) = \varprojlim_r \mathrm{Pic}^0(X_0(N))[\ell^r].$$

Similarly to the case of elliptic curves, choosing compatible bases for these torsion groups leads to an isomorphism

$$\mathrm{Ta}_\ell(\mathrm{Pic}^0(X_0(N))) \simeq \mathbb{Z}_\ell^{2g}.$$

Now, it turns out that the modular curve $X_0(N)$ can be defined *algebraically*, as can any function defined upon it. As a result, we obtain an action of $G_{\mathbb{Q}}$

on the divisor group, which descends to an action on the Picard group. The fields generated by the torsion groups $\mathrm{Pic}^0(X_0(N))[\ell^r]$ are seen to be Galois extensions of the rationals, and thus are also acted on by $G_{\mathbb{Q}}$, and moreover this action is compatible with the structure of the Tate module. We can therefore define a homomorphism

$$\rho_{X_0(N)} : G_{\mathbb{Q}} \to \mathrm{Aut}(\mathrm{Ta}_\ell(\mathrm{Pic}^0(X_0(N)))) \simeq \mathrm{GL}_{2g}(\mathbb{Z}_\ell).$$

This is not yet the representation we seek, however, as there has been no mention of a specific modular form. It is now that the restriction of our attention to cusp forms which are eigenforms for the Hecke operators comes into play. Define the Hecke algebra $\mathbb{T}_{\mathbb{Z}}$ to be the $\mathbb{Z}$-algebra generated by the Hecke operators T_p. Then it is possible to define an action of $\mathbb{T}_{\mathbb{Z}}$ on the Picard group $\mathrm{Pic}^0(X_0(N))$, which restricts to ℓ-power torsion, and thus extends to an action on the Tate module $\mathrm{Ta}_\ell(X_0(N))$. Moreover, this action can be defined algebraically, and so commutes with the $G_{\mathbb{Q}}$-action on the Tate module.

We now fix a weight 2 cuspidal Hecke eigenform f of level N, and let I_f denote the ideal in $\mathbb{T}_{\mathbb{Z}}$ given by

$$I_f = \{T \in \mathbb{T}_{\mathbb{Z}}, Tf = 0\}.$$

The action of $\mathbb{T}_{\mathbb{Z}}$ on the Picard group descends to an action on the Jacobian $\mathrm{Jac}(X_0(N))$, and we can define an abelian variety

$$A_f = \mathrm{Jac}(X_0(N))/I_f\mathrm{Jac}(X_0(N)).$$

Let $\mathbb{Q}_f$ denote the number field generated by the Hecke eigenvalues $a_p(f)$, and let d denote its degree over the rationals. In an analogous manner to the case of elliptic curves, one can define an ℓ-adic Tate module

$$\mathrm{Ta}_\ell(A_f) = \varprojlim_r A_f[\ell^r] \simeq \mathbb{Z}_\ell^{2d},$$

and we have a natural action of $G_{\mathbb{Q}}$ on this module. Tying this together, we obtain the following result:

Theorem 2.4.2. *Let $f \in \mathcal{S}_2(\Gamma_0(N))$ be an eigenform for the Hecke operators T_p, and let $\mathbb{Q}_f$ denote the number field generated by its Hecke eigenvalues. Then, given a prime ℓ and a maximal ideal λ of the ring of integers $\mathcal{O}_{\mathbb{Q}_f}$ lying above ℓ, we have a 2-dimensional irreducible ℓ-adic Galois representation*

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

which is unramified at all primes p not dividing ℓN. For each such prime, the characteristic polynomial of $\rho_{f,\ell}(\mathrm{Frob}_p)$ is

$$X^2 - a_p(f)X + p.$$

Since the characteristic polynomial is conjugation-invariant, it is independent of our choice of Frobenius element at each unramified prime, and is preserved under isomorphism of Galois representations. We may therefore rephrase the statement of the Modularity Theorem, resulting in:

Theorem 2.4.3. *Let E be a rational elliptic curve, with conductor N. Then there exists an eigenform $f \in \mathcal{S}_2(\Gamma_0(N))$ for the Hecke operators T_p with number field $\mathbb{Q}_f \simeq \mathbb{Q}$ such that*

$$\rho_{f,\ell} \simeq \rho_{E,\ell}$$

for all primes ℓ.

Since this implies equality of the characteristic polynomials at the Frobenius elements Frob_p, **Theorem 2.3.1** follows immediately.

2.5 L-functions

With a view to what we shall consider in the next chapter, we shall touch upon another important concept in modern number theory: that of an *L-function*. These are meromorphic functions defined on the complex plane, which can be attached to a variety of mathematical objects.

L-functions arise by means of analytically continuing an *L-series*, which is an infinite series that converges absolutely on some complex half-plane, defining a function there. The most common example of an L-series is that of a *Dirichlet* L-series, which are constructed using Dirichlet characters. Specifically, let $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$ be a Dirichlet character for some N, and extend it to a function on the integers by composition with the reduction map modulo N. Then we define the Dirichlet L-series

$$L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}.$$

Here s denotes a complex variable, and $L(s, \chi)$ converges absolutely for $\mathbb{R}e[s] > 1$.

Since Dirichlet characters are multiplicative, and the L-series converges absolutely, we have a decomposition of $L(s, \chi)$ into a product of *local factors* $L_p(s, \chi)$, where

$$L_p(s, \chi) = \begin{cases} (1 - \chi(p)p^{-s})^{-1}; & \text{if } p \nmid N, \\ 1; & \text{if } p|N \end{cases}$$

for $\mathbb{R}e[s] > 1$, which we call the *Euler product expansion* of $L(s, \chi)$.

The Riemann zeta function is a well-known example of a Dirichlet L-function, obtained by taking the trivial character with $N = 1$. The resulting L-series is given by

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

for $\mathbb{R}e[s] > 1$, which can be shown to extend to a meromorphic function on the whole of $\mathbb{C}$, with a simple pole located at the point $s = 1$. Study of the Riemann zeta function has important applications to number theory, most notably with regards to the distribution of primes.

We shall proceed by discussing L-series attached to our three main objects of interest, namely modular forms, elliptic curves, and Galois representations. Over $\mathbb{Q}$, each of these is known to extend to a true L-function, but this need not be true for general number fields, and so we shall restrict our attention to the Euler product form of these L-series, which is a concept that will readily generalize to other settings.

To begin with, then, let $f \in \mathcal{S}_k(N, \chi)$ be a cusp form. Then we can define an L-series $L(s, f)$ attached to f, which converges absolutely for $\mathbb{R}e[s] > \frac{k}{2} + 1$, by means of an Euler product, whose local factors $L_p(s, f)$ are given by

$$L_p(s, f) = (1 - a_p p^{-s} + \chi(p) p^{k-1-2s})^{-1}$$

at each prime not dividing N. Here a_p denotes the eigenvalue of f under the action of the Hecke operator T_p. One can also define local factors at the finitely many primes which divide N, but we shall not do so here.

Similarly, to an elliptic curve E defined over $\mathbb{Q}$ we attach an L-series $L(s, E)$, which converges absolutely for $\mathbb{R}e[s] > \frac{3}{2}$, by means of an Euler product with local factors $L_p(s, E)$ given by

$$L_p(s, E) = (1 - a_p p^{-s} + p^{1-2s})^{-1}$$

for each prime at which E has good reduction. In this case a_p denotes the quantity $a_p(E)$ defined previously. We note that this resembles the L-series attached to a cusp form of weight 2 and trivial character.

Finally, let $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_n(\overline{\mathbb{Q}}_\ell)$ be an ℓ-adic Galois representation. Then one can attach an *Artin* L-series $L(s, \rho)$ to ρ which converges absolutely for $\mathbb{R}e[s] > 1$. The local factors $L_p(s, \rho)$ in the Euler product expansion are given by

$$L_p(s, \rho) = \det(1 - \rho(\mathrm{Frob}_p) p^{-s})^{-1}$$

at all but finitely many primes.

One can easily check that the L-series attached to modular forms and elliptic curves are equivalent to the Artin L-series attached to their respective Galois representations, and thus the Modularity Theorem can be rephrased in terms of an equivalence of L-functions. We shall return to this topic later, when we discuss generalizations of modularity within the framework of the Langlands programme, in which L-functions play a key role.

2.6 The Eichler-Shimura Isomorphism

In practice, one often wishes to determine which modular form f corresponds to a given elliptic curve E. As a result, we are interested in methods of determining the Hecke eigenvalues $a_p(f)$, and then comparing these to the local data $a_p(E)$. This idea will prove to have great significance when we move to non-classical modular forms defined over number fields, where we do not know whether all elliptic curves are modular, but where there exist techniques to prove isomorphism of Galois representations given the characteristic polynomials of Frobenius elements at a finite set of primes.

A result which shall motivate our methods is the Eichler-Shimura isomorphism, which states that modular forms can be viewed as certain classes in the cohomology of the congruence subgroup $\Gamma_0(N)$. More importantly, it turns out that the action of Hecke operators on modular forms can be realized in this new setting, so that the arithmetic data we seek is preserved. Since the topological setting lends itself more amenably to computational methods, it provides us with an easier pathway to identifying Galois representations.

We begin with some basic notions from group cohomology. Given a group G and a G-module M, we define the *first cohomology group of G with coefficients in M* $H^1(G;M)$ to be the quotient of the group of "twisted homomorphisms", or *cocycles*

$$\{f : G \to M, f(g_1 g_2) = g_1 \cdot f(g_2) + f(g_1)\},$$

modulo the subgroup of *coboundaries*, which are cocycles that take the form

$$f(g) = g(m) - m,\ g \in G,$$

for some $m \in M$.

We apply this to the group $\Gamma_0(N)$. For our purposes, we will restrict our attention to cohomology with coefficients in $\mathbb{C}$, on which $\Gamma_0(N)$ acts trivially. From the definition we observe that $H^1(\Gamma_0(N), \mathbb{C})$ is simply the group of homomorphisms $\mathrm{Hom}(\Gamma_0(N), \mathbb{C})$ from $\Gamma_0(N)$ to the additive group $\mathbb{C}$. Now, for any cusp $s \in \mathbb{P}^1(\mathbb{Q})$, let Γ_s denote the stabilizer of s in $\Gamma_0(N)$. By definition, we have a map of cohomology groups

$$H^1(\Gamma_0(N), \mathbb{C}) \to H^1(\Gamma_s, \mathbb{C})$$

obtained by restriction. We therefore obtain a map

$$\mathcal{P} : H^1(\Gamma_0(N), \mathbb{C}) \to \bigoplus_{s \in \mathbb{P}^1(\mathbb{Q})} H^1(\Gamma_s, \mathbb{C}),$$

and we define the *parabolic cohomology of* $\Gamma_0(N)$, $H^1_{\mathcal{P}}(\Gamma_0(N), \mathbb{C})$, to be the kernel of this map (in other words, the elements of $\mathrm{Hom}(\Gamma_0(N), \mathbb{C})$ which vanish on the stabilizers of cusps).

We are now in a position to state the Eichler-Shimura isomorphism:

Theorem 2.6.1. *We have isomorphisms*

$$\begin{aligned} \mathrm{Eis}_2(N) \oplus \mathcal{S}_2(N) \oplus \overline{\mathcal{S}_2(N)} &\simeq \mathrm{H}^1(\Gamma_0(N), \mathbb{C}), \\ \mathcal{S}_2(N) \oplus \overline{\mathcal{S}_2(N)} &\simeq \mathrm{H}^1_{\mathcal{P}}(\Gamma_0(N), \mathbb{C}), \end{aligned}$$

where

$$\overline{\mathcal{S}_2(N)} := \{\overline{f}, f \in \mathcal{S}_2(N)\}.$$

The theorem exists in greater generality; one can replace trivial coefficients with more exotic systems to obtain higher-weight modular forms. Since we are primarily interested in the correspondence between elliptic curves and weight 2 modular forms, the above statement is sufficient for our needs.

We make note of the fact that the above cohomology groups have an alternative realisation as cohomology groups of the open and closed modular curves $Y_0(N)$ and $X_0(N)$; indeed, we have isomorphisms

$$\begin{aligned} H^1(\Gamma_0(N), \mathbb{C}) &\simeq H^1(Y_0(N), \mathbb{C}), \\ H^1_{\mathcal{P}}(\Gamma_0(N), \mathbb{C}) &\simeq H^1(X_0(N), \mathbb{C}). \end{aligned}$$

This is a standard result (see for example the appendix of **[Hid93]**) and essentially involves constructing a simplicial complex from the modular curve, and then proving that the cohomology of the resulting resolution is isomorphic to the group cohomology.

The idea behind the proof of the Eichler-Shimura isomorphism is simple; given a form $f \in \mathcal{M}_2(N)$, we wish to somehow construct a function from $\Gamma_0(N)$ to $\mathbb{C}$ which is dependent on f. We do this by utilising *differentials*. Given $f \in \mathcal{M}_2(N)$, define a holomorphic differential ω_f on $\mathfrak{h}$ by

$$\omega_f := f(z)dz.$$

One can then define a function $\Psi_f : \Gamma_0(N) \to \mathbb{C}$ by

$$\Psi_f(\gamma) := \int_{z_0}^{\gamma(z_0)} \omega_f,$$

for some choice of base-point $z_0 \in \mathfrak{h}$. This in fact gives rise to a well-defined cohomology class, which moreover is independent of our choice of base-point.

In the same manner, we can define a holomorphic differential

$$\omega_{\overline{f}} := \overline{f(z)}d\overline{z}$$

for any $\overline{f} \in \overline{\mathcal{S}_2(N)}$. The isomorphism in the theorem is then obtained by sending a pair $(f, \overline{g})$ to the cohomology class of the map $\Psi_f + \Psi_{\overline{g}}$.

If f is in fact a cusp form, then the differential ω_f extends to a holomorphic differential at the cusps $\mathbb{P}^1(\mathbb{Q})$. In particular, we may take the base-point z_0 to be a cusp s, in which case it is clear that $\Psi_f|_{\Gamma_s}$ is trivial, and thus Ψ_f defines a class in the first parabolic cohomology group.

Recall from **Section 2.2** the Hecke correspondence on modular curves:

$$\begin{array}{ccc} X(\Gamma_1) & \xrightarrow{\widetilde{\alpha_g}} & X(\Gamma_2) \\ {\scriptstyle \pi_1}\downarrow & & \downarrow{\scriptstyle \pi_2} \\ X(\Gamma) & & X(\Gamma) \end{array}$$

where Γ is a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$, $\Gamma_1 = \Gamma \cap g^{-1}\Gamma g$ and $\Gamma_2 = \Gamma \cap g\Gamma g^{-1}$ have finite index in Γ for some $g \in \mathrm{GL}_2^+(\mathbb{R})$, π_i denotes the projection map from $X(\Gamma_i)$ to $X(\Gamma)$ and $\widetilde{\alpha_g}$ is the diffeomorphism from $X(\Gamma_1)$ to $X(\Gamma_2)$ sending a point $\Gamma_1 x$ to the point $\Gamma_2 gx$.

This induces a correspondence between cohomology groups:

$$\begin{array}{ccc} H^1(X(\Gamma_1), \mathbb{C}) & \xrightarrow{\widetilde{\alpha_{g,*}}} & H^1(X(\Gamma_2), \mathbb{C}) \\ {\scriptstyle \pi_1^*}\uparrow & & \downarrow{\scriptstyle \pi_{2,*}} \\ H^1(X(\Gamma), \mathbb{C}) & & H^1(X(\Gamma), \mathbb{C}) \end{array}$$

We refer to the map $(\pi_2\widetilde{\alpha_g})_*\pi_1^*$ as the *Hecke operator* arising from this correspondence. A stronger version of the Eichler-Shimura isomorphism than that which we have presented states that the isomorphism preserves the action of Hecke operators, which we shall now explain.

As in the case of Hecke operators acting on modular forms, let $\Gamma = \Gamma_0(N)$ and, for a prime p not dividing N, set $g = \left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right)$. In this particular case, we can give an explicit description of the resulting Hecke operator (which we shall also denote by T_p) through the action induced by the maps between modular curves on the corresponding spaces of differentials.

Let $\omega_f = f(z)dz$ denote a differential on the modular curve $X(\Gamma)$. The map π_1^* simply pulls ω_f back to a differential on $X(\Gamma_1)$, which we shall (by a minor abuse of notation) also refer to as ω_f. The map $(\pi_2\widetilde{\alpha_g})_*$ corresponds to integration along the fibres of the map $\pi_2\widetilde{\alpha_g}$. Since the groups Γ_1 and Γ_2 have been chosen to have finite index in Γ, this map has only finitely many fibres, and so we obtain a finite sum of differentials.

More precisely, let $\{\gamma_i\}$ be a set of representatives for the coset space $\Gamma_2\backslash\Gamma$. The fibres of a point $\Gamma x \in X(\Gamma)$ under π_2 are then given by the set of points $\{\Gamma_2\gamma_i x\}$, and the fibres of these points under the map $\widetilde{\alpha_g}$ are given by the set $\{\Gamma_2 g^{-1}\gamma_i x\}$. Now, by **Lemma 2.2.1** (replacing the element g in the lemma with g^{-1}), we see that the elements $\{g^{-1}\gamma_i\}$ are a set of representatives of the orbit space $\Gamma\backslash\Gamma g\Gamma$, and thus we can simplify the fibres of the point Γx under the map $\pi_2\widetilde{\alpha_g}$ to the set $\{\Gamma_1 g_i x\}$, where g_i is a set of representatives of the above orbit space.

As a result, we find that

$$(\pi_2\widetilde{\alpha_g})_*(\omega_f) = \sum_{i=1}^{p+1} f(g_i z)d(g_i z).$$

Observe that for $g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2^+(\mathbb{R})$,

$$d(gz) = d\left(\frac{az+b}{cz+d}\right) = \det(g)(cz+d)^{-2}dz,$$

and so

$$(\pi_2\widetilde{\alpha_g})_*(\omega_f) = \sum_{i=1}^{p+1} f|_{g_i}(z)dz = \omega_{T_p(f)}.$$

Thus the action of the Hecke operator T_p on differentials by the formula

$$T_p(\omega_f) = \omega_{T_p(f)}.$$

Note that, under this action, if $f \in \mathcal{M}_2(N)$ is an eigenform for the operator T_p, then the corresponding differential ω_f is an eigenfunction, with the same eigenvalue. The induced Hecke action on cohomology classes is then defined by

$$T_p([\Psi_f]) = [\Psi_{T_p(f)}]$$

(one can check that this is well-defined).

Chapter 3

Automorphic Forms and Representations

In this chapter, we discuss an important generalization of modular forms, the notion of an *automorphic form*, which allows us to consider forms defined over arbitrary number fields.

We begin in **Section 3.1** by discussing automorphic forms, which are functions on adele groups that obey certain functional equations, which reflect those imposed on modular forms. In particular, we show how a classical modular form gives rise to an automorphic form. Moreover, we discuss a generalization of the classical Hecke action to the space of automorphic forms, and establish that, for an automorphic form constructed from a classical modular form, the two actions are equivalent.

Section 3.2 provides an exposition of *automorphic representations*, which are a useful construction that allow us to study automorphic forms through the representation theory of local fields. We also rephrase the Hecke action on automorphic forms in terms of such objects. **Section 3.3** states how the local representations which define an automorphic representation are associated with Galois representations over local fields, and the properties shared by such representations.

Echoing **Section 2.6**, **Section 3.4** then shows how we can view certain automorphic representations as cohomology classes of symmetric spaces (which take the place of the upper-half plane in the classical theory), which moreover preserves the Hecke action on automorphic representations. Finally, **Section 3.5** gives an example of a *global correspondence*, in which one can attach global Galois representations to certain automorphic representations, which is compatible with the local correspondences discussed in **Section 3.3**.

3.1 Automorphic Forms for GL_2

A theorem as beautiful as the Modularity Theorem doesn't deserve to languish forever in the realm of the rationals, especially since the definition of an elliptic curve can easily be extended to arbitrary number fields simply by changing our coefficient field. However, things are not so simple when dealing with modular forms; *a priori*, their definition has little to do with the rationals, save for their behaviour under the modular group. This leads us to ask the question: can we "free" classical modular forms from the upper half-plane, and instead give a definition which is more amenable to altering the coefficient field? It turns out that we can, and in fact the modular group plays a key role in this. The material in the following sections can be found in **[JL70]**, or the expositions in **[Bum98], Chapter 3** and **[Gel97], Chapter VI**.

It is a standard fact that the upper half-plane $\mathfrak{h}$ can be identified with a quotient of the group $\mathrm{SL}_2(\mathbb{R})$. Indeed, this group acts transitively on $\mathfrak{h}$, and the subgroup $\mathrm{SO}(2)$ stabilizes the point $i \in \mathfrak{h}$, so we obtain a bijection

$$\mathrm{SL}_2(\mathbb{R})/\mathrm{SO}(2) \longrightarrow \mathfrak{h},\ g\mathrm{SO}(2) \longmapsto g(i).$$

We can therefore think of a cusp form $f \in \mathcal{S}_k(N)$, for k a positive integer, as a function on $\mathrm{SL}_2(\mathbb{R})$ which is right-invariant under the group $\mathrm{SO}(2)$, and which exhibits the usual properties under the left action of $\Gamma_0(N)$. Things become interesting if we twist this idea, and instead consider functions ϕ on $\mathrm{SL}_2(\mathbb{R})$ which are left-invariant under $\Gamma_0(N)$, and satisfy a certain symmetry with respect to the right action of $\mathrm{SO}(2)$. More precisely, denoting by k_θ the element of $\mathrm{SO}(2)$ corresponding to an anti-clockwise rotation through an angle θ, we require

$$\phi(\gamma g k_\theta) = e^{-ik\theta}\phi(g),$$

for all $\gamma \in \Gamma_0(N),\ g \in \mathrm{SL}_2(\mathbb{R})$.

Cusp forms give rise to such functions: indeed, given $f \in \mathcal{S}_k(N)$ we can define such a function ϕ_f by

$$\phi_f(g) = f|_g(i)$$

(it is a straightforward check to see that this function satisfies the desired properties). Ideally this mapping would be a bijection, but it is not: indeed, any modular *function* f will give rise to such a ϕ_f, so we expect that both the holomorphicity of a modular form f and its behaviour at the cusps should somehow be mirrored in ϕ.

Perhaps unsatisfyingly, we shall not provide the full details here, as we would soon like to generalize this idea to account for a different base field, which will include the rational setting as a special case, for which we shall provide a more detailed description. Suffice to say, the holomorphicity of f translates to the

vanishing of ϕ under the action of a certain differential operator on the Lie group $\mathrm{SL}_2(\mathbb{R})$, and the behaviour of f at the cusps translates to a certain growth condition on ϕ.

We now take what may seem a radical departure, in keeping with the modern theory, by considering functions *adelically*. Justification for this move can be found by considering the seminal work of John Tate in his thesis, produced in 1950, which concerns generalizations of Dirichlet L-series to number fields. Such objects, known as *Hecke L-series* due to their discovery by Erich Hecke, were already known to extend analytically to L-functions, but Tate provided greater insight into their behaviour by realizing them as functions on adele class groups. The local factors of a Dirichlet L-function then correspond to functions on the local field at each prime. Since we have already seen that the important arithmetic properties of classical modular forms are reflected in their L-functions, it is unsurprising that we should choose to follow this path when moving to arbitrary number fields.

We begin by considering the adelic analogue of a Dirichlet character: a *Hecke character*. We can consider such characters as one-dimensional analogues of modular forms (which can be thought of as two-dimensional objects, given their connection with the group SL_2) , and thus they provide a more accessible introduction to the concepts we will be working with.

Fix, therefore, a number field F, with ring of integers $\mathcal{O}_F$, and let $\mathbb{A}_F$ denote the ring of adeles over F. We define a character $\chi : \mathbb{A}_F^\times \to \mathbb{C}^\times$ to be a product

$$\chi = \bigotimes_v \chi_v,$$

running over all places v of F, where all but finitely many of the χ_v are *unramified*, meaning that χ_v is trivial on the unit group $\mathcal{O}_v^\times$ of the valuation ring. A *Hecke character* is then a character which is trivial on $F^\times$, embedded diagonally into $\mathbb{A}_F^\times$, i.e., a character of the *idele class group* $F^\times \backslash \mathbb{A}_F^\times$.

Since $\mathbb{A}_F^\times = \mathrm{GL}_1(\mathbb{A}_F)$, we can think of Hecke characters as "automorphic forms for GL_1". Typically, we would like our algebraic group (GL_1 in this case) to be defined over the rationals. Since we would like to consider arbitrary number fields, we replace GL_1 with the $\mathbb{Q}$-group $\mathrm{Res}_{F/\mathbb{Q}}(\mathrm{GL}_1)$ for a number field F, where $\mathrm{Res}_{F/\mathbb{Q}}$ denotes Weil restriction of scalars (this has the property that $\mathrm{Res}_{F/\mathbb{Q}}(\mathrm{GL}_1(A)) \simeq \mathrm{GL}_1(A \otimes_{\mathbb{Q}} F)$ for any $\mathbb{Q}$-algebra A; in particular, $\mathrm{Res}_{F/\mathbb{Q}}(\mathrm{GL}_1(\mathbb{A}_\mathbb{Q})) \simeq \mathbb{A}_F^\times$, and $\mathrm{Res}_{F/\mathbb{Q}}(\mathrm{GL}_1(\mathbb{Q})) \simeq F^\times$). Henceforth we shall denote by $\mathbb{A}$ the adele ring $\mathbb{A}_\mathbb{Q}$ over the rationals.

In the special case in which $F = \mathbb{Q}$, we can obtain a Hecke character on $\mathbb{A}$ from a Dirichlet character $\psi : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$. Indeed, suppose for each prime p we define subgroups $K_p(N)$ and $K_p^*(N)$ of $\mathbb{Z}_p$ by

$$K_p(N) = \begin{cases} \{x \in \mathbb{Z}_p;\ x = 1 \pmod N\}, & \text{if } p|N, \\ \mathbb{Z}_p^\times, & \text{if } p \nmid N, \end{cases}$$

and

$$K_p^*(N) = \begin{cases} \{x \in \mathbb{Z}_p;\ x = 1 \pmod N\}, & \text{if } p|N, \\ \mathbb{Q}_p^\times, & \text{if } p \nmid N. \end{cases}$$

If we let

$$K(N) = \mathbb{R}_+^\times \times \prod_p K_p(N) \text{ and } K^*(N) = \mathbb{R}_+^\times \prod_p K_p^*(N),$$

then we have identifications

$$\mathbb{A}^\times/\mathbb{Q}^\times \simeq K^*(N)/(\mathbb{Q}^\times \cap K^*(N))$$

and

$$K^*(N)/(K(N)(\mathbb{Q}^\times \cap K^*(N))) \simeq (\mathbb{Z}/N\mathbb{Z})^\times$$

(see, for example, **[Bum98], Section 3.1**). Precomposing χ with this second map gives us a character on $K^*(N)$ which is trivial on $\mathbb{Q} \cap K^*(N)$, which by the first identification can be realized as a Hecke character on $\mathbb{A}^\times/\mathbb{Q}^\times$.

We move on to the two-dimensional case. In a departure from the classical theory, we shall work with the group GL_2 rather than SL_2; in part this is due to the fact that the centre of the group GL_2 is a torus, and thus has nicer properties than the centre of SL_2, which simply consists of the matrices $\pm I$. In particular, we will be able to define Hecke characters on the centre of the group, which shall be important later.

To this end, fix a number field F, let $G = \mathrm{Res}_{F/\mathbb{Q}}(\mathrm{GL}_2)$, and denote by Z the centre of G. Note that $G(\mathbb{R}) \simeq \mathrm{GL}_2(\mathbb{R})^r \times \mathrm{GL}_2(\mathbb{C})^s$, where F has r real and s pairs of complex conjugate embeddings. Let K_∞ denote the compact open subgroup of $G(\mathbb{R})$ given by

$$K_\infty \simeq \mathrm{O}(2)^r \times \mathrm{U}(2)^s,$$

and let

$$K_f = \prod_p K_p,$$

where each K_p is a compact open subgroup of the group $G(\mathbb{Q}_p)$ (we shall not specify a choice just yet). Let $K = K_f \cdot K_\infty$.

Finally, let $\mathfrak{g}$ denote the Lie algebra of $G(\mathbb{R})$, and $\mathfrak{g}_\mathbb{C}$ its complexification. In addition, denote by $\mathcal{U}(\mathfrak{g}_\mathbb{C})$ the *universal enveloping algebra* of $\mathfrak{g}_\mathbb{C}$. We shall not discuss this in too much detail, merely noting that it can be identified with the space of left-invariant differential operators on $G(\mathbb{R})$. We denote by $\mathcal{Z}$ the centre of $\mathcal{U}(\mathfrak{g}_\mathbb{C})$.

As mentioned previously, automorphic forms for G are the two-dimensional analogue of Hecke characters, and thus are functions on $G(\mathbb{A})$ which are left-invariant under the subgroup $G(\mathbb{Q})$. To give the full definition, an *automorphic form* for G *of level* K_f is a function

$$\varphi : G(\mathbb{Q})\backslash G(\mathbb{A}) \to \mathbb{C}$$

which satisfies the following properties:

- The restriction of φ to $G(\mathbb{R})$ is smooth.
- φ is invariant under the right regular action of K_f, and the image of φ under the right regular action of K_∞ is a finite-dimensional vector space (such a function is called K-*finite*).
- φ lies in a finite-dimensional vector space that is invariant under the action of $\mathcal{Z}$ (such a function is called $\mathcal{Z}$-*finite*).
- φ is of *moderate growth*. To explain this notion, define a local height function $\|\cdot\|_v : \mathrm{GL}_2(F_v) \to \mathbb{R}$ at each finite place v of F by

  $$\|g\|_v = \max(|g_{i,j}|_v, |\det(g_v)|_v^{-1}),$$

  where the $g_{i,j}$ run through the matrix coefficients of g. We then define a global height function $\|\cdot\|$ to be the product of the local heights. Then φ is of moderate growth if there exist constants C and N such that

  $$|\varphi(g)| < C\,\|g\|^N \text{ for all } g \in G(\mathbb{A}).$$

If, in addition, φ satisfies the following *cuspidal condition*, namely that

- $\displaystyle\int_{F\backslash\mathbb{A}_F} \varphi\left(\left(\begin{smallmatrix}1 & x\\ 0 & 1\end{smallmatrix}\right) g\right) dx = 0$ for all $g \in G(\mathbb{A})$,

then we say that φ is a *cuspidal automorphic form* for G.

The form ϕ_f obtained from a cusp form $f \in \mathcal{S}_k(N)$ can be realized as an automorphic form for GL_2 according to this definition, once we specify an appropriate open compact subgroup K_f and extend ϕ_f to a function on $\mathrm{GL}_2(\mathbb{A})$. For our choice of subgroup K_f we take the group

$$K_0(N) = \prod_p K_p(N),$$

where

$$K_p(N) = \begin{cases} \left\{ \left(\begin{smallmatrix}a & b\\ c & d\end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{Z}_p);\ c = 0 \pmod N \right\}, & \text{if } p|N, \\ \mathrm{GL}_2(\mathbb{Z}_p), & \text{if } p \nmid N. \end{cases}$$

We then exploit the homeomorphism

$$\Gamma_0(N)\backslash \mathrm{SL}_2(\mathbb{R}) \simeq \mathrm{GL}_2(\mathbb{Q})\backslash \mathrm{GL}_2(\mathbb{A})/A_G^0(\mathbb{R})K_f,$$

where $A_G^0(\mathbb{R})$ denotes the elements in the centre of $\mathrm{GL}_2(\mathbb{R})$ with positive eigenvalues (and thus is isomorphic to $\mathbb{R}_+$), to extend ϕ_f to a function on $\mathrm{GL}_2(\mathbb{A})$, where it defines an automorphic form.

Explicitly, we make use of the *strong approximation theorem* (see **[Bum98], Theorem 3.3.1**) to express any element $g \in \mathrm{GL}_2(\mathbb{A})$ as a product

$$g = \gamma g_\infty k_0,$$

where $\gamma \in \mathrm{GL}_2(\mathbb{Q})$, $g_\infty \in \mathrm{GL}_2^+(\mathbb{R})$ and $k_0 \in K_0(N)$. We then define a function φ_f on $\mathrm{GL}_2(\mathbb{A})$ by

$$\varphi_f(g) = \phi_f(g_\infty).$$

The function φ_f is in fact an automorphic form, and is said to have *trivial central character*, meaning that

$$\varphi_f(zg) = \varphi_f(g)$$

for all $z \in Z(\mathbb{A})$, the centre of $\mathrm{GL}_2(\mathbb{A})$, and all $g \in \mathrm{GL}_2(\mathbb{A})$. This is easy to see: the $\mathbb{Q}_p$-component of any such z in fact lies in $\mathrm{GL}_2(\mathbb{Z}_p)$ for all but finitely many primes p so, after clearing denominators, we may assume that

$$z = z' z_\infty k_0$$

with $z' \in \mathrm{GL}_2(\mathbb{Q})$, $z_\infty \in \mathrm{GL}_2^+(\mathbb{R})$ and $k_0 \in K_0(N)$ (since each $\mathbb{Q}_p$-component is diagonal, once it lies in $\mathrm{GL}_2(\mathbb{Z}_p)$ we know it lies in $K_p(N)$).

Thus, letting $z_\infty = \left(\begin{smallmatrix} z_0 & 0 \\ 0 & z_0 \end{smallmatrix}\right)$, and decomposing $g = \gamma g_\infty k_0'$, we have

$$\begin{aligned}
\varphi_f(zg) &= \phi_f(z_\infty g_\infty) \\
&= f|_{z_\infty g_\infty}(i) \\
&= f|_{g_\infty z_\infty}(i) \\
&= \det(z_\infty)^{\frac{k}{2}} z_0^{-k} f|_{g_\infty}(i) \\
&= f|_{g_\infty}(i) \\
&= \varphi_f(g),
\end{aligned}$$

as required.

It is clear that this depends on the fact that f has trivial character. If we were to consider a cusp form $f \in \mathcal{S}_k(N, \chi)$, for some Dirichlet character χ on $(\mathbb{Z}/N\mathbb{Z})^\times$, we would like the corresponding form φ_f to mirror the effect of χ on f.

We therefore consider automorphic forms with non-trivial character. Precisely, fix a Hecke character $\chi : \mathbb{A}_F^\times \to \mathbb{C}^\times$, and extend it to a function $\omega = \omega_\chi$ on $Z(\mathbb{A})$, where Z is the centre of GL_2, by defining

$$\omega\left(\left(\begin{smallmatrix} a & 0 \\ 0 & a \end{smallmatrix}\right)\right) = \chi(a).$$

We then say that an automorphic form φ for GL_2 has *central character* ω if

$$\varphi(zg) = \omega(z)\varphi(g)$$

for all $z \in Z(\mathbb{A})$, $g \in G(\mathbb{A})$. We denote by $\mathcal{A}_0(G(\mathbb{Q})\backslash G(\mathbb{A}), \omega)$ the space of cuspidal automorphic forms with central character ω.

We state without proof that a cusp form $f \in \mathcal{S}_k(N, \chi)$ does indeed correspond to an automorphic form φ_f with central character ω_χ, where ω_χ is the character on $Z(\mathbb{A})$ induced by realizing χ as a Hecke character as described previously (see, for example, **[Bum98], Section 3.6**, but note that we have to slightly alter our construction of the form φ_f). For future reference, we note that the conditions we have imposed on automorphic forms imply in particular that they are square-integrable, and thus lie in the Hilbert space $L_0^2(G(\mathbb{Q})\backslash G(\mathbb{A}), \omega)$ of square-integrable functions on $G(\mathbb{A})$ which are trivial on the component $G(\mathbb{Q})$, have central character ω, and satisfy the cuspidal condition (in fact, they form a dense subset).

Just as we can translate classical modular forms into this new, adelic setting, so too can we translate the action of Hecke operators. Since the role of the congruence subgroups $\Gamma_0(N)$ in classical theory is taken on by the compact subgroups $K_0(N)$ when considering automorphic forms, it should not be too much of a surprise to see that these operators arise from Hecke correspondences of the form

$$\begin{array}{ccc} K_1 & \xrightarrow{\alpha_{g_f}} & K_2 \\ {\scriptstyle \iota_1}\downarrow & & \downarrow{\scriptstyle \iota_2} \\ K & & K \end{array}$$

where K is a compact subgroup of $\mathrm{GL}_2(\mathbb{A}_f)$, $g_f \in \mathrm{GL}_2(\mathbb{A}_f)$ is an element such that $K_1 := K \cap g_f^{-1} K g_f$ and $K_2 := K \cap g_f K g_f^{-1}$ have finite index in K, ι_i denotes the inclusion $K_i \hookrightarrow K$, and α_{g_f} is the homomorphism:

$$K_1 \to K_2, k_0 \mapsto g_f k_0 g_f^{-1}.$$

Analogously to the classical case, let $\{g_1, \ldots, g_n\}$ be a set of representatives for the orbit space Kg_fK/K (note that, while the congruence subgroups of classical theory act on the left, our compact subgroups act on the right) so that

$$Kg_fK = \coprod_{i=1}^{n} g_i K.$$

Then we can define an operator T_{g_f} on automorphic forms of level K by setting

$$T_{g_f}(\varphi)(g) = \sum_{i=1}^{n} \varphi(gg_i).$$

We shall soon see how to recover the action of Hecke operators on classical forms in terms of automorphic forms. Before proceeding, however, we shall need to establish the following notation:

For a prime p, let

$$\iota_p : \mathrm{GL}_2(\mathbb{Q}) \hookrightarrow \mathrm{GL}_2(\mathbb{A}_f)$$

denote the embedding sending a matrix in $\mathrm{GL}_2(\mathbb{Q})$ to the $\mathbb{Q}_p$-component of $\mathrm{GL}_2(\mathbb{A}_f)$. Similarly, let

$$\iota_\infty : \mathrm{GL}_2(\mathbb{Q}) \hookrightarrow \mathrm{GL}_2(\mathbb{A})$$

denote the embedding sending a matrix to the real component of $\mathrm{GL}_2(\mathbb{A})$.

Additionally, for a prime p, let

$$\hat{\iota}_p : \mathrm{GL}_2(\mathbb{Q}) \hookrightarrow \mathrm{GL}_2(\mathbb{A}_f)$$

denote the embedding sending a matrix in $\mathrm{GL}_2(\mathbb{Q})$ to all $\mathbb{Q}_q$-components with $q \neq p$. Finally, let

$$\iota = \iota_p \cdot \hat{\iota}_p \cdot \iota_\infty$$

denote the diagonal embedding of a matrix in $\mathrm{GL}_2(\mathbb{Q})$ into $\mathrm{GL}_2(\mathbb{A})$ (note that the latter two maps are well-defined, in that an element of $\mathrm{GL}_2(\mathbb{Q})$ lies in $\mathrm{GL}_2(\mathbb{Z}_p)$ for all but finitely many primes p).

Now, let $G = \mathrm{GL}_2$, let $K = K_0(N)$ and, for a prime p not dividing N, let $g_f = \iota_p \left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right)$. A set of representatives for the orbit space Kg_fK is then given by $\{\iota_p(g_0), \ldots, \iota_p(g_{p-1}), \iota_p(g_p)\}$, where

$$g_i = \begin{cases} \left(\begin{smallmatrix} p & i \\ 0 & 1 \end{smallmatrix}\right), & \text{if } i \in 0, \ldots, p-1, \\ \left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right), & \text{if } i = p. \end{cases}$$

We then define the Hecke operator T_p by the action

$$T_p(\varphi)(g) = \sum_{i=0}^{p} \varphi(g\iota_p(g_i)).$$

For an arbitrary element $g \in \mathrm{GL}_2(\mathbb{A})$, write

$$g = \gamma g_\infty k_0$$

with $\gamma \in \mathrm{GL}_2(\mathbb{Q})$, $g_\infty \in \mathrm{GL}_2(\mathbb{R})$ and $k_0 \in K$, using the strong approximation theorem. Then

$$\begin{aligned} T_p(\varphi)(g) &= \sum_{i=0}^{p} \varphi(\gamma g_\infty k_0 \iota_p(g_i)) \\ &= \sum_{i=0}^{p} \varphi(\gamma g_\infty \iota_p(g_i) k'_{0,i}) \\ &= \sum_{i=0}^{p} \varphi(\gamma \iota_p(g_i) g_\infty k'_{0,i}) \end{aligned}$$

noting that, by the double coset decomposition

$$K g_f K = \coprod_{i=0}^{p} \iota_p(g_i) K,$$

we have $k_0 \iota_p(g_i) = \iota_p(g_j) k'_{0,j}$ for some $k'_{0,j} \in K$ and some $j \in 0, \ldots, p$ (we rely on the fact that distinct g_i give rise to distinct g_j for a fixed choice of k_0, which follows from the disjointness of the right cosets $\iota_p(g_i)$).

Note that, for $q \neq p$, $g_i^{-1} \in \mathrm{GL}_2(\mathbb{Z}_q)$, and moreover the lower-left entry of each g_i^{-1} is equal to zero, implying that $\hat{\iota}_p(g_i^{-1}) \in K$. Thus, in the decomposition

$$\iota_p(g_i) = \iota(g_i) \iota_\infty(g_i^{-1}) \hat{\iota}_p(g_i^{-1}),$$

we have $\iota(g_i) \in \mathrm{GL}_2(\mathbb{Q})$, $\iota_\infty(g_i^{-1}) \in \mathrm{GL}_2^+(\mathbb{R})$ and $\hat{\iota}_p(g_i^{-1}) \in K$.

Suppose now that $\varphi = \varphi_f$ for some $f \in \mathcal{M}_k(N)$. Then

$$\begin{aligned} T_p(\varphi_f)(g) &= \sum_{i=0}^{p} \varphi_f(\gamma \iota(g_i) \iota_\infty(g_i^{-1}) g_\infty \hat{\iota}_p(g_i^{-1}) k'_{0,i}) \\ &= \sum_{i=0}^{p} \phi_f(g_i^{-1} g_\infty). \end{aligned}$$

For each $i \in \{0, \ldots, p\}$, we have $g_i^{-1} = \left(\begin{smallmatrix} p^{-1} & 0 \\ 0 & p^{-1} \end{smallmatrix}\right) \hat{g}_i$, where

$$\hat{g}_i = \begin{cases} \left(\begin{smallmatrix} 1 & -i \\ 0 & p \end{smallmatrix}\right), & \text{if } i \in \{0, \ldots, p-1\}, \\ \left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right), & \text{if } i = p, \end{cases}$$

i.e., $\{\hat{g}_0, \ldots, \hat{g}_p\}$ is a set of representatives for the orbit space $\Gamma_0(N) \left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right) \Gamma_0(N)$ associated to the classical Hecke operator T_p.

Since we have already seen that ϕ_f acts trivially on scalar matrices, we find that

$$\begin{aligned} T_p(\varphi_f)(g) &= \sum_{j=0}^{p} \phi_f(\hat{g}_j g_\infty) \\ &= \sum_{j=0}^{p} f|_{\hat{g}_j g_\infty}(i) \\ &= \sum_{j=0}^{p} (f|_{\hat{g}_j})|_{g_\infty}(i) \\ &= \phi_{T_p(f)}(g_\infty) \\ &= \varphi_{T_p(f)}(g). \end{aligned}$$

Thus if f is an eigenform for the Hecke operators T_p, so too is φ_f, and the eigenvalues of f are preserved under this correspondence.

It will prove useful later on to explain precisely how we came to the definition

$$T_p(\varphi)(g) = \sum_{i=0}^{p} \varphi(g\iota_p(g_i)).$$

To this end, given a compact subgroup K_f of $\mathrm{GL}_2(\mathbb{A}_f)$, define the *Hecke algebra* $\mathcal{H}_p$ at the prime p to be the set of locally constant functions with compact support on $\mathrm{GL}_2(\mathbb{Q}_p)$, and the *Hecke algebra* $\mathcal{H}_{K_p}$ to be the subset of functions that are both left- and right-invariant under the action of the subgroup K_p of K_f. The Hecke algebra is a commutative unital ring under convolution (see, for example, **[Bum98], Section 4.6**).

The ring $\mathcal{H}_{K_p}$ admits an action on automorphic forms of level K_f, given by

$$\sigma(\varphi)(g) = \int_{\mathrm{GL}_2(\mathbb{A})} \sigma(h)\varphi(gh)dh$$

for $\sigma \in \mathcal{H}_{K_p}$.

For our particular example, in which $K_f = K_0(N)$, let p be a prime not dividing N, and define $T_p \in \mathcal{H}_{K_p}$ to be the characteristic function of the double coset

$$K_p \left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right) K_p,$$

normalised by a factor of $\frac{1}{\mathrm{vol}(K_p)}$, so that

$$\int_{K_p} T_p(h)dh = 1.$$

Then, letting $\{g_0, \ldots, g_p\}$ be our set of representatives for this double coset, we have

$$\begin{aligned} T_p(\varphi)(g) &= \frac{1}{\mathrm{vol}(K_p)} \int\limits_{K_p \left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right) K_p} \varphi(gh)dh \\ &= \frac{1}{\mathrm{vol}(K_p)} \sum_{i=0}^{p} \int\limits_{g_i K_p} \varphi(gh)dh \\ &= \frac{1}{\mathrm{vol}(K_p)} \sum_{i=0}^{p} \int\limits_{K_p} \varphi(gg_i)dh \\ &= \sum_{i=0}^{p} \varphi(gg_i), \end{aligned}$$

as required.

3.2 Representation Theory of GL_2

Recall that our definition of an automorphic form with central character ω implies that such objects lie in the Hilbert space $L^2(\mathrm{GL}_2(\mathbb{Q})\backslash\mathrm{GL}_2(\mathbb{A}), \omega)$ of square-integrable functions on $\mathrm{GL}_2(\mathbb{A})$. This space is acted on by $G(\mathbb{A})$ under the right regular action, and we can study this behaviour by considering the representation theory of $G(\mathbb{A})$ (this statement is not entirely accurate - at the archimedean places v of F we will study objects known as $(\mathfrak{g}, K)$-modules rather than true representations of $G(F_v)$ - but suffices for the moment). We shall therefore spend this section describing the representation theory of GL_2.

In order to understand the representation theory of $\mathrm{GL}_2(\mathbb{A}_F)$, we first consider the corresponding theory of the groups $\mathrm{GL}_2(F_v)$, where v is a place of the number field F, and then piece together these local theories to obtain a global theory.

We begin with the non-archimedean places. Let v be a finite place of F, F_v the completion of F with respect to v, and $\mathcal{O}_v$ the valuation ring of F_v. For ease of notation, we will denote by G the group $\mathrm{GL}_2(F_v)$ for the duration of this discussion.

We define an *admissible representation* of G on a complex vector space V to be a homomorphism

$$\pi : G \to \mathrm{GL}(V)$$

that is *smooth*, by which we mean that the stabilizer in G of any point $v \in V$ is open, and that satisfies the property that for any compact open subgroup K of G, the space

$$V^K := \{v \in V, \pi(k)v = v \text{ for all } k \in K\}$$

of K-fixed vectors is finite-dimensional. We will be interested in *irreducible* representations; i.e., those V which admit no smaller G-invariant subspace. It can be shown that any smooth, irreducible representation of G is automatically admissible. We say that π is *unramified* if the space of $\mathrm{GL}_2(\mathcal{O}_v)$-fixed vectors is non-trivial. Analogously to the example of Hecke characters, the adelic representations we shall consider will be unramified at all but finitely many places.

We now discuss our main source of admissible representations: *induced representations*. These are constructed from characters applied to the Borel subgroup of upper-triangular matrices. Explicitly, let $\chi_1, \chi_2 : F_v^\times \to \mathbb{C}^\times$ be two characters, and define $B(\chi_1, \chi_2)$ to be the set of functions $f : G \to \mathbb{C}^\times$ which are smooth under the right regular action of G, and satisfy

$$f\left(\begin{pmatrix} a_1 & x \\ 0 & a_2 \end{pmatrix} g\right) = \chi_1(a_1)\chi_2(a_2)\left|\frac{a_1}{a_2}\right|^{\frac{1}{2}} f(g)$$

for all $g \in G$ (we understand $|\cdot|$ to mean the non-archimedean absolute value $|\cdot|_v$).

It is simple to see that the $B(\chi_1, \chi_2)$ are admissible. Indeed, the smoothness of each f implies that $B(\chi_1, \chi_2)$ is smooth as a G-representation. Moreover, the *Iwasawa decomposition* of G shows that $G = B \cdot K$, where B denotes the Borel subgroup and $K = \mathrm{GL}_2(\mathcal{O}_v)$ is a maximal compact open subgroup of G, and so any $f \in B(\chi_1, \chi_2)$ is defined completely by its values on K. In particular, since any compact open subgroup K' has finite index in K, any $f \in B(\chi_1, \chi_2)^{K'}$ is defined by its values on a finite set of representatives for K/K', and thus $B(\chi_1, \chi_2)^{K'}$ is finite-dimensional.

The representations we will be interested in can be derived from induced representations. Although $B(\chi_1, \chi_2)$ need not be irreducible, the following result (see **[Kud04], Theorem 3.1**) shows that every induced representation contains a unique irreducible subrepresentation or quotient:

Theorem 3.2.1. *Let $\chi_1, \chi_2 : F_v^\times \to \mathbb{C}^\times$ be two characters. Then:*

(i) *If $\chi_1\chi_2^{-1} \neq |\cdot|^{\pm 1}$, then the representation $B(\chi_1, \chi_2)$ is irreducible.*

(ii) *If $\chi_1\chi_2^{-1} = |\cdot|$, write $\chi_1 = \chi|\cdot|^{\frac{1}{2}}$ and $\chi_2 = \chi|\cdot|^{-\frac{1}{2}}$, for $\chi : F_v^\times \to \mathbb{C}^\times$ a character. Then $B(\chi_1, \chi_2)$ has a one-dimensional quotient on which G acts by the character $\chi \circ \det$, and an infinite-dimensional irreducible subrepresentation $\sigma(\chi)$.*

(iii) *If $\chi_1\chi_2^{-1} = |\cdot|^{-1}$, write $\chi_1 = \chi|\cdot|^{-\frac{1}{2}}$ and $\chi_2 = \chi|\cdot|^{\frac{1}{2}}$, for $\chi : F_v^\times \to \mathbb{C}^\times$ a character. Then $B(\chi_1, \chi_2)$ has a one-dimensional submodule on which G acts by the character $\chi \circ \det$, and an infinite-dimensional irreducible quotient $\sigma(\chi)$.*

We call the $B(\chi_1, \chi_2)$ *principal series representations*, and the $\sigma(\chi)$ *special representations*. In the special case where χ is the trivial character, we call $\sigma(\chi)$ the *Steinberg representation*, which we denote by St. One can easily see that for any character χ, $\sigma(\chi) \simeq \mathrm{St} \otimes \chi$, and thus special representations are also known as *twists* of the Steinberg representation.

The above examples are all that we shall require: indeed, it is known that every irreducible admissible representation of G is either an irreducible principal series, a twist of the Steinberg representation, a one-dimensional representation of the form $\chi \circ \det$, for χ a character of $F_v^\times$, or else is a *supercuspidal representation*, which we shall not define. Each of these types of representation are known to be inequivalent.

Since we will require most of our representations to be unramified, we would like to classify such representations. Recall that for a representation π to be unramified, we require that it has a non-trivial $\mathrm{GL}_2(\mathcal{O}_v)$-fixed vector. In particular, an unramified *character* $\chi : F_v^\times \to \mathbb{C}^\times$ is trivial on the unit group $\mathcal{O}_v^\times$, and thus is defined completely by its value on a uniformiser ϖ. The following result (see **[Kud04], Theorem 3.3**) says that unramified representations can be classified by pairs of unramified characters:

Theorem 3.2.2.

(i) *For every pair of unramified characters $\chi_1, \chi_2 : F_v \to \mathbb{C}^\times$, there is an unramified irreducible admissible representation $\pi(\chi_1, \chi_2)$ of G. If $\chi_1\chi_2^{-1} \neq |\cdot|^{\pm 1}$, then $\pi(\chi_1, \chi_2)$ is given by the irreducible principal series $B(\chi_1, \chi_2)$. Otherwise, $\pi(\chi_1, \chi_2)$ is given by the one-dimensional representation $\chi \circ \det$, where $\chi_1 = \chi|\cdot|^{\pm\frac{1}{2}}$, $\chi_2 = \chi|\cdot|^{\mp\frac{1}{2}}$.*

(ii) *Every unramified irreducible representation of G is isomorphic to one of the $\pi(\chi_1, \chi_2)$. Moreover, any two such representations are inequivalent, with the exception that*

$$\pi(\chi_1, \chi_2) \simeq \pi(\chi_2, \chi_1).$$

The unramified representations we shall consider will *always* take the form of an irreducible principal series. To each such representation, we can assign a semisimple conjugacy class in $\mathrm{GL}_2(\mathbb{C})$, obtained via the mapping

$$\pi = \pi(\chi_1, \chi_2) \mapsto \left[\begin{pmatrix} \chi_1(\varpi) & 0 \\ 0 & \chi_2(\varpi) \end{pmatrix} \right].$$

In fact (see **[Kud04], Corollary 3.4**), this map is a bijection, and we call the conjugacy class corresponding to π the *Langlands class* t_π of π.

For an unramified representation π_v of G, we can define a local L-factor $L(s, \pi_v)$ by setting

$$L(s, \pi_v) = [(1 - \chi_1(\varpi)q^{-s})(1 - \chi_2(\varpi)q^{-s})]^{-1},$$

where q is the cardinality of the residue field of F_v. We shall bear this in mind for later, when we shall consider local Galois representations.

At this juncture, we would like to return to the action of Hecke operators on automorphic forms, and see how this can be extended to the setting of admissible representatives of GL_2 over non-archimedean local fields. For a place v of F, fix a compact open subgroup K_v of $\mathrm{GL}_2(F_v)$, and recall that the Hecke algebra $\mathcal{H}_{K_v}$ is a commutative ring consisting of locally constant functions on $\mathrm{GL}_2(F_v)$ with compact support, which are K_v-biinvariant.

Given an admissible representation (π, V_π), we can define an action of $\mathcal{H}_{K_v}$ on V by

$$\pi(\sigma)w = \int_{\mathrm{GL}_2(F_v)} \sigma(g)\pi(g)w dg$$

for all $\sigma \in \mathcal{H}_{K_v}$ and $w \in V$. It is not difficult to see that this is in fact a representation of the ring $\mathcal{H}_{K_v}$ (which we recall is a ring under convolution). Moreover, the space V^{K_v} of K_v-fixed vectors in V is preserved under this action, and thus forms a $\mathcal{H}_{K_v}$-module.

The following fact (see **[Bum98], Proposition 4.2.3**) will be useful to us:

Proposition 3.2.3. *Let (π, V_π) be an irreducible admissible representation of $\mathrm{GL}_2(F_v)$. Then the space V^{K_v} of K_v-fixed vectors in V is either trivial or a finite-dimensional admissible $\mathcal{H}_{K_v}$-module, for all compact open subgroups K_v of $\mathrm{GL}_2(F_v)$.*

Now, suppose further that $K_v = \mathrm{GL}_2(\mathcal{O}_v)$. In this case, $\mathcal{H}_{K_v}$ is commutative (a proof of which can be found in **[Bum98], Theorem 4.6.1**), and Schur's lemma, combined with the finite-dimensionality of V^{K_v}, implies that in fact V^{K_v} (if non-trivial) is a one-dimensional representation of $\mathcal{H}_{K_v}$. In particular, fixing a vector $w_{K_v} \in V^{K_v}$, we obtain a character $\theta : \mathcal{H}_{K_v} \to \mathbb{C}$ by setting

$$\pi(\sigma) w_{K_v} = \theta(\sigma) w_{K_v}.$$

We consider this in the context of the adelic extension of classical Hecke operators. For an integer N and a prime p not dividing N, set $K_p = \mathrm{GL}_2(\mathbb{Z}_p)$, and let $\pi = \pi(\chi_1, \chi_2)$ be an unramified principal series. The corresponding space V^{K_p} of K_p-fixed vectors can easily be seen to be spanned by the function ϕ_p, where

$$\phi_p\left(\left(\begin{smallmatrix} a_1 & x \\ 0 & a_2 \end{smallmatrix}\right) k_0\right) = \chi_1(a_1)\chi_2(a_2)\left|\frac{a_1}{a_2}\right|_p^{\frac{1}{2}}$$

for $a_1, a_2 \in F_v$ and $k_0 \in K_p$.

Recall that the Hecke operator T_p is defined to be the normalized characteristic function of the double coset $K_p \left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right) K_p$. Letting $\{g_0, \ldots, g_{p-1}, g_p\}$ be the set of representatives for this double coset established in the previous section, we therefore see that

$$\begin{aligned}
\pi(T_p)\phi_p &= \int_{\mathrm{GL}_2(\mathbb{Q}_p)} T_p(g)\pi(g)\phi_p dg \\
&= \frac{1}{\mathrm{vol}(K_p)} \int_{K_p\left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right)K_p} \pi(g)\phi_p dg \\
&= \frac{1}{\mathrm{vol}(K_p)} \sum_{i=0}^{p} \int_{g_i K_p} \pi(g)\phi_p dg \\
&= \frac{1}{\mathrm{vol}(K_p)} \sum_{i=0}^{p} \int_{K_p} \pi(g_i g)\phi_p dg \\
&= \sum_{i=0}^{p} \phi_p(g_i)\phi_p.
\end{aligned}$$

Now, recalling that the representatives g_i are given by

$$g_i = \begin{cases} \left(\begin{smallmatrix} p & i \\ 0 & 1 \end{smallmatrix}\right), & \text{if } i \in \{0, \ldots, p-1\}, \\ \left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right), & \text{if } i = p, \end{cases}$$

we see that

$$\phi_p(g_i) = \begin{cases} \chi_1(p)|p|^{\frac{1}{2}}\phi_p, & \text{if } i \in \{0, \ldots, p-1\}, \\ \chi_2(p)|p|^{-\frac{1}{2}}\phi_p, & \text{if } i = p, \end{cases}$$

and thus deduce that

$$\pi(T_p)(\phi_p) = p^{\frac{1}{2}}(\chi_1(p) + \chi_2(p))\phi_p = p^{\frac{1}{2}}\mathrm{Tr}(t_\pi)\phi_p,$$

where t_π denotes the Langlands class of π.

Thus

$$\theta(T_p) = p^{\frac{1}{2}}\mathrm{Tr}(t_\pi),$$

a result which we shall return to later.

Having discussed the non-archimedean theory, let us now consider the case where v is an archimedean place of F. As before, let G denote $\mathrm{GL}_2(F_v)$, and let K be a maximal compact subgroup of G (so $K \simeq \mathrm{O}(2)$ or $\mathrm{U}(2)$, depending on whether v corresponds to a real or complex embedding). A representation $\pi : G \to \mathrm{GL}(V)$, for V a complex vector space, is called *admissible* if it is *smooth* (i.e., infinitely differentiable) and if, when restricted to the subgroup K, the resulting representation contains each irreducible unitary representation of K with *finite* multiplicity.

As alluded to in the previous section, we do *not* want to consider such representations. The reason for this can be seen by considering automorphic forms. Recall that such forms span a finite-dimensional vector space under the right regular action of the maximal compact subgroup at the archimedean places of F.

Analogously, given a representation $\pi : G \to \mathrm{GL}(V)$ as above, one defines the subspace V_K of *K-finite vectors* of V to be

$$V_K := \{v \in V;\ \pi(K)v \text{ spans a finite-dimensional vector space}\}.$$

One would hope that the space V_K is preserved under the action of $\pi(G)$, but this need not be the case. It *is* the case, however, that V_K is preserved under the corresponding action of the Lie algebra $\mathfrak{g}$ of G, which motivates the following definition:

A $(\mathfrak{g}, K)$-*module* is a complex vector space V with actions of both $\mathfrak{g}$ and K, satisfying the following conditions:

1. The actions of $\mathfrak{g}$ and K are compatible, in the sense that
$$k(Xv) = (\mathrm{Ad}(k)X)(kv),$$
for all $k \in K, X \in \mathfrak{g}$, where Ad denotes the adjoint action of K on $\mathfrak{g}$, and
$$Xv = \frac{\mathrm{d}}{\mathrm{dt}} \left(\exp(tX)\right)|_{t=0}$$
for all $x \in \mathfrak{k}$, the Lie algebra of K, for all $v \in V$.
2. For all $v \in V$, the K-translates of v span a finite-dimensional vector space.

Given any irreducible admissible representation π of G, the space of K-finite vectors is a $(\mathfrak{g}, K)$-module. As such, we will sometimes make reference to representations of G as $(\mathfrak{g}, K)$-modules, implicitly meaning the corresponding space of K-finite vectors.

The condition of K-finiteness implies that a $(\mathfrak{g}, K)$-module V admits a decomposition into finite-dimensional irreducible representations of K. We say that V is *admissible* if every isomorphism class of representations of K occurs with finite multiplicity in any such decomposition.

As in the non-archimedean case, we can define a principal series $B(\chi_1, \chi_2)$, where χ_1 and χ_2 are two (not necessarily unitary) characters of F_v, and once again all irreducible admissible $(\mathfrak{g}, K)$-modules arise from these principal series. However, the classification of these representations differs, and so we shall briefly discuss it.

It turns out that the irreducible admissible $(\mathfrak{g}, K)$-modules are characterized by the irreducible representations of the subgroup K_0 of K, given by

$$K_0 = \begin{cases} \mathrm{SO}(2); & \text{if } K = \mathrm{O}(2), \\ \mathrm{SU}(2); & \text{if } K = \mathrm{U}(2). \end{cases}$$

To begin with, we consider the case in which $F_v \simeq \mathbb{R}$. The irreducible representations of $\mathrm{SO}(2)$ take the form

$$\rho_n : \mathrm{SO}(2) \to \mathbb{C}^\times, \ \rho_n(k_\theta) = e^{in\theta},$$

where $K_\theta \in \mathrm{SO}(2)$ corresponds to an anticlockwise rotation through an angle θ. Using the Iwasawa decomposition $\mathrm{GL}_2(\mathbb{R}) = B \cdot \mathrm{SO}(2)$, we can define a function $\phi_n \in B(\chi_1, \chi_2)$ by

$$\phi_n \left(\begin{pmatrix} a_1 & x \\ 0 & a_2 \end{pmatrix} k_\theta \right) = \chi_1(a_1)\chi_2(a_2) \left| \frac{a_1}{a_2} \right|^{\frac{1}{2}} e^{in\theta}.$$

The functions ϕ_n span $B(\chi_1, \chi_2)$, and so we can define the irreducible admissible representations of $\mathrm{GL}_2(\mathbb{R})$ in terms of them. In fact, we have the following classification (see **[JL70], Theorem 5.11**):

Theorem 3.2.4. *Let χ_1 and χ_2 be two characters of $\mathbb{R}^\times$.*

(i) *If $\chi_1\chi_2^{-1}$ is not of the form $x \mapsto x^r\mathrm{sgn}(x)$, where r a non-zero integer, then the representation $B(\chi_1, \chi_2)$ is irreducible, and we denote by $\pi(\chi_1, \chi_2)$ any $(\mathfrak{g}, K)$-module equivalent to $B(\chi_1, \chi_2)$.*

(ii) *If $\chi_1\chi_2^{-1}(x) = x^r\mathrm{sgn}(x)$, where r is a positive integer, then the space $B(\chi_1, \chi_2)$ contains an infinite-dimensional irreducible subrepresentation, $B_s(\chi_1, \chi_2)$, spanned by the functions*

$$\{\ldots, \phi_{-r-3}, \phi_{-r-1}, \phi_{r+1}, \phi_{r+3}, \ldots\}.$$

The quotient, $B_f(\chi_1, \chi_2) := B(\chi_1, \chi_2)/B_s(\chi_1, \chi_2)$, is finite-dimensional. We denote by $\pi(\chi_1, \chi_2)$ and $\sigma(\chi_1, \chi_2)$ any $(\mathfrak{g}, K)$-modules equivalent to $B_f(\chi_1, \chi_2)$ and $B_s(\chi_1, \chi_2)$ respectively.

(iii) *If $\chi_1\chi_2^{-1}(x) = x^r\mathrm{sgn}(x)$, where r is a negative integer, then the space $B(\chi_1, \chi_2)$ contains a finite-dimensional irreducible subrepresentation, $B_f(\chi_1, \chi_2)$, spanned by the functions*

$$\{\phi_{r+1}, \ldots, \phi_{-r-1}\}.$$

The quotient, $B_s(\chi_1, \chi_2) := B(\chi_1, \chi_2)/B_f(\chi_1, \chi_2)$, is infinite-dimensional. We denote by $\pi(\chi_1, \chi_2)$ and $\sigma(\chi_1, \chi_2)$ any $(\mathfrak{g}, K)$-modules equivalent to $B_f(\chi_1, \chi_2)$ and $B_s(\chi_1, \chi_2)$ respectively.

(iv) *Any irreducible admissible $(\mathfrak{g}, K)$-module is equivalent to $\pi(\chi_1, \chi_2)$ or $\sigma(\chi_1, \chi_2)$ for some characters χ_1 and χ_2 of $\mathbb{R}^\times$.*

Recall that when we say a $(\mathfrak{g}, K)$-module is equivalent to a representation of $\mathrm{GL}_2(\mathbb{R})$, we really mean that it is equivalent to the $(\mathfrak{g}, K)$-module arising by considering the K-finite vectors of the representation. In keeping with the notation established in the non-archimedean setting, we have denoted by π any irreducible principal series or finite-dimensional representation, and by σ any of the remaining infinite-dimensional representations, which are known as *discrete series* representations. The *weight* of a discrete series is the integer $r+1$, where

$$\chi_1\chi_2^{-1}(x) = x^r\mathrm{sgn}(x).$$

The complex case is similar, but now we have to utilise the irreducible representations of SU(2). Unlike those of SO(2), these are not one-dimensional; rather, there is a unique irreducible representation of degree $n+1$ for each positive integer n, which we denote by ρ_n. This can be realised by the action of SU(2) on the space of homogeneous polynomials of degree n in two variables with complex coefficients, given by

$$\begin{pmatrix} \alpha & \beta \\ -\overline{\beta} & \overline{\alpha} \end{pmatrix} f(X,Y) = f(\overline{\alpha}X - \beta Y, \overline{\beta}X + \alpha Y), \quad \begin{pmatrix} \alpha & \beta \\ -\overline{\beta} & \overline{\alpha} \end{pmatrix} \in \mathrm{SU}(2).$$

For each n, let $B(\chi_1, \chi_2, \rho_n)$ denote the set of functions in $B(\chi_1, \chi_2)$ which transform according to ρ_n (where again we use the Iwasawa decomposition $\mathrm{GL}_2(\mathbb{C}) = B \cdot \mathrm{SU}(2)$). Then we have the following classification (see **[JL70], Theorem 6.2**):

Theorem 3.2.5. *Let χ_1 and χ_2 be two characters of $\mathbb{C}^\times$.*

(i) *If $\chi_1\chi_2^{-1}$ is not of the form $z \mapsto z^p\overline{z}^q$ or $z \mapsto z^{-p}\overline{z}^{-q}$ for integers $p, q \geq 1$ then $B(\chi_1, \chi_2)$ is irreducible, and we denote by $\pi(\chi_1, \chi_2)$ any $(\mathfrak{g}, K)$-module equivalent to $B(\chi_1, \chi_2)$.*

(ii) *If $\chi_1\chi_2^{-1}(z) = z^p\overline{z}^q$, with $p, q \geq 1$, then the space $B(\chi_1, \chi_2)$ contains an infinite-dimensional irreducible subrepresentation, $B_s(\chi_1, \chi_2)$, defined by*

$$B_s(\chi_1, \chi_2) = \sum_{\substack{n \geq p+q \\ n \equiv p+q \pmod 2}} B(\chi_1, \chi_2, \rho_n).$$

The quotient, $B_f(\chi_1, \chi_2) := B(\chi_1, \chi_2)/B_s(\chi_1, \chi_2)$, is finite-dimensional. We denote by $\pi(\chi_1, \chi_2)$ and $\sigma(\chi_1, \chi_2)$ any $(\mathfrak{g}, K)$-modules equivalent to $B_f(\chi_1, \chi_2)$ and $B_s(\chi_1, \chi_2)$ respectively.

(iii) *If $\chi_1\chi_2^{-1}(z) = z^{-p}\overline{z}^{-q}$ with $p, q \geq 1$, then the space $B(\chi_1, \chi_2)$ contains a finite-dimensional irreducible subrepresentation, $B_f(\chi_1, \chi_2)$, defined by*

$$B_f(\chi_1, \chi_2) = \sum_{\substack{|p-q| \leq n < p+q \\ n \equiv p+q \pmod 2}} B(\chi_1, \chi_2, \rho_n).$$

The quotient, $B_s(\chi_1, \chi_2) := B(\chi_1, \chi_2)/B_f(\chi_1, \chi_2)$, is infinite-dimensional. We denote by $\pi(\chi_1, \chi_2)$ and $\sigma(\chi_1, \chi_2)$ any $(\mathfrak{g}, K)$-modules equivalent to $B_f(\chi_1, \chi_2)$ and $B_s(\chi_1, \chi_2)$ respectively.

(iv) *Any irreducible admissible $(\mathfrak{g}, K)$-module is equivalent to $\pi(\chi_1, \chi_2)$ or $\sigma(\chi_1, \chi_2)$ for some characters χ_1 and χ_2 of $\mathbb{C}^\times$.*

Finally, we can return to the global theory. Once again, let F be a number field, and set G to be the $\mathbb{Q}$-group $\mathrm{Res}_{F/\mathbb{Q}}(\mathrm{GL}_2)$. Let $\mathbb{A}_f$ denote the *finite* adeles (i.e., the restriction of the adeles to the non-archimedean places), so that

$$G(\mathbb{A}_f) \simeq \prod_{\substack{v|p \\ p \text{ prime}}} \mathrm{GL}_2(F_v),$$

let $\mathfrak{g}$ denote the Lie algebra of $G(\mathbb{R})$, and let $K_\infty = \mathrm{O}(2)^r \times \mathrm{U}(2)^s$, where F has r real and s pairs of complex conjugate embeddings.

We define a $(\mathfrak{g}, K_\infty)\times G(\mathbb{A}_f)$-module (π, V_π) to be a $(\mathfrak{g}, K_\infty)$-module equipped with a smooth action of $G(\mathbb{A}_f)$ (in the sense that every vector $v \in V$ is fixed by a compact open subgroup of $G(\mathbb{A}_f)$) such that the actions of $(\mathfrak{g}, K_\infty)$ and $G(\mathbb{A}_f)$ commute.

We say that a $(\mathfrak{g}_\infty, K_\infty) \times G(\mathbb{A}_f)$-module (π, V_π) is *irreducible* if it has no proper subspaces preserved by the actions of $\mathfrak{g}$, K_∞ and $G(\mathbb{A}_f)$, and that it is *admissible* if the multiplicity of every irreducible representation of the compact open subgroup $K_\infty \times \prod \mathrm{GL}_2(\mathcal{O}_v)$ in V is finite.

It is known (see **[Kud04], Theorem 2.5**), that *any* irreducible admissible $(\mathfrak{g}, K_\infty) \times G(\mathbb{A}_f)$-module π takes the form $\pi = \otimes \pi_v$, where we run over all places v, and where each π_v is either a representation of $\mathrm{GL}_2(F_v)$ (if v is a non-archimedean place of F) or a $(\mathfrak{g}, K)$-module for $\mathrm{GL}_2(\mathbb{R})$ or $\mathrm{GL}_2(\mathbb{C})$ (if v is a real or complex place of F) such that all but finitely many of the π_v are unramified.

The following result (see, for example, **[Kud04], Theorem 2.6**) justifies our interest in these objects:

Theorem 3.2.6.

(i) *The space $\mathcal{A}_0(G(\mathbb{Q})\backslash G(\mathbb{A}), \omega)$ decomposes as an algebraic direct sum*

$$\mathcal{A}_0(G(\mathbb{Q})\backslash G(\mathbb{A}), \omega) = \bigoplus_{(\pi, V_\pi)} m_\pi V_\pi,$$

where the sum runs over all irreducible admissible $(\mathfrak{g}, K_\infty)\times G(\mathbb{A}_f)$-modules (π, V_π), and the m_π are non-negative integers.

(ii) (*Strong Multiplicity One*) *Each irreducible admissible $(\mathfrak{g}, K_\infty) \times G(\mathbb{A}_f)$-module appears in the above decomposition with multiplicity at most one (that is, the integers $m_\pi \in \{0, 1\}$ for all (π, V_π)). Moreover, if (π_1, V_{π_1}) and (π_2, V_{π_2}) are two admissible $(\mathfrak{g}, K_\infty) \times G(\mathbb{A}_f)$-modules appearing in the above decomposition, with $\pi_1 = \otimes \pi_{1,v}$ and $\pi_2 = \otimes \pi_{2,v}$, such that $\pi_{1,v}$ and $\pi_{2,v}$ are equivalent for all but finitely many places v, then $V_{\pi_1} = V_{\pi_2}$.*

Thus we can better understand automorphic forms through the study of $(\mathfrak{g}, K_\infty) \times G(\mathbb{A}_f)$-modules. Any irreducible admissible $(\mathfrak{g}, K_\infty) \times G(\mathbb{A}_f)$-module which appears as a summand in $\mathcal{A}_0(G(\mathbb{Q})\backslash G(\mathbb{A}), \omega)$ with multiplicity one is known as a *cuspidal automorphic representation* (with central character ω). It is known (see for example **[Bum98], Chapter 3.5, p. 332**) that, given a cuspidal automorphic representation π, the representations π_v at the unramified non-archimedean places are all irreducible principal series.

Returning once again to the classical situation, let $f \in \mathcal{S}_k(N)$ be a cusp form of weight k and level N, which we suppose is an eigenform for the Hecke operators T_p with p not dividing N. We have seen that the corresponding automorphic form φ_f of level $K_0(N)$ and trivial character is also an eigenform for the operators T_p (realized adelically). Moreover, we have the following result (see, for example, **[Bum98], Theorem 3.6.1**):

Proposition 3.2.7. *If $f \in \mathcal{S}_k(N)$ is an cuspidal eigenform for the Hecke operators T_p, with p not dividing N, then φ_f lies in an irreducible subspace of $\mathcal{A}_0(\mathrm{GL}_2(\mathbb{Q})\backslash \mathrm{GL}_2(\mathbb{A}), \mathbf{1})$ of automorphic forms with trivial central character, and thus corresponds to an automorphic representation π_f.*

Now, since φ_f is an eigenform for the Hecke operators, we know that

$$T_p(\varphi_f) = a_p(f)\varphi_f,$$

where $a_p(f)$ is the eigenvalue of f with respect to T_p, for a prime p not dividing N. Moreover, since φ_f is of level $K_0(N)$, and $K_p(N) = \mathrm{GL}_2(\mathbb{Z}_p)$ if p does not divide N, it is clear that the components $\pi_{f,p}$ are unramified at such primes. They therefore take the form of an unramified principal series $\pi_{f,p}(\chi_1, \chi_2)$ for some pair of characters χ_1, χ_2, for which we have seen that the space of $K_p(N)$-fixed vectors is one-dimensional, on which the Hecke operator T_p acts as multiplication by the scalar

$$\theta(T_p) = p^{\frac{1}{2}} \mathrm{Tr}(t_{\pi_{f,p}}),$$

where $t_{\pi_{f,p}}$ is the Langlands parameter of $\pi_{f,p}$.

Thus

$$a_p(f) = p^{\frac{1}{2}} \mathrm{Tr}(t_{\pi_{f,p}}),$$

and we may henceforth restrict our attention solely to automorphic representations, safe in the knowledge that the arithmetic information we covet is preserved.

3.3 The Local Langlands Correspondence

Having introduced automorphic representations as a generalization of classical modular forms, we would like to discuss the Galois representations attached to them. Unfortunately, this is not as straightforward as the classical case - indeed, in general it is not known how to construct such representations. What one *can* say is what behaviour we would expect the Galois representation attached to an automorphic representation to exhibit, which is what we aim to describe in this section.

As before, let F be a number field, and $G = \mathrm{Res}_{F/\mathbb{Q}}(\mathrm{GL}_2)$. Given an ℓ-adic Galois representation

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

one can define local representations

$$\rho_v : \mathrm{Gal}(\overline{F}_v/F_v) \to \mathrm{GL}_2(\overline{\mathbb{Q}}_\ell)$$

for each place v by composing ρ with the natural map (up to conjugation) $\mathrm{Gal}(\overline{F}_v/F_v) \to \mathrm{Gal}(\overline{F}/F)$.

Now, given a cuspidal automorphic representation $\pi = \otimes \pi_v$ of $G(\mathbb{A})$, there is a well-defined notion of what it means for a local Galois representation ρ_v to be attached to the admissible representation π_v (which we shall explain in more detail later). Our hope, therefore, is that given π, one can find a *global* representation ρ such that the local representations ρ_v are attached to the local components π_v in this manner (at least for all but finitely many primes). In a later section, we shall describe a result proving the existence of such a ρ for certain number fields F (with appropriate conditions on the automorphic representation π), but for now we shall make the correspondence between local representations more explicit (for a more detailed reference, see **[Cog04]**).

Let v be a non-archimedean place of F, and let I_v and Frob_v denote the inertia subgroup and a geometric Frobenius element of $\mathrm{Gal}(\overline{F}_v/F_v)$ respectively. Define the *Weil group* W_v to be the subgroup of $\mathrm{Gal}(\overline{F}_v/F_v)$ generated by Frob_v and I_v; this can be seen to have dense image in $\mathrm{Gal}(\overline{F}_v/F_v)$. We have a valuation map

$$v : W_v \to \mathbb{Z},\ v(\mathrm{Frob}_v^r x) = r \text{ for all } r \in \mathbb{Z},\ x \in I_v,$$

and consequently define a map

$$\|\cdot\| : W_v \to F_v, w \mapsto q^{-v(w)},$$

where the residue field of F_v has cardinality q.

Any representation of $\mathrm{Gal}(\overline{F}_v/F_v)$ immediately gives rise to a representation of W_v, and much of the information we are interested in is preserved under this

correspondence (since it is linked to the geometric Frobenius). We can extend W_v to a group scheme W_v', known as the *Weil-Deligne group*, defined by setting

$$W_v' = W_v \ltimes \mathbb{G}_a,$$

where W_v acts on the additive group $\mathbb{G}_a$ via

$$wxw^{-1} = \|w\| x.$$

The main reason for studying the Weil-Deligne group is that its representation theory is simpler: effectively it allows us to ignore the topology of the target field. To expand on this, we define a representation ρ' of W_v' to be a pair (ρ, N), where

$$\rho : W_v \to \mathrm{GL}(V)$$

is a homomorphism from W_v to the group of automorphisms of an n-dimensional vector space V, which is continuous with respect to the *discrete* topology on V (i.e., the kernel of ρ contains an open subgroup of I_v) and N is a nilpotent endomorphism of V such that

$$\rho(w) N \rho(w)^{-1} = \|w\| N$$

for all $w \in W_k$.

We call a representation ρ' of W_v' *irreducible* if the corresponding representation ρ of W_v is. Note that, being nilpotent, N has non-trivial kernel, and that this kernel is a ρ-invariant subspace of V. Thus for any irreducible representation of W_v', we must have $N = 0$, and so irreducible representations of W_v' simply correspond to irreducible representations of W_v that are continuous with respect to the discrete topology on V.

We call a representation ρ' of W_v' *Frobenius semisimple* if the representation ρ of W_v is semisimple (that is, a direct sum of irreducible representations). Any representation ρ' has a canonical Frobenius semisimplification ρ'_{Frob}, which we define as follows: given a lift ϕ of Frob_v to W_v, we can decompose $\rho(\phi)$ as a product $\Phi_u \Phi_s = \Phi_s \Phi_u$, where Φ_u is unipotent and Φ_s semisimple (that is, every Φ_s-invariant subspace of the vector space V has a Φ_s-invariant complement). We obtain ρ'_{Frob} by leaving N and $\rho|_{I_v}$ unchanged, and replacing $\rho(\mathrm{Frob}_v)$ with Φ_s.

For our purposes, we will choose the vector space V to be defined over either $\overline{\mathbb{Q}}_\ell$ or $\mathbb{C}$. In fact, since the definition of a representation of W_v' makes no mention of the topology on V, any choice of isomorphism $\overline{\mathbb{Q}}_\ell \simeq \mathbb{C}$ gives rise to an identification between ℓ-adic and complex representations of W_v', so for practical purposes we consider only the latter. Moreover, when considering *irreducible* representations, we can restrict ourselves to complex representations of the Weil group W_v.

With these ideas in place, one can easily define the local L-factor attached to a Frobenius semisimple representation $\rho' = (\rho, N)$ of W_v'. To do this, define V_N to be the subspace of $\ker(N)$ fixed by the action of I_v under ρ. We then set

$$L(s, \rho) = \det(1 - q^{-s}\rho(\mathrm{Frob}_v)|V_N)^{-1},$$

where we recall that q is the cardinality of the residue field of F_v.

We shall omit a discussion of the archimedean places, as these will not play a prominent role in our work. It turns out that the irreducible admissible representations of $\mathrm{GL}_2(F_v)$ and the irreducible representations of the Weil-Deligne group W_v' are closely linked:

Theorem 3.3.1. *Let v be a non-archimedean place of F. Then there is a bijection between the 2-dimensional irreducible admissible representations of $\mathrm{GL}_2(F_v)$ and the 2-dimensional representations of W_v'.*

We denote the image of an irreducible admissible representation π_v under this correspondence by ρ_{π_v}. One can show that if π_v is an unramified principal series $\pi_v = \pi(\chi_1, \chi_2)$, then ρ_{π_v} is the direct sum $\widetilde{\chi_1} \oplus \widetilde{\chi_2}$ of unramified characters, where $\widetilde{\chi}_i(\mathrm{Frob}_v) = \chi_i(\varpi)$, for a uniformiser ϖ of F_v. With this in mind, it is straightforward to see that we have an equivalence of local L-factors

$$L(s, \pi_v) = L(s, \rho_{\pi_v}).$$

In particular, we note that

$$\mathrm{Tr}(\rho_{\pi_v}(\mathrm{Frob}_v)) = \mathrm{Tr}(t_{\pi_v}),$$

where t_{π_v} denotes the Langlands class of π_v.

We now return to the global situation. As mentioned previously, a global Galois representation ρ gives rise to a local Galois representation ρ_v for each non-archimedean place v, which in turn gives rise to a representation of the Weil group W_v. If this is irreducible, then it corresponds to a representation of the Weil-Deligne group W_v', which we denote by $\mathrm{WD}(\rho_v)$. By fixing an isomorphism $\iota : \overline{\mathbb{Q}}_\ell \to \mathbb{C}$ if necessary, we will always assume that $\mathrm{WD}(\rho_v)$ is a complex representation.

Now, given a cuspidal automorphic representation $\pi = \otimes\pi_v$, we will say that a Galois representation ρ is *attached* to π if, for all but finitely many places v of F, we have

$$\mathrm{WD}(\rho_v) \simeq \mathscr{L}_v(\pi_v),$$

where $\mathscr{L}_v(\pi_v)$ denotes the representation of W_v' corresponding to π_v under **Theorem 3.3.1**.

We shall soon give an explicit example of a class of automorphic representations to which we can attach Galois representations. These representations will be connected to the cohomology of certain arithmetic groups, and so we shall begin with a discussion of precisely what this means.

3.4 Automorphic Representations and Cohomology

We now discuss the promised generalization of the Eichler-Shimura isomorphism. As before, fix a number field F, with ring of integers $\mathcal{O}_F$, and let G denote the $\mathbb{Q}$-group $\mathrm{Res}_{F/\mathbb{Q}}(\mathrm{GL}_2)$. The group cohomology of G can be decomposed into two summands - the *cuspidal* and *Eisenstein* cohomology of G, the former of which is connected to cuspidal automorphic representations for G, and is our main object of interest. We shall give a more detailed description of this cuspidal cohomology in the following exposition, which follows the spirit of Joachim Schwermer's treatment in **[Sch06]**.

Before proceeding further, we establish some notation. Let $\mathbb{A}$ denote the ring of adeles over the rationals, which we decompose into finite and infinite parts

$$\mathbb{A} = \mathbb{A}_f \times \mathbb{R}$$

as standard. If S_f and S_∞ denote the sets of finite and infinite places of F respectively, then we obtain a similar decomposition

$$\mathrm{G}(\mathbb{A}) = \mathrm{G}(\mathbb{A}_f) \times \mathrm{G}(\mathbb{R}) \simeq \prod_{v \in S_f}{}' \mathrm{GL}_2(F_v) \times \prod_{v \in S_\infty} \mathrm{GL}_2(F_v),$$

where the product over the finite places S_f is restricted with respect to the subgroups $\mathrm{GL}_2(\mathcal{O}_v)$.

Noting that

$$G(\mathbb{R}) \simeq \mathrm{GL}_2(\mathbb{R})^r \times \mathrm{GL}_2(\mathbb{C})^s,$$

where the number field F has signature $[r, s]$, we fix a standard choice of compact open subgroup K_∞ of $G(\mathbb{R})$ by setting

$$K_\infty = \mathrm{O}(2)^r \times \mathrm{U}(2)^s.$$

We shall not yet specify a compact open subgroup K_f of $G(\mathbb{A}_f)$, instead we shall simply state that all such subgroups under our consideration will be of the form

$$K_f = \prod_{v \in S_f}{}' K_v,$$

where K_v is a compact subgroup of $\mathrm{GL}_2(F_v)$, which we take to be $\mathrm{GL}_2(\mathcal{O}_v)$ for all but finitely many places $v \in S_f$.

Let A_G denote the maximal $\mathbb{Q}$-split torus in the centre of G, which can be identified with the multiplicative $\mathbb{Q}$-group $\mathbb{G}_m$. Moreover, let $A_G(\mathbb{R})$ denote the set of real points of A_G, and $A_G^0(\mathbb{R})$ the connected component of $A_G(\mathbb{R})$ containing the identity, so that $A_G^0(\mathbb{R}) \simeq \mathbb{R}_+$, embedded diagonally into the components of $G(\mathbb{R})$ (we refer to $A_G^0(\mathbb{R})$ as the *split component* of G).

Recall from **Section 3.1** that we have an identification

$$\Gamma_0(N)\backslash \mathrm{SL}_2(\mathbb{R}) \simeq \mathrm{GL}_2(\mathbb{Q})\backslash \mathrm{GL}_2(\mathbb{A})/A_G^0(\mathbb{R})K_0(N),$$

and thus can identify the open modular curve $Y_0(N)$ with the double coset space

$$\mathrm{GL}_2(\mathbb{Q})\backslash \mathrm{GL}_2(\mathbb{A})/A_G^0(\mathbb{R})K_\infty K_0(N),$$

where $K_\infty = \mathrm{SO}(2)$. Motivated by this, we would like to consider spaces of the form

$$X_{K_f} := G(\mathbb{Q})\backslash G(\mathbb{A})/A_G^0(\mathbb{R})K_\infty K_f$$

for various choices of compact open subgroup $K_f \subset G(\mathbb{A}_f)$.

We shall be interested in cohomology with trivial coefficients (in keeping with the classical connection between elliptic curves and modular forms of weight 2). Given a compact subgroup K_f, we define the de Rham complex $\Omega(X_{K_f}, \mathbb{C})$ to be the complex of smooth, complex-valued differential forms on X_{K_f}, and let $H^*(X_{K_f}, \mathbb{C})$ denote the cohomology of $\Omega(X_{K_f}, \mathbb{C})$.

While we will be interested in spaces X_{K_f} for a specific choice of K_f, it is useful at first to consider all such subgroups at once by means of a direct limit over the cohomology groups $H^*(X_{K_f}, \mathbb{C})$. Explicitly, given a second compact subgroup K_f' of $G(\mathbb{A})$, with $K_f' \subset K_f$, we obtain an inclusion $H^*(X_{K_f}, \mathbb{C}) \hookrightarrow H^*(X_{K_f'}, \mathbb{C})$, thus forming a directed system of cohomology groups. We denote the direct limit by

$$H^*(G, \mathbb{C}) = \varinjlim_{K_f} H^*(X_{K_f}, \mathbb{C}).$$

We note that $H^*(G, \mathbb{C})$ admits a natural $G(\mathbb{A}_f)$-module structure, induced by the natural map $g : X_{K_f} \to X_{g^{-1}K_f g}$ for $g \in G(\mathbb{A}_f)$. Thus, given a particular compact subgroup $K_f \subset G(\mathbb{A}_f)$, one may recover the cohomology of X_{K_f} simply by taking K_f-invariants.

Now, let M_G denote the connected component of the intersection of the kernels of all $\mathbb{Q}$-rational characters of G, and $\mathfrak{m}_G$ the corresponding Lie algebra of $M_G(\mathbb{R})$. Denoting by $\mathfrak{g}$ and $\mathfrak{a}_G$ the Lie algebras of $G(\mathbb{R})$ and $A_G^0(\mathbb{R})$ respectively, we have a decomposition

$$\mathfrak{g} = \mathfrak{a}_G \oplus \mathfrak{m}_G,$$

and so we can view $\mathfrak{m}_G$ as the Lie algebra of $A_G^0(\mathbb{R})\backslash G(\mathbb{R})$.

For ease of notation, write $\mathcal{A}(G)$ and $\mathcal{A}_0(G)$ for the spaces $\mathcal{A}_(G(\mathbb{Q})\backslash G(\mathbb{A}), \mathbf{1})$ and $\mathcal{A}_0(G(\mathbb{Q})\backslash G(\mathbb{A}), \mathbf{1})$ of automorphic (respectively cuspidal automorphic) forms for G with trivial central character (in which we run through *all* possible compact subgroups K_f). Then we have an isomorphism of $G(\mathbb{A}_f)$-modules:

$$H^*(G, \mathbb{C}) \simeq H^*(\mathfrak{m}_G, K_\infty;\ \mathcal{A}(G)),$$

where the cohomology on the right-hand side is the relative Lie algebra cohomology with respect to $(\mathfrak{m}_G, K_\infty)$ (see, for example, **[Sch06], Section 3.2**).

There is a decomposition

$$H^*(G, \mathbb{C}) = H^*_{\text{Eis}}(G, \mathbb{C}) \oplus H^*_{\text{cusp}}(G, \mathbb{C})$$

of $H^*(G, \mathbb{C})$ into *Eisenstein* and *cuspidal cohomology*, where

$$H^*_{\text{cusp}}(G, \mathbb{C}) \simeq H^*(\mathfrak{m}_G, K_\infty;\ \mathcal{A}_0(G)).$$

We are primarily interested in the cuspidal cohomology, but we briefly mention that the Eisenstein cohomology can be thought of as being connected to automorphic forms for parabolic subgroups of G (i.e., it arises from subgroups of G of strictly smaller rank).

Since we are concerned with the cuspidal cohomology $H^*_{\text{cusp}}(G, \mathbb{C})$, we would like to understand more about its structure. Given a cuspidal automorphic representation π, let $V_\pi = V_{\pi_\infty} \otimes V_{\pi_f}$ denote the $(\mathfrak{g}, K_\infty) \times G(\mathbb{A}_f)$-module associated with the representation π. Then we have a decomposition of $\mathrm{G}(\mathbb{A}_f)$-modules

$$H^*_{\text{cusp}}(G, \mathbb{C}) = \bigoplus_\pi H^*(\mathfrak{m}_G, K_\infty; V_{\pi_\infty}) \otimes V_{\pi_f},$$

where the sum ranges over those cuspidal automorphic subrepresentations of the space $\mathcal{A}(G)$ (see **[Sch06], Theorem 4.1**).

In particular, fixing a compact open subgroup K_f and taking K_f-invariants, we find that

$$H^*_{\text{cusp}}(X_{K_f}, \mathbb{C}) = \bigoplus_\pi H^*(\mathfrak{m}_G, K_\infty; V_{\pi_\infty}) \otimes V_{\pi_f}^{K_f},$$

where now the sum is restricted to those cuspidal automorphic representations *of level* K_f of the space $\mathcal{A}_0(G)$.

For our purposes, we will say that a cuspidal automorphic representation π is *of cohomological type* and *weight two* if the summand $H^*(\mathfrak{m}_G, K_\infty; V_{\pi_\infty})$ is non-zero. Higher weight representations correspond to non-trivial coefficient systems in the cohomology.

As in the classical case, the cohomology $H^*(X_{K_f}, \mathbb{C})$ admits a Hecke action. Indeed, let $K = K_f$, and choose $g \in G(\mathbb{A}_f)$ such that each of the subgroups $K_1 := K \cap g^{-1}Kg$ and $K_2 := K \cap gKg^{-1}$ have finite index in K. Then the Hecke correspondence

$$\begin{array}{ccc} K_1 & \xrightarrow{\alpha_{g_f}} & K_2 \\ {\scriptstyle \iota_1}\downarrow & & \downarrow{\scriptstyle \iota_2} \\ K & & K \end{array}$$

from **Section 3.1** induces a correspondence on the cohomology groups

$$\begin{array}{ccc} H^*(X_{K_1}, \mathbb{C}) & \xrightarrow{\alpha_{g_f,*}} & H^*(X_{K_2}, \mathbb{C}) \\ \uparrow{\scriptstyle \iota_1^*} & & \downarrow{\scriptstyle \iota_{2,*}} \\ H^*(X_K, \mathbb{C}) & & H^*(X_K, \mathbb{C}) \end{array}$$

via the action on the corresponding de Rham complexes. We shall not give an explicit computation here, rather we shall wait until later, when we have shaped the cohomology into a more computationally accessible form.

We will make one final observation regarding the action of Hecke operators on cohomology. Suppose first that we restrict to cohomology with *rational* coefficients. According to **[Har06], Chapter 2, Proposition 2.2**, $H^*(G, \mathbb{Q})$ is a $G(\mathbb{A}_f)$-module, and by taking K_f-coinvariants we obtain the rational cohomology groups $H^*(X_{K_f}, \mathbb{Q})$, on which the Hecke operators act as defined previously. Crucially, it can be shown that the rational cuspidal cohomology in fact generates the complex vector space $H^*_{\text{cusp}}(X_{K_f}, \mathbb{C})$, and so in particular the action of the Hecke operators on cuspidal cohomology groups can be defined rationally. We will bear this in mind for future reference.

While we do not have an explicit description of the $(\mathfrak{m}_G, K_\infty)$-cohomology appearing in the decomposition of $H^*_{\text{cusp}}(X_{K_f}, \mathbb{C})$, we can at least state a result concerning the degrees in which we can have non-vanishing cuspidal cohomology. Indeed, let X denote the symmetric space

$$X = G(\mathbb{R})/A_G^0(\mathbb{R})K_\infty,$$

and let $\ell_0(G) = \text{rk}(\mathfrak{g}) - \text{rk}(\mathfrak{k}) - 1$, where $\mathfrak{g}$ and $\mathfrak{k}$ denote the Lie algebras of the (real) Lie groups $G(\mathbb{R})$ and K_∞ respectively (here the rank of a real Lie algebra is given by the dimension of a Cartan subalgebra). Then we have the following result:

Proposition 3.4.1.

$$H^i_{\text{cusp}}(G, \mathbb{C}) = 0 \text{ if } i \notin \left[\frac{1}{2}(\dim(X) - \ell_0(G)), \frac{1}{2}(\dim(X) + \ell_0(G))\right].$$

This is similar to, but differs slightly from, **[Sch06], Theorem 6.2**, in that the result there allows arbitrary coefficient systems, and makes no mention of the split component $A_G^0(\mathbb{R})$. Justification for this result can be found on page 34 of **[Gun11]**.

For our example, in which $G = \mathrm{Res}_{F/\mathbb{Q}}(\mathrm{GL}_2)$, we can give a simple formula for the degrees in which the cuspidal cohomology is non-vanishing. As before, let F have signature $[r, s]$, so that

$$G(\mathbb{R}) \simeq \mathrm{GL}_2(\mathbb{R})^r \times \mathrm{GL}_2(\mathbb{C})^s,$$

and

$$K_\infty \simeq \mathrm{O}(2)^r \times \mathrm{U}(2)^s.$$

In the next chapter, we shall see that the dimension of the symmetric space X is given by

$$\dim(X) = 3r + 4s - 1,$$

which makes use of the identifications

$$\mathrm{SL}_2(\mathbb{R})/\mathrm{SO}(2) \simeq \mathfrak{h}_2 \text{ and } \mathrm{SL}_2(\mathbb{C})/\mathrm{SU}(2) \simeq \mathfrak{h}_3,$$

where $\mathfrak{h}_2$ and $\mathfrak{h}_3$ denote hyperbolic 2- and 3-space respectively.

To work out the value $\ell_0(G)$, we note that the Lie algebras $\mathfrak{gl}_2(\mathbb{R})$ and $\mathfrak{gl}_2(\mathbb{C})$ comprise all 2×2 real (respectively complex) matrices, while $\mathfrak{o}(2)$ and $\mathfrak{u}(2)$ comprise all 2×2 real skew-symmetric (respectively complex skew-hermitian) matrices. For each of the above, with the exception of $\mathfrak{o}(2)$, the subalgebra of all diagonal matrices is a Cartan subalgebra, while $\mathfrak{o}(2)$ is a 1-dimensional (and thus abelian) Lie algebra. Thus

$$\mathrm{rk}(\mathfrak{g}) = \begin{cases} 2; & \text{if } \mathfrak{g} = \mathfrak{gl}_2(\mathbb{R}), \\ 4; & \text{if } \mathfrak{g} = \mathfrak{gl}_2(\mathbb{C}), \\ 1; & \text{if } \mathfrak{g} = \mathfrak{o}(2), \\ 2; & \text{if } \mathfrak{g} = \mathfrak{u}(2), \end{cases}$$

and so

$$\ell_0(G) = r + 2s - 1.$$

Combining this information, we have the following result:

Corollary 3.4.2. *Let $G = \mathrm{Res}_{F/\mathbb{Q}}(\mathrm{GL}_2)$, where F is a number field with signature $[r, s]$. Then $H^i(G, \mathbb{C})$ is non-zero only if*

$$i \in [r + s, 2r + 3s - 1].$$

3.5 A Global Langlands Correspondence

We now give the promised example of a Galois representation attached to a cuspidal automorphic representation, as presented by C.P. Mok in **[Mok14]**, which will form the basis for our later study. While Mok's result is more general, we shall restrict our attention to automorphic representations with *trivial* central character, echoing the classical treatment in which elliptic curves correspond to modular forms without character.

We begin by stating the result (an adaptation of **[Mok14], Theorem 1.1**). Recall that we say a cuspidal automorphic representation π is *of cohomological type* if it corresponds to a non-zero summand in the cohomology $H^*_{\text{cusp}}(G, \mathbb{C})$.

Theorem 3.5.1. *Let F be a CM field, and let π be a cuspidal automorphic representation of $\mathrm{Res}_{F/\mathbb{Q}}(\mathrm{GL}_2)$ of cohomological type, with trivial central character, and fix a prime ℓ. Then there exists an ℓ-adic Galois representation*

$$\rho_\pi : \mathrm{Gal}(\overline{F}/F) \to \mathrm{GL}_2(\overline{\mathbb{Q}}_\ell)$$

such that, for each place v of F not dividing ℓ, we have the local-to-global compatibility statement, up to semisimplification:

$$\mathrm{WD}(\rho_{\pi,v})^{ss} \simeq \mathscr{L}_v(\pi_v \otimes |\det|_v^{-\frac{1}{2}})^{ss}.$$

Furthermore, if π_v is not a twist of Steinberg (e.g., is an unramified principal series) then we have the full local-to-global compatibility statement, up to Frobenius semisimplification:

$$\mathrm{WD}(\rho_{\pi,v})_{\mathrm{Frob}} \simeq \mathscr{L}_v(\pi_v \otimes |\det|_v^{-\frac{1}{2}}).$$

We will require a few details regarding the representation ρ_π. Note first that for each place v at which the representation π_v is unramified, so too is the representation $\mathscr{L}_v(\pi_v \otimes |\det|_v^{-\frac{1}{2}})$. Since Frobenius semisimplification preserves the action on inertia groups, this implies that ρ is similarly unramified at these places.

Next, for each unramified place v, we have

$$\mathrm{Tr}(\mathscr{L}_v(\pi_v \otimes |\det|_v^{-\frac{1}{2}})(\mathrm{Frob}_v)) = q^{\frac{1}{2}}\mathrm{Tr}(t_{\pi_v}),$$

where q is the cardinality of the residue field of F_v, and t_{π_v} denotes the Langlands class of π_v.

In particular, suppose that φ is an automorphic form of level $K_0(\mathfrak{n})$, for some ideal $\mathfrak{n}$ of F, which is an eigenform for the Hecke operators $T_{\mathfrak{p}}$, and let π be its associated automorphic representation. If v is a place of F not dividing $\mathfrak{n}$, then the subgroup $K_v(\mathfrak{n})$ of $K_0(\mathfrak{n})$ is, by definition, the group $\mathrm{GL}_2(\mathcal{O}_v)$. Since φ is invariant under $K_0(\mathfrak{n})$, it follows that there is a non-trivial vector fixed by the action of $\mathrm{GL}_2(\mathcal{O}_v)$ under π_v (which in fact spans the one-dimensional space of $\mathrm{GL}_2(\mathcal{O}_v)$-fixed vectors, by the results of **Section 3.2**), and thus π_v is unramified. In this case, $q^{\frac{1}{2}}\mathrm{Tr}(t_{\pi_v})$ is equal to $\theta(T_v)$ as in **Section 3.2** (where we extend the notion of a Hecke operator to arbitrary fields in the obvious manner).

Finally, by **Theorem 3.3.1**, the determinant of the local Galois representation ρ_v is equivalent to $|\det|_v^{-\frac{1}{2}}$. Denoting by ϖ a uniformiser of F_v, we have

$$|\det(\varpi)|_v^{-\frac{1}{2}} = q,$$

where q is the cardinality of the residue field of F_v. Under the aforementioned correspondence, we observe that

$$\det(\rho_v(\mathrm{Frob}_v)) = q,$$

and thus the determinant of ρ_v is given by the local cyclotomic character, which we recall is the same as the determinant of the Galois representation attached to a rational elliptic curve.

Chapter 4

Koecher Theory

Motivated by the results of **Section 3.4**, we aim to study automorphic representations through the corresponding cohomology of certain symmetric spaces for the group $\mathrm{Res}_{F/\mathbb{Q}}(\mathrm{GL}_2)$, with the aim of being able to compute the data attached to the Galois representations constructed in **Section 3.5** in the case where F is a CM quartic field.

We begin by establishing the structure of the global symmetric spaces we will study in **Section 4.1**, and show that they can be realised as cones of binary Hermitian forms over the field F. Such cones are examples of *positivity domains*, and in **Section 4.2** we recall the theory of Koecher (generalising work of Voronoï) which provides us with a decomposition of such domains. In **Section 4.3** we continue our exploration of this theory by studying the *Koecher polytope*, an infinite polytope which captures the information of this decomposition in a manner that will lend itself more readily to our future calculations.

Finally, in **Sections 4.4** and **4.5** we return, armed with the knowledge of the previous sections, to our case of interest, and provide some details of the Koecher polytope specific to our global symmetric space.

4.1 A Model for the Symmetric Space of GL_2

Let F be a number field, with signature $[r, s]$ and ring of integers $\mathcal{O}_F$, and let G denote the reductive $\mathbb{Q}$-group $\mathrm{Res}_{F/\mathbb{Q}}(\mathrm{GL}_2)$, where $\mathrm{Res}_{F/\mathbb{Q}}$ denotes the Weil restriction of scalars. By the results of **Section 3.4**, we can study automorphic forms for G by instead looking at the cohomology of certain symmetric spaces

$$X_{K_f} = G(\mathbb{Q})\backslash G(\mathbb{A})/A_G^0(\mathbb{R})K_\infty K_f,$$

where $A_G^0(\mathbb{R})$ is the split component of G, and K_f is a compact open subgroup of $G(\mathbb{A}_f)$. These spaces can, in turn, be realized as quotient spaces of the globally symmetric space

$$X = G(\mathbb{R})/A_G^0(\mathbb{R})K_\infty.$$

As touched upon earlier, there is a geometric realization of this space, echoing the role of the complex upper half-plane in the theory of classical modular forms. Indeed, note that

$$G(\mathbb{R}) \simeq \mathrm{GL}_2(\mathbb{R})^r \times \mathrm{GL}_2(\mathbb{C})^s,$$

while

$$K_\infty \simeq \mathrm{O}(2)^r \times \mathrm{U}(2)^s.$$

In addition, we have identifications

$$\mathrm{GL}_2(\mathbb{R})/\mathrm{O}(2) \simeq \mathfrak{h}_2 \times \mathbb{R}_+$$

and

$$\mathrm{GL}_2(\mathbb{C})/\mathrm{U}(2) \simeq \mathfrak{h}_3 \times \mathbb{R}_+,$$

where $\mathfrak{h}_2$ and $\mathfrak{h}_3$ denote hyperbolic 2- and 3-space respectively. Recalling that $A_G^0(\mathbb{R}) \simeq \mathbb{R}_+$, we obtain the final identification

$$X \simeq \mathfrak{h}_2^r \times \mathfrak{h}_3^s \times \mathbb{R}_+^{r+s-1}.$$

We will now present an alternative description of the symmetric space X, in terms of a cone of binary Hermitian forms over F, which will have the benefit of being more amenable to computations. The field F has r real embeddings and s conjugate pairs of complex embeddings; for each conjugate pair, fix a particular embedding $F \hookrightarrow \mathbb{C}$. For each infinite place v, define

$$V_v = \begin{cases} \mathrm{Sym}_2(\mathbb{R}); & \text{if } v \text{ is real;} \\ \mathrm{Herm}_2(\mathbb{C}); & \text{if } v \text{ is complex,} \end{cases}$$

where $\mathrm{Sym}_2(\mathbb{R})$ and $\mathrm{Herm}_2(\mathbb{C})$ denote the real vector spaces of real symmetric and complex Hermitian 2×2 matrices respectively.

Define the *space of Hermitian forms over F* to be

$$\mathcal{V} = \prod_v V_v.$$

This is a real vector space, with

$$\dim_{\mathbb{R}}(\mathcal{V}) = 3r + 4s.$$

We can equip $\mathcal{V}$ with an inner product $\langle\ ,\ \rangle$ by setting

$$\langle X, Y\rangle = \sum_v c_v \mathrm{Tr}(X_v Y_v),$$

where $c_v = 1$ if v is a real place of F, and $c_v = 2$ if v is a complex place of F.

The vector space $\mathcal{V}$ admits an action of the group $G(\mathbb{R})$. Indeed, identifying $G(\mathbb{R}) \simeq \mathrm{GL}_2(\mathbb{R})^r \times \mathrm{GL}_2(\mathbb{C})^s$ via the embeddings corresponding to the infinite places of F, we have, for an arbitrary element $g = (g_v) \in G(\mathbb{R})$:

$$g \cdot X = (g_v X_v g_v^*) \text{ for all } X \in \mathcal{V},$$

where g_v^* denotes the transpose of g_v if v is a real embedding, and the complex conjugate transpose of g_v if v is a complex embedding.

We can define a cone $\mathcal{C}$ contained in $\mathcal{V}$ by setting C_v to be the cone of positive definite matrices in V_v for each v, and then defining

$$\mathcal{C} = \prod_v C_v.$$

With respect to the inner product $\langle\ ,\ \rangle$ previously defined on $\mathcal{V}$, $\mathcal{C}$ is *self-adjoint*, meaning that we have a characterization

$$\mathcal{C} = \{X \in \mathcal{V};\ \langle X, Y\rangle > 0 \text{ for all } Y \in \overline{\mathcal{C}} \setminus \{0\}\},$$

where the closure $\overline{\mathcal{C}}$ of $\mathcal{C}$ consists of all positive semi-definite forms (in the sense that we allow each component to be positive semi-definite).

The group action of $G(\mathbb{R})$ on $\mathcal{V}$ restricts to an action on $\mathcal{C}$, and in fact any linear automorphism of $\mathcal{C}$ arises in this way. Moreover, we have the following result:

Proposition 4.1.1. *The action of $G(\mathbb{R})$ on the cone $\mathcal{C}$ described above is transitive.*

Proof. Since both $\mathcal{C}$ and $G(\mathbb{R})$ decompose into products indexed by the infinite places of F, it suffices to prove transitivity of the action componentwise. Let $X_1, X_2 \in C_v$ for some place v. Since both are positive definite real symmetric (respectively Hermitian) matrices, there exist orthogonal (respectively unitary) matrices M_1 and M_2 such that the matrices $M_i X_i M_i^*$are diagonal, say

$$M_i X_i M_i^* = \begin{pmatrix} \alpha_i & 0 \\ 0 & \beta_i \end{pmatrix},$$

where the α_i and β_i are positive real numbers.

If we define

$$g = M_2^* \begin{pmatrix} (\frac{\alpha_2}{\alpha_1})^{\frac{1}{2}} & 0 \\ 0 & (\frac{\beta_2}{\beta_1})^{\frac{1}{2}} \end{pmatrix} M_1,$$

then $g \in G(\mathbb{R})$, and we have $g \cdot X_1 = X_2$, as required. □

Now, consider the point $I = (I_v) \in \mathcal{C}$, where each I_v is the 2×2 identity matrix in the factor $\mathrm{Sym}_2(\mathbb{R})$ or $\mathrm{Herm}_2(\mathbb{R})$. It is clear to see that under the action of $G(\mathbb{R})$, each I_v is fixed by the orthogonal subgroup $\mathrm{O}(2)$ or unitary subgroup $\mathrm{U}(2)$ of $\mathrm{GL}_2(F_v)$, depending on whether v is real or complex. It therefore follows that $\mathcal{C} \simeq G(\mathbb{R})/K_\infty$, where K_∞ is the standard maximal compact subgroup of $G(\mathbb{R})$ defined previously. Furthermore, if we quotient out $\mathcal{C}$ by positive real homotheties, we obtain an isomorphism

$$\mathcal{C}/\mathbb{R}_+ \simeq G(\mathbb{R})/A_G^0(\mathbb{R})K_\infty,$$

thus confirming our earlier statement that we can realise our symmetric space X as a cone of Hermitian forms over F.

4.2 Koecher's Reduction Theory

As stated previously, the benefit of viewing the symmetric space X as a cone of positive definite Hermitian forms is that it makes computations more straightforward. To clarify this statement, we will now give a brief exposition of the work of Koecher on *positivity domains* ([**Koe60**]), which will give us a computable model for this cone. We follow the treatment given by Paul Gunnells (see for example, [**Gun11**] or [**GY13**]).

Let V be a finite-dimensional real vector space, equipped with an inner product $\langle\ ,\ \rangle$, and give V the standard topology induced by this inner product. For a subset $C \subset V$, let $\overline{C}$ denote its closure (with respect to the aforementioned topology), $\mathrm{Int}(C)$ its relative interior, and $\partial\overline{C} = \overline{C} \setminus \mathrm{Int}(C)$ its boundary.

We call a subset $C \subset V$ a *positivity domain* if the following are satisfied:
i. C is open and non-empty;
ii. $\langle X, Y\rangle > 0$ for all $X, Y \in C$; and
iii. For each $X \in V \setminus C$ there exists a non-zero $Y \in \overline{C}$ such that $\langle X, Y\rangle \leq 0$.

Proposition 4.2.1. *The cone $\mathcal{C}$ of positive definite Hermitian forms over F defined in the previous section (viewed as a subset of the full space $\mathcal{V}$ of Hermitian forms) is a positivity domain.*

Proof. This follows immediately from the fact that $\mathcal{C}$ is self-adjoint. □

In fact, it is easy to see that *any* positivity domain is a cone (in the sense that it is convex and closed under positive real homotheties) and cannot contain any lines.

Now, let D be a discrete non-empty subset of $\overline{C} \setminus \{0\}$. For each $\Phi \in C$, let

$$m_D(\Phi) = \inf_{X \in D}\{\langle \Phi, X\rangle\},$$

the *minimum* of Φ (with respect to D). In [**Koe60**] it is shown that $m_D(\Phi) \geq 0$, and furthermore that the infimum is achieved only on a finite set of points. We call this set the set of *minimal vectors* of Φ, and denote it by $M_D(\Phi)$:

$$M_D(\Phi) := \{X \in D;\ \langle \Phi, X\rangle = m_D(\Phi)\}.$$

We call a point $\Phi \in C$ *perfect* (with respect to D) if the linear span of its minimal vectors $M_D(\Phi)$ is the full space V.

In the specific example of the cone $\mathcal{C}$ of positive definite Hermitian forms over F, we refer to perfect points as perfect *forms*. We have the following characterization of such forms:

Proposition 4.2.2. *Let $\mathcal{C}$ denote the cone of positive definite Hermitian forms over F, and let D be a discrete non-empty subset of $\overline{\mathcal{C}}$. Then a point $\Phi \in \mathcal{C}$ is perfect if, and only if, it can be recovered uniquely from the data $\{m_D(\Phi), M_D(\Phi)\}$ (that is, if $\Phi' \in \mathcal{C}$ satisfies $m_D(\Phi') = m_D(\Phi)$ and $M_D(\Phi') = M_D(\Phi)$, then $\Phi' = \Phi$).*

Proof. Let $v_1, \ldots, v_r$ and $v_{r+1}, \ldots, v_{r+s}$ denote the set of real and complex places of F respectively, and define an $\mathbb{R}$-basis for $\mathcal{V}$ by giving each V_{v_i} the basis

$$\mathcal{B}_i = \begin{cases} \{x_{i,1}, x_{i,2}, x_{i,3}\}; & i \in \{1, \ldots, r\} \\ \{x_{i1}, x_{i2}, x_{i3}, x_{i4}\}; & i \in \{r+1, \ldots, r+s\}, \end{cases}$$

where

$$x_{i1} = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right),\ x_{i2} = \left(\begin{smallmatrix} 0 & 0 \\ 0 & 1 \end{smallmatrix}\right),\ x_{i3} = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right),\ x_{i4} = \left(\begin{smallmatrix} 0 & \alpha \\ -\alpha & 0 \end{smallmatrix}\right),$$

and $\alpha^2 = -1$.

Now, let

$$A = \sum_{i,j} a_{ij} x_{ij}, \text{ and } B = \sum_{i,j} b_{ij} x_{ij}$$

be any two points in $\mathcal{V}$. Then

$$\langle A, B \rangle = \sum_{i=1}^{r+s} (a_{i1}b_{i1} + a_{i2}b_{i2} + 2a_{i3}b_{i3}) + 2 \sum_{i=r+1}^{r+s} a_{i4}b_{i4} = \mathbf{a}\hat{\mathbf{b}}^T,$$

where

$$\mathbf{a}_{ij} = a_{ij},$$

and

$$\hat{\mathbf{b}}_{ij} = \begin{cases} b_{ij}; & \text{if } j = 1, 2, \\ 2b_{ij}; & \text{if } j = 3, 4. \end{cases}$$

Given $\Phi \in \mathcal{C}$, let $M_D(\Phi) = \{P_1, \ldots, P_t\}$ denote the set of minimal vectors of Φ, and let

$$P_k = \sum_{i,j} p_{ij}^{(k)} x_{ij} \text{ for each } k, \text{ and } \Phi = \sum_{i,j} \phi_{ij} x_{ij}.$$

We obtain a linear system of equations

$$\mathbf{p}^{(k)} \hat{\phi}^T = m_D(\phi),\ k = 1, \ldots, t,$$

as above. From this it is clear that we have a unique solution for Φ if, and only if, the $\mathbf{p}^{(k)}$ form the rows of a matrix of rank $3r + 4s$, which occurs if, and only if, Φ is perfect. $\square$

Throughout our work, we will fix a choice of discrete set D, taking the set Ξ consisting of points of the form $q(x)$, $x \in \mathcal{O}_F^2 \setminus \{0\}$, where

$$q(x) = (x_v x_v^*),$$

with each x_v the image of x under the embedding $F^2 \hookrightarrow F_v^2$. Note that each matrix $x_v x_v^*$ has rank one, and thus $q(x) \in \overline{\mathcal{C}}$.

It is clear that a point Φ in a positivity domain C is perfect if, and only if, $\lambda\Phi$ is also perfect for any $\lambda \in \mathbb{R}_+$, in which case $m_D(\lambda\Phi) = \lambda m_D(\Phi)$. We may therefore consider only those perfect forms Φ for which $m_D(\Phi) = 1$. Given a discrete set D, we denote by $\mathrm{Perf}(D)$ the set of perfect points for D whose minimum is 1.

One of the benefits of studying positivity domains is that they exhibit a *reduction theory*: given a positivity domain C, we will find that we can decompose C into a family of cones Σ which has only finitely many orbits under the action of certain discrete subgroups Γ of the automorphism group $G_C \subset \mathrm{GL}(V)$ of C. This is reminiscent of the classical situation, and the fundamental domains for the action of congruence subgroups $\Gamma \subset \mathrm{SL}_n(\mathbb{Z})$ on the complex upper half-plane $\mathfrak{h}_2$.

In the case of binary Hermitian forms over a number field, this theory will utilize the discrete set Ξ we have described previously. More generally, given a positivity domain C, call a non-empty discrete set $D \subset \overline{C} \setminus \{0\}$ *admissible* if for any sequence (Φ_i) in C converging to a point in ∂C, we have $m_D(\Phi_i) \to 0$.

Proposition 4.2.3. *The set Ξ defined above is an admissible subset of the cone $\mathcal{C}$ of positive definite Hermitian forms over F.*

Proof. See **[Koe60], Lemma 11**. □

We are almost in a position to discuss the aforementioned reduction theory. Before we proceed, we need a few basic notions from the field of convex geometry.

A *polyhedral cone* in a real vector space V is a subset σ of the form

$$\sigma = \sigma(v_1, \ldots, v_t) = \left\{ \sum \lambda_i v_i;\ \lambda_i \geq 0 \right\},$$

where $v_1, \ldots, v_t \in V$ is a fixed set of vectors. We say that the set $\{v_1, \ldots, v_t\}$ is a *spanning set* for σ. If σ admits a linearly independent spanning set, then we call σ *simplicial*. The dimension of a polyhedral cone σ is the dimension of its linear span; if $d = \dim(\sigma)$, we call σ a d-cone.

Fix an inner product space V, with positivity domain C, and let $D \subset \overline{C} \setminus \{0\}$ be an admissible subset. Given a perfect point $\Phi \in \mathrm{Perf}(D)$, one can naturally define a polyhedral cone $\sigma(\Phi) = \sigma(P_1, \ldots, P_t)$, where $\{P_1, \ldots, P_t\} = M(\Phi)$ is the set of minimal vectors of Φ. We call such a cone the *perfect pyramid* associated to Φ. By definition, it is a cone of dimension $\dim_{\mathbb{R}}(V)$, although it need not be simplicial. Let $\Sigma = \Sigma_D$ denote the set of perfect pyramids, together with all their proper faces, as we range over all perfect points $\Phi \in \mathrm{Perf}(D)$. Then Koecher proves in **[Koe60]** the following result:

Theorem 4.2.4. *The perfect pyramids have the following properties:*

(i) *Any compact subset of C meets only finitely many perfect pyramids.*

(ii) *Two different perfect pyramids have no interior point in common.*

(iii) *Given a perfect pyramid σ, there are only finitely many perfect pyramids σ' such that $\sigma \cap \sigma'$ contains a point of C. By part* (ii)*, this must lie on the boundaries of σ and σ'.*

(iv) *The intersection of any two perfect pyramids is a common face of each.*

(v) *Let σ be a perfect pyramid and τ a codimension one face of σ. If τ does not lie completely in the boundary ∂C, then there exists precisely one other perfect pyramid σ' such that $\sigma \cap \sigma' = \tau$.*

(vi) $\bigcup_{\sigma \in \Sigma} \sigma \cap C = C$.

By a *facet* of a perfect pyramid σ, we shall mean a codimension one face. If two perfect pyramids σ and σ' meet in a facet τ as in condition (v) above, we say that σ and σ' are *neighbours*.

We call Σ the *Koecher fan*, and the cones in Σ the *Koecher cones*.

Let $G_C \subset \mathrm{GL}(V)$ denote the group of automorphisms of V which fix the cone C, and let $\Gamma \subset G_C$ be a discrete subgroup which preserves the admissible set D. In **[Koe60], Section 5.4** it is shown that Γ admits a properly discontinuous action on C. Then:

Theorem 4.2.5. *We have an explicit reduction theory for Γ in the following sense:*

(i) *There are finitely many Γ-orbits in Σ.*

(ii) *Every $X \in C$ is contained in a unique cone in Σ.*

(iii) *If $\sigma \in \Sigma$ does not lie completely in the boundary ∂C, the stabilizer*

$$S_\sigma := \{\gamma \in \Gamma;\ \gamma(\sigma) = \sigma\}$$

is finite.

If we choose representatives $\sigma_1, \ldots, \sigma_k$ of the orbits of $\Gamma \in \Sigma$, and let

$$\Omega = \Omega(\Gamma) = \bigcup_{i=1}^{k} (\sigma_i \cap C),$$

then the intersection of each cone $\sigma \in \Sigma$ with C has a Γ-translate which is contained in Ω. This is not quite a fundamental domain, as we have non-trivial stabilizers to worry about, but since these are finite groups, it doesn't in practice cause a problem.

4.3 The Koecher Polytope

For computational purposes, we will use an alternative realization of the Koecher fan and perfect pyramids, which accounts for the scaling present in the identification

$$X = \mathcal{C}/\mathbb{R}_+.$$

Given an admissible set D in a positivity domain $\overline{C}$, call a point $P \in D$ *primitive* if it is a minimal vector of some perfect point, and define D_{prim} to be the set of all primitive points. We then define the *Koecher polytope* Π to be the convex hull in $\overline{C}$ of D_{prim}. This is an infinite polytope, of dimension $\dim_{\mathbb{R}}(\mathcal{V})$. By a *facet* of Π we shall mean any subpolytope of Π of codimension one, while a *face* of Π refers to a subpolytope of arbitrary dimension (which is necessarily a subpolytope of some facet of Π). We say that two facets of Π are *neighbours* if their boundaries intersect in a face of Π of codimension two.

Given an arbitrary face $\mathcal{F}$ of Π, we define the *cone above* $\mathcal{F}$ to be the polyhedral cone $\sigma(P_1, \ldots, P_n)$, where the P_i are the vertices of $\mathcal{F}$. The following result gives a justification for considering Π in lieu of the Koecher fan Σ.

Proposition 4.3.1. *Given a perfect point $\Phi \in \overline{C}$, the convex hull of the minimal vectors of Φ defines a facet of the Koecher polytope Π. Moreover, if no facet τ of a perfect pyramid $\sigma \in \Sigma$ is contained in the boundary ∂C, then this in fact establishes a bijection between perfect points and facets of Π.*

Proof. (See also **[GY13], Proposition 2.7**). Let Φ be a perfect point, with minimal vectors $P_1, \ldots, P_k$. The perfect pyramid $\sigma(\Phi)$ is defined to be the set of non-negative linear combinations of the P_i, and so its intersection with the hyperplane

$$\mathcal{H}_\Phi := \{X \in C;\ \langle \Phi, X\rangle = 1\}$$

is precisely the convex hull of the P_i (recalling that we have chosen our perfect forms such that the minimum $m_D(\Phi) = 1$). Since the vectors P_i span V, this intersection must be a convex polytope of codimension one. Moreover, since $\langle \Phi, P\rangle > 1$ for any $P \in D \setminus M_D(\Phi)$, it follows that all other points of Π lie in the half-plane

$$\{X \in C;\ \langle \Phi, X\rangle > 1\}$$

cut out of V by $\mathcal{H}_\Phi$ (we call $\mathcal{H}_\Phi$ a *supporting hyperplane* for Π). Thus $\sigma(\Phi) \cap \mathcal{H}_\Phi$ is a proper subpolytope of Π, of codimension one, i.e., a facet.

Thus to each perfect point Φ we can associate a unique facet $\mathcal{F}_\Phi$ of the Koecher polytope Π. Conversely, the requirement that no facet of a perfect pyramid is contained in the boundary means that we can apply **Theorem 4.2.4** (v), and so any neighbour of $\mathcal{F}_\Phi$ corresponds to a unique perfect point Φ'. It therefore follows that the facets of Π are in bijection with the perfect pyramids, as required. □

We shall see later (in **Proposition 4.4.3**) that the hypothesis of **Proposition 4.3.1** is satisfied in our case of interest. Thus we shall often refer to cones in Σ and faces of Π interchangeably. For each face $\mathcal{F}$ of Π, we define $M(\mathcal{F})$ to be the set of vertices of $\mathcal{F}$ (that is, the minimal subset of D of which $\mathcal{F}$ is the convex hull). If $\mathcal{F}$ is a facet of Π, and $\Phi_{\mathcal{F}}$ is the perfect point associated to $\mathcal{F}$, then every vertex of $\mathcal{F}$ is necessarily a minimal vector of $\Phi_{\mathcal{F}}$, but the converse need not hold (which we shall see later in our specific case).

Henceforth, we shall restrict our attention to the space $\mathcal{C}$ of Hermitian forms over a number field F, under the assumption that the above hypothesis holds. Moreover, motivated by the results of **Section 3.5**, we shall assume further that F is a *CM field*, and that $F/\mathbb{Q}$ is a *Galois* extension. Unless otherwise stated, proofs in the remainder of **Section 4.3** are (to the best of our knowledge) original, and often specifically tailored to our special case. Where a result exists in greater generality, we shall endeavour to make this clear.

Since F is a CM field, there is a unique totally real subfield K of F, such that F/K is a quadratic extension, and a unique non-trivial element $\tau \in \mathrm{Gal}(F/\mathbb{Q})$ which fixes this subfield. Fixing an initial embedding of F into $\mathbb{C}$, we identify our choice of complex embeddings with a set $\{\sigma_1, \ldots, \sigma_n\}$ of coset representatives for the quotient group $\mathrm{Gal}(F/\mathbb{Q})/\langle\tau\rangle$, and note that τ acts on F via complex conjugation, regardless of which embedding we choose.

Recall that, for our admissible subset, we take the set Ξ comprising points of the form $\{q(x);\ x \in \mathcal{O}_F^2\}$ defined previously (for ease of notation, we shall henceforth denote by $m(\Phi)$ and $M(\Phi)$ the minimum and minimal vectors of a perfect form Φ respectively, suppressing any mention of Ξ). Note that in the classical example of $F = \mathbb{Q}$ the subset Ξ_{prim} is precisely the set

$$\Xi = \{q(x);\ x \in \mathbb{Z}^2 \text{ is primitive}\},$$

where we call a vector $x = \left(\begin{smallmatrix} a \\ b \end{smallmatrix}\right)$ *primitive* if $\gcd(a, b) = 1$. For more general fields, however, this need not be the case (in the next section we will see that Ξ_{prim} always contains the latter set - a consequence of **Corollary 4.4.2** - and shall also see an example of a minimal vector which is not an element of this set).

The group $\mathrm{GL}_2(\mathcal{O}_F)$ admits an action on the sets Ξ and Ξ_{prim}, given by

$$g \cdot q(x) = q(gx),\ g \in \mathrm{GL}_2(\mathcal{O}_F),\ x \in \mathcal{O}_F^2.$$

We will typically identify $\mathrm{GL}_2(\mathcal{O}_F)$ with its image in $G(\mathbb{R})$, obtained by embedding $\mathrm{GL}_2(\mathcal{O}_F)$ into each component. Thus $\mathrm{GL}_2(\mathcal{O}_F)$ can be realized as a discrete subgroup of $G(\mathbb{R})$, and its action on Ξ is induced by the action of $G(\mathbb{R})$ on $\mathcal{C}$. In particular, by **Theorem 4.2.5** (combined with **Proposition 4.3.1**) there are only finitely many orbits of faces of Π under the action of $\mathrm{GL}_2(\mathcal{O}_F)$.

The main aim of this section is twofold. Firstly, we wish to construct a set of representatives of the faces of Π under this $\mathrm{GL}_2(\mathcal{O}_F)$-action. In doing so, we shall present an algorithm which allows one to, given a facet $\mathcal{F}$ of Π, construct *all* neighbouring facets $\mathcal{F}'$. Using this, we will present a second algorithm which, given a point $X \in \Pi$, allows one to determine the precise facet $\mathcal{F} = \mathcal{F}(X)$ in which X lies.

Before proceeding, it will be useful to define subsets of the space $\mathcal{V}$ and cone $\mathcal{C}$ which can be defined rationally. Since each point in Ξ can be defined by a series of rational equations (for example, by defining an $\mathbb{Q}$-basis for F) these shall be our starting point. Define, therefore, $\mathcal{V}(\mathbb{Q})$ and $\mathcal{C}(\mathbb{Q})$ to be the subsets of $\mathcal{V}$ and $\mathcal{C}$ respectively comprising all points which can be defined as a rational linear combination of elements of Ξ. Note that, since the minimal vectors of a perfect form span the entire space $\mathcal{V}$, we have $\mathcal{V}(\mathbb{Q}) \otimes_{\mathbb{Q}} \mathbb{R} \simeq \mathcal{V}$.

We make the following alternative characterization:

Proposition 4.3.2. *Let F be as described above. Let $\Phi \in \mathcal{V}$ (respectively $\mathcal{C}$). Then $\Phi \in \mathcal{V}(\mathbb{Q})$ (respectively $\Phi \in \mathcal{C}(\mathbb{Q})$) if, and only if, $\langle \Phi, X \rangle \in \mathbb{Q}$ for all $X \in \Xi$.*

Proof. Note first that $\langle X, Y \rangle \in \mathbb{Q}$ for any $X, Y \in \Xi$. Indeed, let $X = q(x)$, $Y = q(y)$, with $x, y \in \mathcal{O}_F^2$. Then, noting that $\mathrm{Tr}(xx^*yy^*)$ is invariant under complex conjugation, we find that

$$\begin{aligned} \langle X, Y \rangle &= 2 \sum_{i=1}^{n} \sigma_i(\mathrm{Tr}(xx^*yy^*)) \\ &= \mathrm{Tr}_{F/\mathbb{Q}}(\mathrm{Tr}(xx^*yy^*)), \end{aligned}$$

which is clearly rational. Consequently, $\langle \Phi, X \rangle \in \mathbb{Q}$ for any $\Phi \in \mathcal{V}(\mathbb{Q})$ and all $X \in \Xi$.

Conversely, suppose $\langle \Phi, X \rangle \in \mathbb{Q}$ for all $X \in \Xi$, for some $\Phi \in \mathcal{V}$. In particular, choose any $\mathbb{R}$-basis for $\mathcal{V}$ of such points (from the set of minimal vectors of some perfect form, for example). Then, since $\langle X, Y \rangle \in \mathbb{Q}$ for all $X, Y \in \Xi$, we can define an orthogonal $\mathbb{R}$-basis for $\mathcal{V}$ consisting of rational linear combinations of elements in Ξ, using the Gram-Schmidt algorithm. For each such basis vector, the inner product with Φ remains rational, and consequently Φ is a rational linear combination of these basis vectors, and thus of the original elements of Ξ. □

Note that the same result holds if we replace the condition $\langle \Phi, X \rangle \in \mathbb{Q}$ for all $X \in \Xi$ with the weaker condition that $\langle \Phi, X \rangle \in \mathbb{Q}$ for all X in some finite subset of Ξ which spans $\mathcal{V}$ as a real vector space. In particular, all perfect forms lie in $\mathcal{C}(\mathbb{Q})$.

We shall now proceed with the task of constructing the Koecher polytope. This relies heavily on the fact, which we shall now prove, that, given any facet $\mathcal{F}$ of the Koecher polytope Π, we can construct *all* facets $\mathcal{G}$ of Π which are neighbours of $\mathcal{F}$. Thus, by translation (noting that, being a convex subset of a real vector space, Π is connected), we can understand the entire polytope.

Our first step towards this construction is to prove a finiteness result, namely that there are only finitely many points of Ξ within a certain distance of any given facet of Π (where we measure the distance of a point X from a facet $\mathcal{F}$ by evaluating the inner product $\langle \Phi_{\mathcal{F}}, X \rangle$).

Lemma 4.3.3. *Let F be as above, and fix $\lambda \in \mathbb{R}_+$. Then the set*

$$\{x \in \mathcal{O}_F;\ |\sigma(x)|^2 \leq \lambda \text{ for all } \sigma \in \mathrm{Gal}(F/\mathbb{Q})\}$$

is finite.

Proof. The hypothesis that all Galois conjugates of x be bounded in absolute value implies that the coefficients of the characteristic polynomial of x are bounded, and since these coefficients must be integral the result follows. □

In fact, we have the following, more general result:

Proposition 4.3.4. *Let F be as above, and fix $\lambda \in \mathbb{R}_+$. Given $\Phi \in \mathcal{C}(\mathbb{Q})$, the set*

$$\{X \in \Xi;\ 0 < \langle \Phi, X \rangle \leq \lambda\}$$

is finite.

Proof. (For a more general proof, see **[Gun99], Proposition 3**). Let $\Phi = (\phi_i)$, with each ϕ_i positive definite, and let $X = q(x)$, for $x \in \mathcal{O}_F^2$. Then

$$\langle \Phi, X \rangle = 2 \sum_{i=1}^{n} x_i^* \phi_i x_i,$$

where $x_i = \sigma_i(x)$. Since $\langle \Phi, X \rangle$ is bounded, the elements $x_i^* \phi_i x_i \in \mathbb{R}$ are all bounded. Write $\phi_i = \begin{pmatrix} a_i & b_i \\ \bar{b}_i & c_i \end{pmatrix}$, where a_i, c_i, and $\det(\phi_i) \in \mathbb{R}$ are positive, and let $x_i = \begin{pmatrix} w_i \\ z_i \end{pmatrix}$. Then:

$$x_i^* \phi_i x_i = a_i |w_i|^2 + b_i \bar{w}_i z_i + \bar{b}_i w_i \bar{z}_i + c_i |z_i|^2 = a_i \left(|w_i + \frac{b_i}{a_i} z_i|^2 + \frac{\det(\phi_i)}{a_i^2} |z_i|^2 \right).$$

It follows that $|z_i|^2$ is bounded for each element σ_i, and thus there are only finitely many choices for $z \in \mathcal{O}_F$, by **Lemma 4.3.3**. For each value of z, the conjugates w_i are bounded in absolute value with respect to z, and so are also bounded, proving the result. □

Suppose, now, that we are given a facet $\mathcal{F}$ of Π (and so, by **Proposition 4.2.2**, we know the perfect form $\Phi_{\mathcal{F}}$). The following result (whose proof we borrow from **[Gun99], Lemma 1**) gives a means of constructing the perfect forms corresponding to neighbouring facets of Π:

Proposition 4.3.5. *Let $\mathcal{F}$ and $\mathcal{G}$ be neighbouring facets of Π, and let $\mathcal{E} = \mathcal{F} \cap \mathcal{G}$. Choose a point $\Psi \in \mathcal{V}(\mathbb{Q})$ orthogonal to the cone above the polytope $\mathcal{E}$, such that $\langle \Psi, X \rangle \geq 0$ for all $X \in \mathcal{F}$. Then*

$$\Phi_{\mathcal{G}} = \Phi_{\mathcal{F}} + \bar{\rho}\Psi$$

for a unique $\bar{\rho} \in \mathbb{R}_+$.

Proof. The cones above $\mathcal{F}$ and $\mathcal{G}$ are perfect pyramids, and so the cone above $\mathcal{E}$, being a facet of both of these pyramids, is of codimension 1, i.e., a hyperplane in $\mathcal{V}$. Thus Ψ is unique up to a scalar multiple. If $\Psi' = \Phi_{\mathcal{G}} - \Phi_{\mathcal{F}}$, then $\langle \Psi', X \rangle = 0$ for all $X \in \mathcal{E}$, and $\Psi' \neq 0$, so $\bar{\rho}\Psi = \Psi'$ for some non-zero $\bar{\rho} \in \mathbb{R}$, and thus $\Phi_{\mathcal{G}} = \Phi_{\mathcal{F}} + \bar{\rho}\Psi$. Now, let $X \in \mathcal{F} \setminus \mathcal{E}$, so that $\langle \Psi, X \rangle > 0$. Then

$$1 < \langle \Phi_{\mathcal{G}}, X \rangle = \langle \Phi_{\mathcal{F}}, X \rangle + \bar{\rho}\langle \Psi, X \rangle = 1 + \bar{\rho}\langle \Psi, X \rangle,$$

and so $\bar{\rho} > 0$, as required. □

Computation of the point Ψ in the above proposition is a straightforward application of linear algebra, given knowledge of $\mathcal{F}$, $\mathcal{E}$ and Ψ. Computation of $\bar{\rho}$, on the other hand, requires a little more work. If we can find a point $X \in \Xi$ which lies in $\mathcal{G} \setminus \mathcal{E}$, then we can easily compute $\bar{\rho}$, so our plan is to search over "nearby" points $X \in \Xi$ and determine whether or not the points $(\Xi \cap \mathcal{E}) \cup \{X\}$ define a unique form. To begin with, we define a function ρ on the set Ξ by

$$\rho(X) = \frac{1 - \langle \Phi_{\mathcal{F}}, X \rangle}{\langle \Psi, X \rangle}.$$

Proposition 4.3.6. *Given $X \in \Xi$, we have $\rho(X) = \bar{\rho}$ if, and only if, $X \in \mathcal{G} \setminus \mathcal{E}$.*

Proof. Suppose first that $X \in \mathcal{G} \setminus \mathcal{E}$, so that $\langle \Phi_{\mathcal{G}}, X \rangle = 1 < \langle \Phi_{\mathcal{F}}, X \rangle$, and $\langle \Psi, X \rangle \neq 0$. Then

$$\rho(X) = \frac{1 - \langle \Phi_{\mathcal{F}}, X \rangle}{\langle \Psi, X \rangle} = \frac{\langle \Phi_{\mathcal{G}}, X \rangle - \langle \Phi_{\mathcal{F}}, X \rangle}{\langle \Psi, X \rangle} = \bar{\rho}.$$

Conversely, if $\rho(X) = \bar{\rho}$ then clearly $\langle \Psi, X \rangle \neq 0$, hence $X \notin \mathcal{E}$, and

$$\langle \Phi_{\mathcal{G}}, X \rangle = \langle \Phi_{\mathcal{F}}, X \rangle + \rho(X)\langle \Psi, X \rangle = \langle \Phi_{\mathcal{F}}, X \rangle + 1 - \langle \Phi_{\mathcal{F}}, X \rangle = 1,$$

so $X \in \mathcal{G}$, as required. □

Thus we seek to find a point $X \in \Xi$ with $\rho(X) = \bar{\rho}$. To this end, define a set $\mathcal{S}$ by

$$\mathcal{S} := \{X \in \Xi;\ \langle \Psi, X\rangle < 0 \text{ and } \Phi + \rho(X)\Psi \in \mathcal{C}\}.$$

We claim that $\mathcal{S}$ is non-empty. Indeed, if $X \in \Xi$ lies in $\mathcal{G} \setminus \mathcal{E}$, then the above result shows that $\Phi_{\mathcal{F}} + \rho(X)\Psi = \Phi_{\mathcal{G}} \in \mathcal{C}$, and moreover $\rho(X) = \bar{\rho} \in \mathbb{R}_+$, so $\langle \Psi, X\rangle < 0$, and thus $X \in \mathcal{S}$.

Proposition 4.3.7. *The minimal value of $\rho(X)$ as X runs over all elements of $\mathcal{S}$ is $\bar{\rho}$, and this minimum is attained.*

Proof. (See also **[Gun99], Lemma 2**). We have already seen that $\rho(X) = \bar{\rho}$ for some elements of $\mathcal{S}$, so suppose $X \in \mathcal{S}$ with $\rho(X) < \bar{\rho}$. Then

$$\begin{aligned}\langle \Phi_{\mathcal{G}}, X\rangle &= \langle \Phi_{\mathcal{F}}, X\rangle + \bar{\rho}\langle \Psi, X\rangle \\ &< \langle \Phi_{\mathcal{F}}, X\rangle + \rho(X)\langle \Psi, X\rangle \\ &= 1,\end{aligned}$$

which is a contradiction. □

If we could construct the set $\mathcal{S}$ and find an element $X \in \mathcal{S}$ with $\rho(X)$ minimal, then we would have our perfect form $\Phi_{\mathcal{G}}$. However, *a priori*, $\mathcal{S}$ need not be finite, so we shall attempt to restrict our attention to a set which is provably finite, allowing us to perform a search over all of its elements. Given an arbitrary point $P \in \mathcal{S}$, define $\Phi_P = \Phi_{\mathcal{F}} + \rho(P)\Psi \in \mathcal{C}$, and let $\mathcal{T}_P$ be the set

$$\mathcal{T}_P := \{X \in \Xi;\ \langle \Phi_P, X\rangle \leq 1\}.$$

Proposition 4.3.8. *The set $\mathcal{T}_P$ is finite, and contains those points of Ξ which lie in $\mathcal{G} \setminus \mathcal{E}$.*

Proof. (We use the proof from **[Gun99], Lemma 3**) Note first that the points $P, \Phi_{\mathcal{F}}$ and $\Psi \in \mathcal{V}(\mathbb{Q})$, and consequently so too is Φ_P. Thus by **Proposition 4.3.4** the set $\mathcal{T}_P$ is finite. Now, given $X \in \Xi$ lying in $\mathcal{G} \setminus \mathcal{E}$, we have seen that $X \in \mathcal{S}$, and so

$$\begin{aligned}\langle \Phi_P, X\rangle &= \langle \Phi, X\rangle + \rho(P)\langle \Psi, X\rangle \\ &\leq \langle \Phi_{\mathcal{F}}, X\rangle + \bar{\rho}\langle \Psi, X\rangle \\ &= \langle \Phi_{\mathcal{G}}, X\rangle \\ &= 1,\end{aligned}$$

so $X \in \mathcal{T}_P$, as required. □

We finally have all the information we require. Indeed, the above result shows that the set $\mathcal{T}_P \cap \mathcal{S}$ is non-empty. Thus, if we choose an element X of this set such that $\rho(X)$ is minimal, then by **Propositions 4.3.6** and **4.3.7**, $X \in \mathcal{G} \setminus \mathcal{E}$, and so we can construct $\Phi_{\mathcal{G}}$.

With this in mind, it is straightforward to determine a set of representatives for the faces of Π modulo the action of $\mathrm{GL}_2(\mathcal{O}_F)$. It suffices to determine a set of representatives of the *facets* of Π, since any lower-dimensional face of Π will be contained in one of these.

Equivalently, we wish to define a set **Perf** of $\mathrm{GL}_2(\mathcal{O}_F)$-representatives of perfect forms. To do this, we begin with an initial perfect form $\Phi_1 \in \mathcal{C}$, and define $\mathbf{Perf} := \{\Phi_1\}$. We then proceed to determine all perfect forms which are neighbours of Φ_1, find a subset of representatives of the orbits under $\mathrm{GL}_2(\mathcal{O}_F)$ of these forms, and add to the set **Perf** any of these resulting perfect forms which are not $\mathrm{GL}_2(\mathcal{O}_F)$-equivalent to Φ_1. We continue this process inductively.

Now, if Φ and Φ' are two $\mathrm{GL}_2(\mathcal{O}_F)$-equivalent perfect forms, then the sets of neighbouring forms of Φ and Φ' are similarly $\mathrm{GL}_2(\mathcal{O}_F)$-equivalent. It follows, therefore, that if the set **Perf** stabilizes (that is, if at any point we do not add any new forms the **Perf**) then we must have a complete set of $\mathrm{GL}_2(\mathcal{O}_F)$-representatives of perfect forms. Since we know that there are only finitely many $\mathrm{GL}_2(\mathcal{O}_F)$-orbits of perfect forms, we will eventually find that **Perf** stabilizes under this process, at which point we have found a complete set of representatives.

Note that, having found a set of representative perfect forms (and thus facets of the Koecher polytope) one can easily find a set of representatives faces of any lower dimension, simply by decomposing each of the facets, and testing the resulting faces for $\mathrm{GL}_2(\mathcal{O}_F)$-equivalence (which we shall do in **Section 4.5**).

To determine an initial perfect form, we use a method discussed in [**Sch09**], which was suggested to us by Dan Yasaki. A generalisation of **Proposition 4.3.5** states the following:

Proposition 4.3.9. *Let Φ be a positive definite Hermitian form over F, and choose a point $\Psi \in \mathcal{V}(\mathbb{Q})$ orthogonal to the cone $\sigma(\Phi)$, such that $\langle \Psi, P \rangle \geq 0$ for all minimal vectors P of Φ. Then there exists $\rho \in \mathbb{R}_+$ such that the linear span of the minimal vectors of the Hermitian form $\Phi + \rho\Psi$ has dimension strictly greater than that of the minimal vectors of Φ.*

Proof. See the discussion in **[Sch09], Section 7**. □

One can find this constant ρ in the same manner as discussed previously. In practice, therefore, we choose an arbitrary positive definite form, determine its minimal vectors, and repeatedly apply **Proposition 4.3.9** until we obtain a form whose minimal vectors span the entire space $\mathcal{V}$, which must therefore be perfect (if necessary, we then scale this form so that its minimum is equal to 1).

The final goal of this section is to determine, given a point $X \in \mathcal{C}$, the facet $\mathcal{F}(X)$ of Π above which X lies (equivalently, given any point on the Koecher polytope, the facet in which it is contained). The algorithm for doing this is the same as stated in [**Gun99**] for the Voronoi polyhedron, and applies to the more general setting of the Koecher polytope.

The idea behind the algorithm is to choose a perfect form Φ, and then repeatedly pass to a neighbouring perfect form Φ' such that $\langle \Phi', X\rangle < \langle \Phi, X\rangle$. We continue this until this inner product stabilizes, at which point the required facet $\mathcal{F}(X)$ is that associated to the perfect form we have reached. We now provide some justification (which differs somewhat from that presented in [**Gun99**]) for this argument.

Proposition 4.3.10. *Let $\Phi \in \mathcal{C}(\overline{\mathbb{Q}})$ be a perfect form, let $X \in \Pi$, and fix $\lambda \in \mathbb{R}_+$. Then the set*

$$\{g \cdot X;\ g \in \mathrm{GL}_2(\mathcal{O}_F),\ \langle \Phi, g \cdot X\rangle \leq \lambda\}$$

is finite.

Proof. This follows as a result of **Proposition 4.3.4**. Indeed, let

$$X = \sum_{i=1}^{r} \lambda_i X_i,\ \lambda_i \in \mathbb{R}_+,\ \sum_{i=1}^{r} \lambda_i = 1$$

for some $X_i \in \Xi$, and suppose on the contrary that the above set is infinite. If each point X_i had a finite orbit under the action of $\mathrm{GL}_2(\mathcal{O}_F)$, then there would be only a finite number of possible images of X; thus, without loss of generality, we may assume that X_1 has infinitely many $\mathrm{GL}_2(\mathcal{O}_F)$-translates.

However, by **Proposition 4.3.4**, there are only finitely many points $Y \in \Xi$ such that $\langle \Phi, Y\rangle \leq \frac{\lambda}{\lambda_1}$, so we must have $\langle \Phi, g \cdot X_1\rangle > \frac{\lambda}{\lambda_1}$ for some $g \in \mathrm{GL}_2(\mathcal{O}_F)$, whence $\langle \Phi, g \cdot X\rangle > \lambda$, a contradiction. □

Corollary 4.3.11. *Let $X \in \overline{\mathcal{C}}(\mathbb{Q})$ and fix $\lambda \in \mathbb{R}_+$. Then the set of values*

$$\{\langle \Phi, X\rangle;\ \Phi \text{ a perfect form},\ \langle \Phi, X\rangle \leq \lambda\}$$

is finite.

Proof. By **Theorem 4.2.5**, there are only finitely many $\mathrm{GL}_2(\mathcal{O}_F)$-orbits of perfect forms, so let $\Phi_1, \ldots, \Phi_r$ be a set of representatives. Thus for an arbitrary perfect form Φ, we have $\Phi = g \cdot \Phi_i$ for some i and some $g \in \mathrm{GL}_2(\mathcal{O}_F)$, and so

$$\langle \Phi, X\rangle = \langle g \cdot \Phi_i, X\rangle = \langle \Phi_i, g^* \cdot X\rangle,$$

by definition of the inner product on $\mathcal{V}$.

By **Proposition 4.3.10**, only finitely many members of the orbit $\mathrm{GL}_2(\mathcal{O}_F)\cdot X$ satisfy the required inequality, and the result follows. □

We require the following classification of the facet $\mathcal{F}(X)$ in which a point $X \in \Pi$ lies:

Proposition 4.3.12. *Let $\mathcal{F}$ be a facet of Π, and let $X \in \Pi$. Then X is contained in $\mathcal{F}$ if, and only if, $\langle \Phi_{\mathcal{F}}, X\rangle \leq \langle \Phi_{\mathcal{G}}, X\rangle$ for all neighbouring facets $\mathcal{G}$ of $\mathcal{F}$.*

Proof. (For an alternative proof, see **[Gun99], Lemma 4**). If X is contained in $\mathcal{F}$, then $\langle \Phi_{\mathcal{F}}, X\rangle = 1$, and we may write

$$X = \sum_{i=1}^{n} \lambda_i X_i,\ \lambda_i \in \mathbb{R}_+,\ \sum_{i=1}^{r} \lambda_i = 1$$

for some $X_i \in M(\mathcal{F})$. Since for any neighbouring facet $\mathcal{G}$ of $\mathcal{F}$, $\langle \Phi_{\mathcal{G}}, X_i\rangle \geq 1$, we have

$$\langle \Phi_{\mathcal{G}}, X\rangle = \sum_{i=1}^{n} \lambda_i \langle \Phi_{\mathcal{G}}, X_i\rangle \geq \sum_{i=1}^{n} \lambda_i = 1,$$

as required.

Conversely, suppose $X \notin \mathcal{F}$, and let

$$\mathcal{B}_{\mathcal{F}} := \sum_{X_i \in M(\mathcal{F})} X_i$$

denote the (scaled) barycenter of $\mathcal{F}$. Parametrize the line in $\mathcal{C}$ joining X and $\mathcal{B}_{\mathcal{F}}$ by defining

$$P_t := (1-t)\mathcal{B}_{\mathcal{F}} + tX,\ t \in [0,1]$$

(note that, since $\mathcal{C}$ is a convex cone, P_t is indeed contained in $\mathcal{C}$).

Now, P_t lies in the cone above $\mathcal{F}$ for small t, but must eventually leave this cone, as for t close to 1, Q_t lies in the same cone as X, and $X \notin \mathcal{F}$. Thus P_{t_0} must lie in the cone above $\mathcal{E}$ for some codimension two face $\mathcal{E}$ of Π and some $t_0 \in (0,1)$. Let $\mathcal{G}$ be the facet which meets $\mathcal{F}$ in the face $\mathcal{E}$, so we have $\langle \Phi_{\mathcal{F}}, P_{t_0}\rangle = \langle \Phi_{\mathcal{G}}, P_{t_0}\rangle$ (by the construction in **Proposition 4.3.5**). Equating the two, we obtain

$$(1-t_0)\langle \Phi_{\mathcal{F}}, \mathcal{B}_{\mathcal{F}}\rangle + t_0\langle \Phi_{\mathcal{F}}, X\rangle = (1-t_0)\langle \Phi_{\mathcal{G}}, \mathcal{B}_{\mathcal{F}}\rangle + t_0\langle \Phi_{\mathcal{G}}, X\rangle.$$

But $\langle \Phi_{\mathcal{G}}, \mathcal{B}_{\mathcal{F}}\rangle > \langle \Phi_{\mathcal{F}}, \mathcal{B}_{\mathcal{F}}\rangle$, since not every vertex of $\mathcal{F}$ is a minimal vector of $\Phi_{\mathcal{G}}$, and thus we must have $\langle \Phi_{\mathcal{F}}, X\rangle > \langle \Phi_{\mathcal{G}}, X\rangle$, as required. □

As a consequence, we note the following:

Corollary 4.3.13. *Let $\mathcal{F}$ be a facet of Π, and let $X \in \Pi$. Then $\langle \Phi_{\mathcal{G}}, X\rangle = \langle \Phi_{\mathcal{F}}, X\rangle$ for some neighbouring facet $\mathcal{G}$ of $\mathcal{F}$ if, and only if, $X \in \mathcal{F} \cap \mathcal{G}$.*

The reduction algorithm as presented in **[Gun99], Theorem 3** is then:

Theorem 4.3.14. *Given $X \in \Pi$, define an algorithm as follows. Choose a facet $\mathcal{F}$ of Π, and choose the neighbouring facet $\mathcal{G}$ of $\mathcal{F}$ such that $\langle \Phi_{\mathcal{G}}, X\rangle$ is minimal amongst all such neighbours. If $\langle \Phi_{\mathcal{G}}, X\rangle < \langle \Phi_{\mathcal{F}}, X\rangle$, then replace $\mathcal{F}$ with $\mathcal{G}$, and repeat. Otherwise, terminate the procedure.*

This algorithm terminates after a finite number of steps, and the facet $\mathcal{F}(X)$ containing X is the final facet of Π selected by the procedure.

Note that, since any point in $\overline{\mathcal{C}}$ lies above a facet of Π, the algorithm works equally well when applied to an arbitrary point in $\overline{\mathcal{C}}$, since some scalar multiple of it lies in Π.

Proof. By **Proposition 4.3.12**, the algorithm will produced the required facet of Π if it terminates, so it remains to prove termination. At each non-terminating stage, we replace a perfect form Φ with a perfect form Φ' such that $\langle \Phi', X\rangle < \langle \Phi, X\rangle$. **Corollary 4.3.11** shows that there are only finitely many possible values of $\langle \Phi, X\rangle \leq \langle \Phi_{\mathcal{F}}, X\rangle$, where $\mathcal{F}$ is our initial choice of facet, and consequently the algorithm must terminate after a finite number of steps. □

We note, finally, that for an arbitrary point $X \in \mathcal{C}$, we have $\lambda X \in \Pi$ for some $\lambda \in \mathbb{R}_+$. Thus the above algorithm will, given a point X in $\mathcal{C}$ which does not lie in the Koecher polytope, produce the perfect pyramid in which X lies (being the cone above the facet in which λX lies).

4.4 Facets of the Koecher Polytope

As we have seen previously, in order to understand the Koecher polytope Π it suffices to understand a set of representatives for the finite number of $\mathrm{GL}_2(\mathcal{O}_F)$-orbits of facets of Π, as every face is a subpolytope of such a facet. For our future computations, we will require knowledge of both the facets of Π and the perfect forms associated to them, and we shall therefore use this section to discuss a few observations which arose during our study. Throughout this section, we shall assume that F is a *quartic* CM field (we shall discuss the reasons for our further specialization to quartic fields in the next chapter).

Let $F = \mathbb{Q}(t)$ be our quartic CM field, which we shall continue to assume is Galois, and suppose for simplicity that the class group of F is trivial. Denote by K the real quadratic subfield of F. Fix a choice v_1, v_2 of non-conjugate embeddings of F into the complex numbers, and denote by σ the element of $\mathrm{Gal}(F/\mathbb{Q})$ satisfying $v_2 = v_1 \circ \sigma$.

We begin by briefly discussing the practical means by which we switch between facets of Π and their corresponding perfect forms. Moving from a facet to a form is simple: by **Proposition 4.2.2**, knowledge of the vertices of a facet $\mathcal{F}$ (the set of which contains a subset of minimal vectors of $\Phi_{\mathcal{F}}$ which spans $\mathcal{V}$ as a real vector space) immediately allows us to compute $\Phi_{\mathcal{F}}$ by solving a linear system of equations.

Conversely, given a perfect form Φ, we can define a quadratic form $Q : \mathcal{O}_F^2 \to \mathbb{Q}$ by

$$Q(x, y) = \tfrac{1}{2}\langle \Phi, q(x + y) - q(x) - q(y)\rangle$$

(note that by **Proposition 4.3.2**, since $\Phi \in \mathcal{C}(\mathbb{Q})$, this does indeed define a map into $\mathbb{Q}$).

By fixing a $\mathbb{Z}$-basis for $\mathcal{O}_F$, we can identify $\mathcal{O}_F^2$ with $\mathbb{Z}^8$, and compute the rational matrix A_Q of Q with respect to this matrix (note that, since Φ is a positive definite Hermitian form, A_Q is positive definite). We can then define an integral lattice L_Q equipped with an inner product given by

$$\langle P_1, P_2\rangle_Q = P_1^T A_Q P_2,$$

which can be constructed using MAGMA. Note that, if the point $x \in \mathcal{O}_F^2$ corresponds to P_x in L_Q, then

$$\langle \Phi, q(x)\rangle = Q(x, x) = \langle P_x, P_x\rangle_Q =: \|P_x\|_Q^2 ,$$

and so all minimal vectors of Φ correspond to points in L_Q of unit norm, and similarly all points in L_Q of unit norm give rise to a minimal vector (although multiple points can correspond to the same minimal vector).

Since A_Q is positive definite, the set of such vectors is finite, and may be enumerated (using standard routines in MAGMA), allowing us to reconstruct the minimal vectors of our form Φ.

We can therefore choose to work either with the set $M(\Phi)$ of minimal vectors of a perfect form Φ, or the set

$$\{x \in \mathcal{O}_F^2;\ q(x) \in M(\Phi)\}.$$

For computational efficiency, we prefer to work with smaller sets, and so choose to use $M(\Phi)$. However, there is in fact a potentially smaller set, which still retains all the information about the Koecher polytope, namely the set $M(\mathcal{F}_\Phi)$ of *vertices* of the facet $\mathcal{F}_\Phi$.

Recall from the previous section that we define the subset Ξ_{prim} to be the points $q(x), x \in \mathcal{O}_F^2$ that are minimal vectors of some perfect form, and that Π is the convex hull of Ξ_{prim}. In the classical situation, it is easy to see that

$$\Xi_{\text{prim}} = \left\{q(x);\ x \in \mathbb{Z}^2 \text{ is primitive}\right\},$$

where we say that $x = \left(\begin{smallmatrix} a \\ b \end{smallmatrix}\right)$ is primitive if $\gcd(a, b) = 1$. In fact, each such point corresponds to a vertex of Π, but this need not be the case for all fields.

We would therefore like to know how to determine precisely which minimal vectors are vertices. While this can be done simply by constructing the convex hull, this can be time consuming, so we would like to find a swifter method. The following result provides this:

Proposition 4.4.1. *Let F be a Galois quartic CM field, with trivial class group, and let Φ be a perfect form. Then there exists a minimal vector $q(x) \in M(\Phi)$ which is not a vertex of Π if, and only if, there exist at least three vectors $x_1, x_2, x_3 \in \mathcal{O}_F^2$ such that:*

(i) *The points $q(x_1)$, $q(x_2)$ and $q(x_3)$ are distinct minimal vectors of Φ; and*

(ii) *x_1, x_2 and x_3 are scalar multiples of each other.*

Proof. Suppose first that $q(x) \in M(\Phi)$ does not correspond to a vertex of Π. Multiplying by an element of $\mathrm{GL}_2(\mathcal{O}_F)$ if necessary, we may assume that $x = \left(\begin{smallmatrix} z \\ 0 \end{smallmatrix}\right)$ for some $z \in \mathcal{O}_F$ (since if $q(x)$ is a convex linear combination of points in $\mathcal{C}$, so too must $q(gx)$ be). Then we have $\lambda_1, \ldots, \lambda_r \in \mathbb{R}_+$ and $x_1, \ldots, x_r \in \mathcal{O}_F^2$ (where necessarily $r \geq 2$) such that

$$\sum_{i=1}^{r} \lambda_i q(x_i) = q(x)$$

and so, letting $x_i = \left(\begin{smallmatrix} u_i \\ v_i \end{smallmatrix}\right)$, we have in particular

$$\sum_{i=1}^{r} \lambda_i \begin{pmatrix} |u_i|^2 & u_i\overline{v}_i \\ \overline{u}_i v_i & |v_i|^2 \end{pmatrix} = \begin{pmatrix} |z|^2 & 0 \\ 0 & 0 \end{pmatrix}.$$

Since all of the λ_i are positive, it follows that we must have $v_i = 0$ for each i, and the result follows.

Conversely, suppose that we have three vectors $x_1, x_2, x_3 \in \mathcal{O}_F^2$ satisfying conditions (i) and (ii) and, without loss of generality, suppose they take the form $x_i = \left(\begin{smallmatrix} u_i \\ 0 \end{smallmatrix}\right)$ for some $u_i \in \mathcal{O}_F$. Note that if $|u_2|^2 = \lambda |u_3|^2$ for some $\lambda \in \mathbb{Q}$, then $\langle \Phi, q(x_2) \rangle = \lambda \langle \Phi, q(x_3) \rangle$, whence $\lambda = 1$, and $q(x_2) = q(x_3)$. Since the $q(x_i)$ are assumed distinct, this is not possible, and so $|u_2|^2$ and $|u_3|^2$ are two $\mathbb{Q}$-linearly independent elements of the quadratic field K, and thus form a $\mathbb{Q}$-basis for K. In particular, we have $|u_1|^2 = \lambda |u_2|^2 + \mu |u_3|^2$ for some $\lambda, \mu \in \mathbb{Q}$.

Now, since $|u_1|^2 > 0$, at most one of λ, μ can be negative. Thus (relabeling the x_i if necessary) we may assume that $q(x_1) = \lambda q(x_2) + \mu q(x_3)$, where $\lambda, \mu \in \mathbb{Q}_+$. Then

$$1 = \langle \Phi, q(x_1) \rangle = \lambda \langle \Phi, q(x_2) \rangle + \mu \langle \Phi, q(x_3) \rangle = \lambda + \mu,$$

and so $q(x_1)$ is a convex linear combination of $q(x_2)$ and $q(x_3)$, and thus is not a vertex of Π. □

Thus, given a perfect form Φ, we can construct the set of points $x \in \mathcal{O}_F^2$ such that $q(x) \in M(\Phi)$, and take a representative for each minimal vector. From these, it is a quick check to see whether or not we have a set of three vectors satisfying conditions (i) and (ii) above, and from each such set, it is easy to determine which of the corresponding minimal vectors is a convex combination of the other two. Omitting all such minimal vectors, we obtain the set $M(\mathcal{F}_\Phi)$ of vertices of the facet Φ.

To see that this is a valid concern, consider the field $F = \mathbb{Q}(t)$, where t denotes a primitive eighth root of unity. As we shall see in the next section, there is a perfect form $\Phi = [M, M^\sigma]$, where

$$M = \frac{1}{8} \begin{pmatrix} -t^3 + t + 2 & t^3 + t^2 - 1 \\ -t^2 - t - 1 & -t^3 + t + 2 \end{pmatrix}.$$

Now, for $x \in \mathcal{O}_F^2$, we have

$$\begin{aligned} \langle \Phi, q(x) \rangle &= 2\mathrm{Tr}(Mxx^*) + 2\mathrm{Tr}(M^\sigma x^\sigma x^{*,\sigma})) \\ &= \mathrm{Tr}_{F/\mathbb{Q}}(x^* M x). \end{aligned}$$

Using this, one can see that the points

$$X_1 = q\left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right), \; X_2 = q\left(\begin{smallmatrix} t^3 - t + 1 \\ 0 \end{smallmatrix}\right), \; X_3 = q\left(\begin{smallmatrix} 1 - t \\ 0 \end{smallmatrix}\right)$$

are all minimal vectors of Φ, and we have

$$X_3 = \tfrac{1}{2} X_1 + \tfrac{1}{2} X_2,$$

as expected (note too that the vector $\left(\begin{smallmatrix} 1 - t \\ 0 \end{smallmatrix}\right)$ is not primitive, as $\mathrm{Norm}_{F/\mathbb{Q}}(1 - t) = 2$).

We remark that, as we would hope, primitive vectors in $\mathcal{O}_F^2$ do still correspond to vertices of Π:

Corollary 4.4.2. *If $x \in \mathcal{O}_F^2$ is primitive, then $q(x)$ is a vertex of Π.*

Proof. Without loss of generality, we may assume that $x = \left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right)$. If $q(x)$ is not a vertex of Π, then we have $x_1, x_2 \in \mathcal{O}_F^2$ and $\lambda_1, \lambda_2 \in \mathbb{Q}_+$, with $\lambda_1 + \lambda_2 = 1$, such that $q(x) = \lambda_1 q(x_1) + \lambda_2 q(x_2)$, and thus $x_i = \left(\begin{smallmatrix} a_i \\ 0 \end{smallmatrix}\right)$ for some $a_i \in \mathcal{O}_F$. It therefore suffices to show that it is not possible to write

$$1 = \lambda |a_1|^2 + (1-\lambda)|a_2|^2$$

where $0 < \lambda < 1$ and $a_1, a_2 \in \mathcal{O}_F$, with neither of the a_i torsion units.

More generally, we will show that it is not possible to express

$$1 = \lambda w_1 + (1-\lambda) w_2$$

where $0 < \lambda < 1$ and $w_1, w_2 \in \mathcal{O}_K$ are totally positive, unless $w_1 = w_2 = 1$. Indeed, since K is a real quadratic field, it is isomorphic to $\mathbb{Q}(\sqrt{d})$ for some positive square-free integer d. If $d \not\equiv 1 \pmod 4$, then write $w_i = u_i + v_i\sqrt{d}$. Then

$$1 = \mathbb{R}\mathrm{e}[\lambda w_1 + (1-\lambda) w_2] = \lambda u_1 + (1-\lambda) u_2.$$

Since the w_i are totally positive, $u_i \geq 1$, with equality if, and only if, $v_i = 0$. But since $\lambda > 0$, this equation can only hold if $u_1 = u_2 = 1$, as required.

If $d \equiv 1 \pmod 4$, then write $w_i = (u_i + \frac{1}{2}v_i) + \frac{1}{2}v_i\sqrt{d}$. Then

$$1 = \mathbb{R}\mathrm{e}[\lambda w_1 + (1-\lambda) w_2] = \lambda(u_1 + \frac{1}{2}v_1) + (1-\lambda)(u_2 + \frac{1}{2}v_2).$$

Note that, since each w_i is totally positive, we must have $(u_i + \frac{1}{2}v_i) \geq 1$. Indeed, if $(u_i + \frac{1}{2}v_i) = \frac{1}{2}$, then $v_i = 1 - 2u_i$, so $|v_i| \geq 1$. Since $d \geq 5$, $|\frac{1}{2}v_i\sqrt{d}| > \frac{1}{2}$, and so either w_i or its conjugate is negative, contradicting the assumption that w_i be totally positive. Thus we must have $(u_i + \frac{1}{2}v_i) = 1$, whence $v_i = 2 - 2u_i$, so either $v_i = 0$ or $|v_i| \geq 2$. The latter assumption again leads us to conclude that w_i is not totally positive, so $v_i = 0$, and $w_i = 1$, as required. □

As a final note, we recall that throughout the previous chapter, we had assumed that the Koecher polytope satisfied the conditions of **Proposition 4.3.1**, namely that no facet of Π was contained completely in the boundary $\partial\mathcal{C} = \overline{\mathcal{C}} \setminus \mathcal{C}$ of $\mathcal{C}$. We can now justify this claim:

Proposition 4.4.3. *If a face $\mathcal{E}$ of the Koecher polytope Π is contained completely in the boundary $\partial\mathcal{C}$, then $\mathcal{E}$ has at most two vertices.*

Moreover, a non-vertex point in Π lies in the boundary $\partial\mathcal{C}$ if, and only if, it is contained in such a face.

Proof. Let Φ be a perfect form, and let $x, y \in \mathcal{O}_F^2$ such that $q(x)$ and $q(y)$ are distinct minimal vectors of Φ. Without loss of generality, assume that $x = \left(\begin{smallmatrix} a \\ 0 \end{smallmatrix}\right)$ and $y = \left(\begin{smallmatrix} u \\ v \end{smallmatrix}\right)$ for some $a, u, v \in \mathcal{O}_F$, with a non-zero. Then the cone spanned by $q(x)$ and $q(y)$ is contained in the boundary if, and only if

$$\lambda \begin{pmatrix} |a|^2 & 0 \\ 0 & 0 \end{pmatrix} + (1-\lambda) \begin{pmatrix} |u|^2 & u\bar{v} \\ \bar{u}v & |v|^2 \end{pmatrix}$$

is semi-definite for all $\lambda \in [0,1]$, i.e., if, and only if,

$$\lambda(1-\lambda)|a|^2|v|^2 = 0$$

for all $\lambda \in [0,1]$, which occurs if, and only if, $v = 0$, i.e., x and y lie in the same F-span.

Thus a face is contained within the boundary if, and only if, the vectors corresponding to its vertices span a 1-dimensional vector space. But by **Proposition 4.4.1**, these can correspond to at most two such vertices in any given cone.

For the second statement, suppose we have vertices $q(x_1), \ldots, q(x_r)$ and $\lambda_1, \ldots, \lambda_r \in \mathbb{R}_+$ such that

$$\sum_{i=1}^{r} \lambda_i q(x_i) \in \partial\mathcal{C},$$

and assume without loss of generality that $x_1 = \left(\begin{smallmatrix} a \\ 0 \end{smallmatrix}\right)$. Then, writing the remaining sum as $\left(\begin{smallmatrix} u & v \\ \bar{v} & w \end{smallmatrix}\right)$, where $u, w \in \mathcal{O}_K^+$ and $uw - |v|^2 \in \mathcal{O}_K^+ \cup \{0\}$ (since the sum defines a point in $\overline{\mathcal{C}}$), we must have $\lambda_1|a|^2w + (uw - |v|^2) = 0$, whence $v = w = 0$. Thus $x_1, \ldots, x_r$ all lie in the same F-span, so $r \leq 2$, and the result follows. $\square$

Thus clearly no facet of Π (whose vertices by definition must span the real vector space $\mathcal{V}$) can be contained fully in the boundary of $\mathcal{C}$.

4.5 Examples

We illustrate these ideas by providing details of the decomposition of the Koecher polytope for three examples of quartic CM fields F of small discriminant.

4.5.1 The Field F_1

Let $F_1 = \mathbb{Q}(t)$, where $t = \zeta_{12}$ denotes a primitive twelfth root of unity. Let $\sigma \in \mathrm{Gal}(F/\mathbb{Q})$ be the automorphism of F sending t to t^7. There are two equivalence classes of perfect forms under the action of $\mathrm{GL}_2(\mathcal{O}_F)$, with representatives given by the Hermitian forms $[M_1, M_1^\sigma]$ and $[M_2, M_2^\sigma]$, where

$$M_1 = \frac{1}{12}\begin{pmatrix} -t^3+2t+3 & 2t^3+t^2-t-2 \\ -t^3-t^2-t-1 & -t^3+2t+3 \end{pmatrix}$$

and

$$M_2 = \frac{1}{12}\begin{pmatrix} -t^3+2t+3 & 3t^3+t^2-t-2 \\ t^3-t^2-t-1 & -t^3+2t+5 \end{pmatrix},$$

whose corresponding perfect pyramids have 20 and 8 vertices respectively.

We present details of the decomposition of the Koecher polytope below. By a *boundary face* we mean a face of Π that lies completely within the bondary $\partial\mathcal{C}$ of the cone of positive definite forms; the columns denoted *simplicial* and *non-simplicial faces* implicitly refer to faces which have non-trivial intersection with $\mathcal{C}$.

Dimension	Simplicial Faces	Non-Simplicial Faces	Boundary Faces	Total
1	1	0	1	2
2	4	0	0	4
3	12	1	0	13
4	15	2	0	17
5	11	3	0	14
6	4	2	0	6
7	1	1	0	2

We also note:

- There is a single 3-dimensional non-simplicial face, with 6 vertices.
- There are two 4-dimensional non-simplicial faces, each with 7 vertices.
- There are three 5-dimensional non-simplicial faces, each with 8 vertices.
- There is one 6-dimensional non-simplicial face with 10 vertices, and one with 11 vertices.
- The single 7-dimensional non-simplicial face has 20 vertices, as noted previously.

4.5.2 The Field F_2

Let $F_2 = \mathbb{Q}(t)$, where t is a root of the polynomial $x^4 - x^3 + 2x^2 + x + 1$. Let $\sigma \in \mathrm{Gal}(F/\mathbb{Q})$ be the automorphism of F sending t to $t^3 - t^2 + 2t + 1$. There are two equivalence classes of perfect forms under the action of $\mathrm{GL}_2(\mathcal{O}_F)$, with representatives given by the Hermitian forms $[M_1, M_1^\sigma]$ and $[M_2, M_2^\sigma]$, where

$$M_1 = \frac{1}{60}\begin{pmatrix} 3t^3 + 21 & -12t^3 + 14t^2 - 22t - 8 \\ 6t^3 - 14t^2 + 22t - 4 & 3t^3 + 21 \end{pmatrix}$$

and

$$M_2 = \frac{1}{60}\begin{pmatrix} 3t^3 + 51 & -28t^3 + 30t^2 - 40t - 16 \\ 7t^3 - 30t^2 + 40t - 11 & 30 \end{pmatrix},$$

whose corresponding perfect pyramids have 40 and 8 vertices respectively.

As before, we present details of the decomposition of the Koecher polytope:

Dimension	Simplicial Faces	Non-Simplicial Faces	Boundary Faces	Total
1	1	0	1	1
2	4	1	0	5
3	9	2	0	11
4	7	7	0	14
5	4	6	0	10
6	2	4	0	6
7	1	1	0	2

We also note:

- There is a single 2-dimensional non-simplicial face, with 4 vertices.
- There are two 3-dimensional non-simplicial faces, each with 5 vertices.
- There are four 4-dimension non-simplicial faces with 6 vertices, and three with 7 vertices.
- There is a single 5-dimensional non-simplicial face with 8 vertices, two with 9 vertices, and three with 10 vertices.
- There is a single 6-dimensional non-simplicial face with 12 vertices, two with 15 vertices, and one with 20 vertices.
- The single 7-dimensional non-simplical face has 40 vertices, as noted previously.

4.5.3 The Field F_3

Let $F_3 = \mathbb{Q}(t)$, where $t = \zeta_8$ denotes a primitive eighth root of unity. Let $\sigma \in \mathrm{Gal}(F/\mathbb{Q})$ denote the automorphism of F sending t to t^3. There are three equivalence classes of perfect forms under the action of $\mathrm{GL}_2(\mathcal{O}_F)$, with representatives given by the Hermitian forms $[M_1, M_1^\sigma], [M_2, M_2^\sigma]$ and $[M_3, M_3^\sigma]$, where

$$M_1 = \frac{1}{16}\begin{pmatrix} -2t^3+2t+4 & -t^2-2t-2 \\ 2t^3+t^2-2 & -2t^3+2t+4 \end{pmatrix},$$

$$M_2 = \frac{1}{8}\begin{pmatrix} -t^3+t+2 & -t^3-2t^2-2t-1 \\ 2t^3+2t^2+t-1 & -4t^3+4t+6 \end{pmatrix}$$

and

$$M_3 = \frac{1}{8}\begin{pmatrix} -t^3+t+2 & t^3+t^2-1 \\ -t^2-t-1 & -t^3+t+2 \end{pmatrix},$$

whose corresponding perfect pyramids have 12, 12 and 24 vertices respectively.

As before, we present details of the decomposition of the Koecher polytope:

Dimension	Simplicial Faces	Non-Simplicial Faces	Boundary Faces	Total
1	2	0	1	3
2	8	0	0	8
3	23	1	0	24
4	33	4	0	37
5	27	7	0	34
6	4	10	0	14
7	0	3	0	3

We also note:

- There is a single 3-dimensional non-simplicial face, with 6 vertices.
- There are two 4-dimensional non-simplicial faces with 6 vertices, and two with 7 vertices.
- There are four 5-dimensional non-simplicial faces with 7 vertices, and three with 8 vertices.
- There are four 6-dimensional non-simplicial faces with 8 vertices, four with 9 vertices, one with 10 vertices, and one with 11 vertices.
- There are two 7-dimensional non-simplicial faces with 12 vertices, and one with 24 vertices, as noted previously.

Chapter 5

The Cohomology of Arithmetic Subgroups

This chapter concerns the practical computation of both the group cohomology $H^*(\Gamma_0(\mathfrak{n}), \mathbb{C})$ and the Hecke action on cohomology classes. We begin in **Section 5.1** by presenting a cell complex, known as the *sharbly complex*, whose homology is dual to the group cohomology we wish to study, and which exhibits a Hecke action.

Section 5.2 provides an in-depth explanation of how we can compute the group cohomology via the homology of the sharbly complex, and the techniques required in order to compute the Hecke action on classes in the sharbly homology. In **Section 5.3** we present details of Hecke eigenclasses in the sharbly homology which correspond to cuspidal automorphic forms, while in **Section 5.4** we discuss some of the practical issues regarding our computations.

5.1 The Sharbly Complex

We now move towards our main task of finding modular elliptic curves, beginning by studying the automorphic representations with which we hope to match such curves. As before, let F be a number field, with ring of integers $\mathcal{O}_F$, and set $G = \mathrm{Res}_{F/\mathbb{Q}}(\mathrm{GL}_2)$. We shall assume throughout that F has trivial class group, and signature $[r, s]$. Given an ideal $\mathfrak{n}$ of F, define an arithmetic subgroup $\Gamma_0(\mathfrak{n})$ of $G(\mathbb{Q}) \simeq \mathrm{GL}_2(F)$ to be the subgroup

$$\Gamma_0(\mathfrak{n}) := \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathcal{O}_F);\ c \in \mathfrak{n} \right\}.$$

Let S_f denote the set of finite places of F. Similarly to the classical case in **Section 3.2**, define a compact subgroup $K_0(\mathfrak{n})$ of

$$G(\mathbb{A}_f) \simeq \prod_{v \in S_f} \mathrm{GL}_2(F_v)$$

to be the product of the subgroups $K_v(\mathfrak{n})$ for $v \in S_f$, where

$$K_v(\mathfrak{n}) = \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathcal{O}_v);\ c \equiv 0 \pmod{\mathfrak{n}} \right\}$$

if v divides $\mathfrak{n}$, and $K_v(\mathfrak{n}) = \mathrm{GL}_2(\mathcal{O}_v)$ otherwise.

Then, denoting by X the symmetric space $G(\mathbb{R})/A_G^0(\mathbb{R})K_\infty$, we have (since F is assumed to have trivial class group) an identification

$$\Gamma_0(\mathfrak{n})\backslash X \simeq A_G^0(\mathbb{R})G(\mathbb{Q})\backslash G(\mathbb{A})/K_\infty K_0(\mathfrak{n}),$$

as in **Section 3.4**. By the results of that section, we can realise automorphic representations through the cohomology of the locally symmetric space $\Gamma_0(\mathfrak{n})\backslash X$. In turn (as for the classical case in **Section 2.6**), we can identify this with the group cohomology $H^*(\Gamma_0(\mathfrak{n}), \mathbb{C})$.

There are two main approaches for computing this cohomology. The first is perhaps the most obvious; using the Koecher decomposition of the symmetric space X, one can naturally construct a cell complex using the resulting Koecher cells. One can then compute the cohomology of $\Gamma_0(\mathfrak{n})\backslash X$ by computing the $\Gamma_0(\mathfrak{n})$-equivariant cohomology of this complex - since there are only finitely many Koecher cells under the action of $\Gamma_0(\mathfrak{n})$, this computation can indeed be performed in practice.

We shall take a second approach, which has noticeable advantages over the first. The trouble with working with the Koecher cell complex is that it is fairly restrictive - the Hecke operators which we shall later want to compute do not preserve the Koecher cells, and so we cannot hope to compute their action on the cohomology using this method. The approach which we shall now explain allows us to compute both the cohomology *and* the Hecke action, by working with a much larger space.

To begin with, we require a few preliminary notions. Let Γ be an arbitrary arithmetic subgroup of $G(\mathbb{Q})$, for G a reductive algebraic group defined over $\mathbb{Q}$. If Γ is torsion-free, we define the *cohomological dimension* of Γ to be the smallest integer ν such that $H^{\nu+1}(\Gamma, M) = 0$ for all coefficient systems M. For an arbitrary arithmetic subgroup Γ, we define the *virtual comological dimension* ν of Γ to be the cohomological dimension of any finite-index torsion-free subgroup (this is known to be well-defined).

A formula for the virtual cohomological dimension is given by the following result (see **[BS73], Theorem 11.4.4**):

Theorem 5.1.1. *Let G be a reductive $\mathbb{Q}$-group, R its radical, and*

$$X = G(\mathbb{R})/A_G^0(\mathbb{R})K$$

a globally symmetric space, where $A_G^0(\mathbb{R})$ denotes the split component of $G(\mathbb{R})$ and K is a maximal compact subgroup of $G(\mathbb{R})$. Then for any arithmetic subgroup Γ of $G(\mathbb{Q})$, we have

$$\nu = \dim(X) - \mathrm{rk}_{\mathbb{Q}}(G/R).$$

Returning to the case of $G = \mathrm{Res}_{F/\mathbb{Q}}(\mathrm{GL}_2)$, where we recall that F has signature $[r, s]$, the radical R is the subgroup of diagonal matrices, and subsequently $\mathrm{rk}_{\mathbb{Q}}(G/R) = 1$, while we have seen previously that $\dim(X) = 3r+4s-1$, and so

$$\nu = 3r + 4s - 2$$

for each arithmetic subgroup Γ of $G(\mathbb{Q})$.

Next, let $\mathbb{P}^1(F)$ denote the projective line over our field F, and let $\mathbb{Z}[\mathbb{P}^1(F)]$ denote the free abelian group generated by it. One defines the *augmentation map* $\epsilon : \mathbb{Z}[\mathbb{P}^1(F)] \to \mathbb{Z}$ by

$$\epsilon\left(\sum n_P P\right) = \sum n_P,$$

and subsequently we define the *Steinberg module* St_2 for $\mathrm{GL}_2(F)$ by the short exact sequence

$$0 \longrightarrow \mathrm{St}_2 \longrightarrow \mathbb{Z}[\mathbb{P}^1(F)] \xrightarrow{\epsilon} \mathbb{Z} \longrightarrow 0.$$

This clearly admits an action of $\mathrm{GL}_2(F)$, induced by the action on $\mathbb{P}^1(F)$.

The Steinberg module is a *dualizing module* for $\Gamma_0(\mathfrak{n})$ (in the sense of **[BS73], Section 11.4**) and so we have

$$H^{\nu-k}(\Gamma_0(\mathfrak{n}), \mathbb{C}) \simeq H_k(\Gamma_0(\mathfrak{n}), \mathrm{St}_2 \otimes_{\mathbb{Z}} \mathbb{C}),$$

a result known as *Borel-Serre duality*.

To compute the homology of $\Gamma_0(\mathfrak{n})$ with coefficients in the Steinberg module, we require an appropriate resolution of St_2. Such a resolution is provided for us by the *sharbly complex*. This is defined as follows: for each k, let A_k denote the $\mathbb{Z}$-module of $\mathbb{Z}$-linear combinations of $(k+2)$-tuples $\mathbf{u} = [u_1, \ldots, u_{k+2}]$, where $u_i \in \mathcal{O}_F^2$. In addition, let R_k denote the submodule generated by the relations:

- $[u_1, \ldots, u_{k+2}] - \mathrm{sgn}(\sigma)[u_{\sigma(1)}, \ldots, u_{\sigma(k+2)}]$, for any permutation $\sigma \in S_{k+2}$;
- $[u, u_2, \ldots, u_{k+2}] - [v, u_2, \ldots, u_{k+2}]$, for any $u, v \in \mathcal{O}_F^2$ with $q(u) = \lambda q(v)$, for some $\lambda \in \mathbb{R}_+$;
- $[u_1, \ldots, u_{k+2}]$, if the F-span of the vectors $u_1, \ldots, u_{k+2}$ is 1-dimensional (we call such sharblies *degenerate*).

We then define the $\mathbb{Z}$-module of *k-sharblies* to be the quotient

$$\mathscr{S}_k = A_k / R_k.$$

Using the relations in R_k, we shall always assume that the vectors $u_i \in \mathcal{O}_F^2$ satisfy the property that there is no point of Ξ on the line segment joining $q(u_i)$ with the origin (that is, if $v_i \in \mathcal{O}_F^2$ with $q(v_i) = \lambda q(u_i)$ for some $\lambda \in \mathbb{R}_+$, then $\lambda \geq 1$).

One can define a boundary map $\partial : \mathscr{S}_k \to \mathscr{S}_{k-1}$ by

$$\partial([u_1, \ldots, u_{k+2}]) = \sum_{i=1}^{k+2} (-1)^{i+1} [u_1, \ldots, \hat{u}_i, \ldots, u_{k+2}],$$

where $\hat{u}_i$ indicates that we omit u_i. The resulting complex $\mathscr{S}_*$ is called the *sharbly complex*. The sharbly complex admits an obvious action of $\mathrm{GL}_2(\mathcal{O}_F)$, given by

$$g \cdot [u_1, \ldots, u_{k+2}] = [gu_1, \ldots, gu_{k+2}], \ g \in \mathrm{GL}_2(\mathcal{O}_F),$$

and this clearly commutes with the boundary map. In particular, for any subgroup Γ of $\mathrm{GL}_2(\mathcal{O}_F)$, we can define the quotient of Γ-*coinvariants*, $(\mathscr{S}_*)_\Gamma$, by enforcing the additional relation

- $[u_1, \ldots, u_{k+2}] - \gamma \cdot [u_1, \ldots, u_{k+2}]$ for all $\gamma \in \Gamma$.

One can define a map $\phi : \mathscr{S}_0 \to \mathrm{St}_2$ as follows: given $u \in \mathcal{O}_F^2$, let $[u]$ denote the line spanned by u, viewed as an element of $\mathbb{P}^1(F)$. Then, given $\mathbf{u} = [u_1, u_2] \in \mathscr{S}_0$, we define

$$\phi(\mathbf{u}) = [u_1] - [u_2].$$

This map is well-defined: indeed, the first and third relations defining the sharbly complex clearly have no effect on ϕ. For the second, suppose that $q(u) = \lambda q(v)$ for some $\lambda \in \mathbb{R}_+$ and $u, v \in \mathcal{O}_F^2$. Without loss of generality (since the map ϕ is $\mathrm{GL}_2(F)$-equivariant) we may assume that $u = \left(\begin{smallmatrix} a \\ 0 \end{smallmatrix}\right)$ and so $v = \left(\begin{smallmatrix} b \\ 0 \end{smallmatrix}\right)$, whence $u = ba^{-1}v$. Since $a, b \in \mathcal{O}_F$, $ba^{-1} \in F$, and so $[u] = [v]$, as required.

Consequently, we can define a sequence

$$\ldots \xrightarrow{\partial} \mathscr{S}_k \xrightarrow{\partial} \ldots \xrightarrow{\partial} \mathscr{S}_1 \xrightarrow{\partial} \mathscr{S}_0 \xrightarrow{\phi} \mathrm{St}_2 \xrightarrow{\epsilon} 0.$$

In fact (see **[AGM11], Theorem 5**) this sequence is exact, and thus provides an acyclic resolution of the Steinberg module. In particular, we have an isomorphism

$$H^{\nu-k}(\Gamma_0(\mathfrak{n}), \mathbb{C}) \simeq H_k((\mathscr{S}_*)_{\Gamma_0(\mathfrak{n})}, \mathbb{C}),$$

the latter of which is straightforward to determine computationally.

All the results we have stated apply to an arbitrary number field. Henceforth, with the results of **Section 3.5** in mind, we shall specialize to CM fields. In fact, we shall restrict ourselves further to *quartic* CM fields, for reasons which shall soon become apparent. In this case, F has signature $[0, 2]$, and thus the virtual cohomological dimension of any subgroup $\Gamma_0(\mathfrak{n})$ is 6, by **Theorem 5.1.1**. In addition, by **Corollary 3.4.2**, we have

$$H^i_{\mathrm{cusp}}(\Gamma_0(\mathfrak{n}), \mathbb{C}) = 0 \text{ if } i \notin [2, 5],$$

so the smallest degree of the sharbly homology in which we could hope to study cuspidal classes is degree 1. In the next section, we shall describe a method for computing the Hecke action on these particular homology groups.

5.2 Hecke Operators and Sharbly Reduction

The action of $\mathrm{GL}_2(\mathcal{O}_F)$ on $(\mathscr{S}_*)_\Gamma$ (for an arithmetic subgroup Γ of $\mathrm{GL}_2(\mathcal{O}_F)$) extends readily to an action of the subgroup $M_2(\mathcal{O}_F) \cap \mathrm{GL}_2(F)$ of $\mathrm{GL}_2(F)$. In particular, suppose $g \in \mathrm{GL}_2(F)$ such that the groups $\Gamma_1 := \Gamma \cap g^{-1}\Gamma g$ and $\Gamma_2 := \Gamma \cap g\Gamma g^{-1}$ have finite index in Γ. Then the resulting Hecke correspondence:

$$\begin{array}{ccc} \Gamma_1 & \xrightarrow{\alpha_g} & \Gamma_2 \\ {\scriptstyle \iota_1}\downarrow & & \downarrow{\scriptstyle \iota_2} \\ \Gamma & & \Gamma \end{array}$$

where ι_i denotes the inclusion $\Gamma_i \hookrightarrow \Gamma$, and α_g is the homomorphism

$$\Gamma_1 \to \Gamma_2, \gamma \mapsto g\gamma g^{-1}$$

defines in turn a correspondence on homology groups:

$$\begin{array}{ccc} H_1(\mathscr{S}_{\Gamma_1}, \mathbb{C}) & \xrightarrow{\alpha_{g,*}} & H_1(\mathscr{S}_{\Gamma_2}, \mathbb{C}) \\ {\scriptstyle \iota_1^*}\uparrow & & \downarrow{\scriptstyle \iota_{2,*}} \\ H_1(\mathscr{S}_\Gamma, \mathbb{C}) & & H_1(\mathscr{S}_\Gamma, \mathbb{C}) \end{array}.$$

Working through the definitions, it is not difficult to see that the corresponding Hecke operator T_g acts on $(\mathscr{S}_*)_\Gamma$ via

$$T_g(\mathbf{u}) = \sum_{i=1}^{n} g_i \cdot \mathbf{u},$$

where we have a decomposition of the double coset space

$$\Gamma g \Gamma = \coprod_{i=1}^{n} \Gamma g_i.$$

Most importantly, the isomorphism

$$H^{\nu-k}(\Gamma_0(\mathfrak{n}), \mathbb{C}) \simeq H_k((\mathscr{S}_*)_{\Gamma_0(\mathfrak{n})}, \mathbb{C}),$$

is *Hecke equivariant* (see, for example, **[AGM13], Theorem 2.4**), meaning that it commutes with the action of the Hecke operators on the respective spaces.

In particular, let $\Gamma = \Gamma_0(\mathfrak{n})$ for some ideal $\mathfrak{n}$ of F, and let $g = \left(\begin{smallmatrix} 1 & 0 \\ 0 & \nu \end{smallmatrix}\right)$, where ν generates a prime ideal $\mathfrak{p}$ of F not dividing $\mathfrak{n}$. Then, by the results of **Section 3.4** and the previous section, we can use the homology of the sharbly complex to compute the Hecke action on the corresponding spaces of cusp forms.

It is straightforward to compute a set of representatives g_i for the double coset $\Gamma_0(\mathfrak{n})\left(\begin{smallmatrix}1&0\\0&\nu\end{smallmatrix}\right)\Gamma_0(\mathfrak{n})$, as the following result shows:

Proposition 5.2.1. *Let $\mathfrak{p}$ be a prime ideal of a number field F with trivial class group, with generator ν, and let $\alpha_0, \ldots, \alpha_{q-1}$ be a representative set of lifts of the elements of $\mathcal{O}_F/\mathfrak{p}$. Then a set of representatives for the g_i is given by*

$$\left\{ \begin{pmatrix} 1 & \alpha_1 \\ 0 & \nu \end{pmatrix}, \ldots, \begin{pmatrix} 1 & \alpha_{q-1} \\ 0 & \nu \end{pmatrix}, \begin{pmatrix} \nu & 0 \\ 0 & 1 \end{pmatrix} \right\}.$$

Moreover, any set of representatives gives the same Hecke action.

Proof. This is a standard result, but for the sake of completeness we give a proof. Let $\gamma = \left(\begin{smallmatrix}a&b\\c&d\end{smallmatrix}\right) \in \Gamma_0(\mathfrak{n})$, and note that

$$\begin{pmatrix} 1 & 0 \\ 0 & \nu \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & \alpha_i \\ 0 & \nu \end{pmatrix}^{-1} = \begin{pmatrix} a & \nu^{-1}(b - a\alpha_i) \\ \nu c & d \end{pmatrix},$$

and

$$\begin{pmatrix} 1 & 0 \\ 0 & \nu \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \nu & 0 \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} \nu^{-1}a & b \\ c & \nu d \end{pmatrix}.$$

If $a \in \mathfrak{p}$, then the right-hand matrix in the second equation lies in $\Gamma_0(\mathfrak{n})$. If $a \notin \mathfrak{p}$, then $b - a\alpha_i \in \mathfrak{p}$ for some α_i, and thus the right-hand matrix in the first equation belongs to $\Gamma_0(\mathfrak{n})$. Thus the cosets $\Gamma_0(\mathfrak{n})g_i$ cover $\Gamma_0(\mathfrak{n})\left(\begin{smallmatrix}1&0\\0&\nu\end{smallmatrix}\right)\Gamma_0(\mathfrak{n})$.

Next, we note that $\Gamma_0(\mathfrak{n})g_i \neq \Gamma_0(\mathfrak{n})g_j$ if $i \neq j$, i.e., the union is disjoint. To see this, we note that

$$\begin{pmatrix} 1 & \alpha_i \\ 0 & \nu \end{pmatrix} \begin{pmatrix} 1 & \alpha_j \\ 0 & \nu \end{pmatrix}^{-1} = \begin{pmatrix} 1 & \nu^{-1}(\alpha_i - \alpha_j) \\ 0 & 1 \end{pmatrix},$$

while

$$\begin{pmatrix} 1 & \alpha_i \\ 0 & \nu \end{pmatrix} \begin{pmatrix} \nu & 0 \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} \nu^{-1} & \alpha_i \\ 0 & \nu \end{pmatrix}.$$

The latter is clearly not an element of $\mathrm{GL}_2(\mathcal{O}_F)$ while the former only belongs to $\Gamma_0(\mathfrak{n})$ if $\nu^{-1}(\alpha_i - \alpha_j) \in \mathcal{O}_F$, i.e., if α_i and α_j project to the same element in $\mathcal{O}_F/\mathfrak{p}$, which implies that $i = j$.

Now, suppose we have two sets of representatives $\{g_1, \ldots, g_n\}$ and $\{g'_1, \ldots, g'_n\}$. Then, after reordering if necessary, we must have $g'_i = \gamma_j g_j$ for some $\gamma_i \in \Gamma_0(\mathfrak{n})$. But then

$$\sum_{i=1}^{n} g'_i \cdot \mathbf{u} = \sum_{i=1}^{n} \gamma_i \cdot (g_i \cdot \mathbf{u}) = \sum_{i=1}^{n} g_i \cdot \mathbf{u}$$

for any sharbly $\mathbf{u}$, using the relations on $(\mathscr{S}_*)_{\Gamma_0(\mathfrak{n})}$, and thus both sets of representatives yield the same Hecke action. □

One problem soon becomes apparent: the operators $T_{\mathfrak{p}}$ do not preserve any finitely-generated submodule of $\mathscr{S}_k$ for any k. Indeed, suppose we define a notion of the "size" of a sharbly as follows (a definition that we borrow from **[GHY13]**): given a 0-sharbly $\mathbf{u} = [u_1, u_2]$, define the size of $\mathbf{u}$ to be the absolute value of $\mathrm{Norm}_{F/\mathbb{Q}}(\det(u_1|u_2))$, where $(u_1|u_2)$ is the matrix with columns given by the vectors u_1 and u_2. One can see that this is well-defined: indeed, we observe that $\det(u_1|u_2) = \det(u_1u_1^* + u_2u_2^*)$, and the conditions we have imposed on the sharbly complex means that the points $u_1u_1^*$ and $u_2u_2^*$ are uniquely determined (since the points $q(u_1)$ and $q(u_2)$ are).

We can extend this notion to an arbitrary k-sharbly $\mathbf{u}$ by defining the size of $\mathbf{u}$ to be the maximal size of a 0-sharbly $\mathbf{u}'$ formed using any of the columns of $\mathbf{u}$. Then, given any prime ideal $\mathfrak{p}$ and a sharbly $\mathbf{u}$, we have $\mathrm{Norm}_{F/\mathbb{Q}}(\det(\gamma_i)) = \mathrm{Norm}_{F/\mathbb{Q}}(\mathfrak{p})$ for each representative γ_i from the corresponding double coset decomposition, and so the Hecke operator will, in general, increase the size of any given sharbly.

We therefore take the following approach: for each value of k, we choose a finite set of k-sharblies, and consider the subcomplex of $(\mathscr{S}_*)_{\Gamma_0(\mathfrak{n})}$ generated by these sets. Suppose that the homology in degree k of this subcomplex is isomorphic to that of the whole complex $(\mathscr{S}_*)_{\Gamma_0(\mathfrak{n})}$ (which can be ascertained by comparing Betti numbers, for example) and that, given a cycle $\xi \in (\mathscr{S}_k)_{\Gamma_0(\mathfrak{n})}$, one can construct a homologous cycle ξ' whose support consists entirely of sharblies contained in our finite set. Then, given a basis for the homology in degree k of our subcomplex, we can apply a given Hecke operator to each basis cycle in turn, and then rewrite the resulting cycle in terms of our original basis, allowing us to effectively compute the Hecke action.

Our choice of subcomplex is as follows: call a k-sharbly $\mathbf{u} = [u_1, \ldots, u_{k+2}]$ *totally reduced* if the points $\{q(u_1), \ldots, q(u_{k+2})\}$ are the vertices of a face of the Koecher polytope Π. Then we take the subcomplex generated by the totally reduced sharblies to be our object of study. Note that, since there are only finitely many faces of Π modulo the action of $\Gamma_0(\mathfrak{n})$, there are only finitely many totally reduced sharblies up to $\Gamma_0(\mathfrak{n})$-equivalence, and so this subcomplex is indeed finitely-generated. For each of the fields we have studied, this particular choice of subcomplex proves to be sufficient, in that the algorithm which follows always produces a sharbly chain whose support consists of totally reduced sharblies.

At this point we remark that our choice of subcomplex differs from that in **[GHY13]**. They define a sharbly $\mathbf{u} = [u_1, \ldots, u_{k+2}]$ to be *reduced* if the points $\{q(u_1), \ldots, q(u_{k+2})\}$ are a *subset* of the vertices of some face of Π. This produces, in general, a much larger subcomplex than that generated by totally reduced sharblies, but (after enforcing some additional relations on the sharbly complex) accounts for non-simplicial faces of Π - our definition of a totally reduced sharbly only corresponds to a *simplicial* face of Π. However, all of our computations match up to those of the aforementioned paper. We shall make use of both the terms *reduced* and *totally reduced* in the sequel.

We will give a new definition of the *size* of a sharbly. Given a sharbly $\mathbf{u} = [u_1, \ldots, u_{k+2}]$, let

$$\mathcal{B}(\mathbf{u}) = \sum_{i=1}^{k+2} q(u_i),$$

and let $\mathcal{F}_{\mathbf{u}}$ and $\Phi_{\mathbf{u}}$ denote the facet of Π above which $\mathcal{B}(\mathbf{u})$ lies and the perfect form corresponding to $\mathcal{F}_{\mathbf{u}}$ respectively (so that $\langle \Phi_{\mathbf{u}}, \mathcal{B}(\mathbf{u}) \rangle$ is minimal amongst all perfect forms). We then define the *size* $N(\mathbf{u})$ of $\mathbf{u}$ to be

$$N(\mathbf{u}) = \langle \Phi_{\mathbf{u}}, \mathcal{B}(\mathbf{u}) \rangle.$$

Note that $N(\mathbf{u}) \geq k+2$, with equality if, and only if, $\mathbf{u}$ is totally reduced (as $N(\mathbf{u}) = k+2$ if, and only if, $\langle \Phi_{\mathbf{u}}, q(u_i) \rangle = 1$ for all $i = 1, \ldots, k+2$, i.e., if, and only if, each $q(u_i)$ is a vertex of $\mathcal{F}_{\mathbf{u}}$). This does not distinguish between reduced and totally reduced sharblies, however.

It seems that the two notions of size (ours and that given in **[GHY13]**) appear to correspond, in the sense that if a sharbly has small size according to one definition, then it has according to the other also, although we are unable to prove an exact relation between the two. The definition of **[GHY13]** seems, in practice, to distinguish between reduced and totally reduced sharblies (for example, a totally reduced non-degenerate 0-sharbly $\mathbf{u}$ often satisfies $\mathrm{Norm}_{F/\mathbb{Q}}(\det(u_1|u_2)) = 1$), while ours extends readily to more general positivity domains.

Given a sharbly chain ξ which defines a cycle in the homology of $(\mathscr{S}_k)_{\Gamma_0(\mathfrak{n})}$, we would like to find a second sharbly chain, homologous to the first, whose support consists of totally reduced sharblies. In the remainder of this section, we shall define an algorithm which, given a 1-sharbly $\mathbf{u}$ in the support of such a cycle ξ, produces a 1-sharbly chain whose support comprises 1-sharblies that are "closer" to being totally reduced than $\mathbf{u}$ (in the sense that either the sizes of the resulting 1-sharblies are smaller than that of $\mathbf{u}$, or these 1-sharblies are totally reduced). Moreover, the resulting chains should satisfy the condition that, when we perform one iteration of the algorithm for each of the sharblies in the support of ξ, then the chain produced by summing over all the resulting 1-sharblies should in fact be a cycle homologous to ξ, thus enabling us to compute the Hecke action on the sharbly homoloy $H_1((\mathscr{S}_*)_{\Gamma_0(\mathfrak{n})}, \mathbb{C})$.

For illustrative purposes, we will first give an algorithm which works for 0-sharblies. Let $\mathbf{u} = [u_1, u_2]$ be an arbitrary 0-sharbly, which is not totally reduced, and let $\mathcal{B}(\mathbf{u})$, $\mathcal{F}_{\mathbf{u}}$ and $\Phi_{\mathbf{u}}$ be as above. Note that, for any $x \in \mathcal{O}_F^2$, we have

$$\partial[u_2, u_1, x] = [u_1, x] + [x, u_2] + [u_2, u_1],$$

so that

$$[u_1, x] + [x, u_2] = \mathbf{u} + \partial[u_2, u_1, x]$$

is homologous to $\mathbf{u}$. Our aim is to find a point $x \in \mathcal{O}_F^2$ such that the sharblies $[u_1, x]$ and $[x, u_2]$ are in a sense *more reduced* than $\mathbf{u}$, by which we mean that they either have smaller size than $\mathbf{u}$ (if $\mathbf{u}$ is not reduced) or are totally reduced (if $\mathbf{u}$ is reduced, but not totally reduced). We call such a point a *reducing point* for $\mathbf{u}$.

Note first that the points $q(u_1)$ and $q(u_2)$ need not be vertices of Π. While in practice this doesn't cause an issue, the following result shows that we can, without loss of generality, assume that both *are* vertices:

Lemma 5.2.2. *Let $\mathbf{u} = [u_1, u_2]$ be a 0-sharbly. Then we can find a chain*

$$\xi = \sum \lambda_{\mathbf{v}} \mathbf{v}$$

of 0-sharblies $\mathbf{v} = [v_1, v_2]$ such that each $q(v_i)$ is a vertex of Π, and ξ is homologous to $\mathbf{u}$.

Proof. For each i, let $u_i = \binom{x_i}{y_i}$, $z_i = \gcd(x_i, y_i)$, and $w_i = z_i^{-1} u_i \in \mathcal{O}_F^2$ (recall that we have restricted attention to fields with trivial class group, and so the notion of gcd makes sense). Then

$$\partial([u_2, u_1, w_1] + [u_2, w_1, w_2]) = [u_2, u_1] + [w_1, w_2],$$

(since the sharblies $[u_i, w_i]$ are degenerate) and the $q(w_i)$ are vertices of Π (by **Corollary 4.4.2**, since each w_i is primitive). Thus

$$\xi = \mathbf{u} + \partial([u_2, u_1, w_1] + [u_2, w_1, w_2])$$

is our desired chain. □

We shall henceforth suppose that both $q(u_1)$ and $q(u_2)$ are vertices of Π. Suppose first that $\mathbf{u}$ is also non-degenerate. There are three possibilities:

(i) $\mathbf{u}$ is reduced, but not totally reduced;

(ii) $\mathbf{u}$ is not reduced, but exactly one of the $q(u_i)$ is a vertex of $\mathcal{F}_{\mathbf{u}}$;

(iii) Neither $q(u_1)$ nor $q(u_2)$ is a vertex of $\mathcal{F}_{\mathbf{u}}$.

In the first case, we choose a reducing point $x \in \mathcal{O}_F^2$ with $q(x) \in M(\mathcal{F}_{\mathbf{u}})$ such that both $[u_1, x]$ and $[x, u_2]$ are totally reduced (or, if this is not possible, at least one of these sharblies is).

In the second case, suppose, without loss of generality, that $q(u_1)$ is a vertex of $\mathcal{F}_{\mathbf{u}}$. Since $q(u_2) \notin \mathcal{F}_{\mathbf{u}}$, there is some neighbouring facet $\mathcal{G}$ such that

$$\langle \Phi_{\mathcal{G}}, q(u_2) \rangle < \langle \Phi_{\mathbf{u}}, q(u_2) \rangle,$$

by **Corollary 4.3.13**. Then, if $q(x) \in M(\mathcal{F}_{\mathbf{u}}) \cap M(\mathcal{G})$, the 0-sharbly $[u_1, x]$ is reduced, and we have

$$N([x, u_2]) = \langle \Phi_{[x,u_2]}, q(x)+q(u_2) \rangle \leq \langle \Phi_{\mathcal{G}}, q(x)+q(u_2) \rangle < \langle \Phi_{\mathbf{u}}, q(x)+q(u_2) \rangle = N(\mathbf{u}),$$

as required, so we choose a reducing point from amongst all such points $x \in \mathcal{O}_F^2$.

In the third and final case, note that for $x \in \mathcal{O}_F^2$ with $q(x) \in M(\mathcal{F}_{\mathbf{u}})$,

$$\begin{aligned} N([u_1, x]) + N([x, u_2]) &\leq \langle \Phi_{\mathbf{u}}, q(u_1) + q(u_2) + 2q(x) \rangle \\ &= N(\mathbf{u}) + 2. \end{aligned}$$

Without loss of generality, suppose $N([u_1, x]) \leq N([u_2, x])$, so that (noting that, since $\mathbf{u}$ is not reduced, $N(\mathbf{u}) > 2$)

$$N([u_1, x]) \leq \tfrac{1}{2} N(\mathbf{u}) + 1 < N(\mathbf{u}).$$

Moreover, if $[u_1, x]$ is not reduced, then, since

$$N([u_1, x]) + N([u_2, x]) \leq N(\mathbf{u}) + 2,$$

we must have $N([u_2, x]) < N(\mathbf{u})$ as well. On the other hand, if $[u_1, x]$ *is* reduced, then the barycentre $\mathcal{B}([u_1, x])$ must lie above the facet of Π containing both $q(u_1)$ and $q(x)$. Since $q(u_1)$ is not a vertex of $\mathcal{F}_{\mathbf{u}}$, $\mathcal{B}([u_1, x])$ *cannot* lie above $\mathcal{F}_{\mathbf{u}}$, and so

$$N([u_1, x]) + N([u_2, x]) < N(\mathbf{u}) + 2,$$

and so once again $N([u_2, x]) < N(\mathbf{u})$. Thus we can choose as a reducing point for $\mathbf{u}$ *any* point $x \in \mathcal{O}_F^2$ with $q(x) \in M(\mathcal{F}_{\mathbf{u}})$.

Finally, suppose that $\mathbf{u}$ is degenerate (that is, $u_2 = \lambda u_1$ for some $\lambda \in F$). Without loss of generality, we may assume that $u_1 = \left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right)$. Since $\mathcal{B}(\mathbf{u})$ must be a *positive* linear combination of vertices of $\mathcal{F}_{\mathbf{u}}$, it is clear that each vertex appearing in this sum must be of the form $q(x)$, where x also lies in the same F-span as u_1. Thus we may choose for our reducing point any such point $x \in \mathcal{O}_F^2$.

The case of 1-sharblies is significantly more complicated. To begin with, let

$$\xi = \sum_{\mathbf{u}} \lambda_{\mathbf{u}} \mathbf{u}$$

be a cycle in $(\mathscr{S}_1)_{\Gamma_0(\mathfrak{n})}$. The cycle condition then implies that

$$\partial \xi = \sum_{\mathbf{u}} \sum_{\mathbf{v}} \lambda_{\mathbf{u}} \mathbf{v} = 0 \pmod{\Gamma_0(\mathfrak{n})},$$

where $\mathbf{v}$ is an edge of $\mathbf{u}$.

Fix a set $\{\mathbf{w}_1, \ldots, \mathbf{w}_n\}$ of $\Gamma_0(\mathfrak{n})$-representatives for the edges $\mathbf{v} \in \mathrm{Supp}(\partial\xi)$, up to sign. There are three possibilities for each $\mathbf{w}_i$ that we must consider:

- $\mathbf{w}_i$ is degenerate;
- $\mathbf{w}_i$ is non-degenerate, and there is no element of $\Gamma_0(\mathfrak{n})$ which reverses the orientation of $\mathbf{w}_i$ (we call such sharblies *non-trivial*);
- $\mathbf{w}_i$ is non-degenerate, but there is some element of $\Gamma_0(\mathfrak{n})$ which reverses the orientation of $\mathbf{w}_i$ (we call such sharblies *trivial*).

While trivial 0-sharblies vanish in $(\mathscr{S}_0)_{\Gamma_0(\mathfrak{n})}$ (as their name suggests), we shall still need to consider them. Suppose that to each 0-sharbly $\mathbf{v} \in \mathrm{Supp}(\partial\xi)$, where $\mathbf{v} \in \Gamma_0(\mathfrak{n})\mathbf{w}_i$, we assign a point $x(\mathbf{v}) \in \mathcal{O}_F^2$ as follows:

- If $\mathbf{w}_i$ is degenerate, then $x(\mathbf{v})$ lies in the same F-span as v_1 and v_2;
- If $\mathbf{w}_i$ is non-trivial, then we can write $\mathbf{v} = \epsilon_{\mathbf{v}}\gamma_{\mathbf{v}}\mathbf{w}_i$ where $\gamma_{\mathbf{v}} \in \Gamma_0(\mathfrak{n})$, and $\epsilon_{\mathbf{v}} = \pm 1$ is well-defined. After fixing an initial choice of point $x(\mathbf{w}_i)$, we set $x(\mathbf{v}) = \gamma_{\mathbf{v}} x(\mathbf{w}_i)$.
- If $\mathbf{w}_i$ is trivial, then we can find some $\gamma_{\mathbf{w}_i} \in \Gamma_0(\mathfrak{n})$ such that $\mathbf{w}_i = -\gamma_{\mathbf{w}_i}\mathbf{w}_i$. Choose an initial point $x(\mathbf{w}_i)$, and replace $\mathbf{w}_i$ with $\frac{1}{2}(\mathbf{w}_i^+ + \mathbf{w}_i^-)$, where $\mathbf{w}_i^{\pm} = \mathbf{w}_i$, but we set $x(\mathbf{w}_i^+) = x(\mathbf{w}_i)$ and $x(\mathbf{w}_i^-) = \gamma_{\mathbf{w}_i} x(\mathbf{w}_i)$. Since $\mathbf{w}_i$ is trivial, we can always find $\gamma_{\mathbf{v}} \in \Gamma_0(\mathfrak{n})$ such that $\mathbf{v} = \gamma_{\mathbf{v}}\mathbf{w}_i$. Then replace $\mathbf{v}$ with $\frac{1}{2}(\mathbf{v}^+ + \mathbf{v}^-)$, where $\mathbf{v}^{\pm} = \mathbf{v}$, and we set $x(\mathbf{v}^{\pm}) = \gamma_{\mathbf{v}} x(\mathbf{w}_i^{\pm})$.

We say such a set of points has been chosen $\Gamma_0(\mathfrak{n})$-*equivariantly*.

Suppose, then, that we have a cycle $\xi \in (\mathscr{S}_1)_{\Gamma_0(\mathfrak{n})}$ together with a set of $\Gamma_0(\mathfrak{n})$-equivariant points $x(\mathbf{v})$ for each $\mathbf{v} \in \mathrm{Supp}(\partial\xi)$. For each representative 0-sharbly $\mathbf{w}_i$, we obtain a chain

$$\eta_i = \sum_{\mathbf{v} \in \Gamma_0(\mathfrak{n})\mathbf{w}_i} \epsilon_{\mathbf{v}} \lambda_{\mathbf{u}} \gamma_{\mathbf{v}} \mathbf{w}_i,$$

where $\mathbf{v}$ is an edge of $\mathbf{u} \in \mathrm{Supp}(\xi)$. Since ξ is a cycle in $(\mathscr{S}_1)_{\Gamma_0(\mathfrak{n})}$, its boundary, which is the sum of the η_i, must vanish modulo $\Gamma_0(\mathfrak{n})$, and thus, since the edges in the support of distinct η_i are inequivalent, each η_i must vanish in $(\mathscr{S}_0)_{\Gamma_0(\mathfrak{n})}$.

In particular, if $\mathbf{w}_i$ is non-trivial, then, since each $\gamma_{\mathbf{v}}\mathbf{w}_i$ is equivalent to $\mathbf{w}_i$ under the action of $\Gamma_0(\mathfrak{n})$, we find that

$$\eta_i = \sum_{\mathbf{v} \in \Gamma_0(\mathfrak{n})\mathbf{w}_i} \epsilon_{\mathbf{v}} \lambda_{\mathbf{u}} \mathbf{w}_i \pmod{\Gamma_0(\mathfrak{n})},$$

and so

$$\sum_{\mathbf{v} \in \Gamma_0(\mathfrak{n})\mathbf{w}_i} \epsilon_{\mathbf{v}} \lambda_{\mathbf{u}} = 0.$$

The following result is key to the implementation of our algorithm:

Proposition 5.2.3. *Let*

$$\xi = \sum \lambda_{\mathbf{u}} \mathbf{u}$$

be a cycle in $(\mathscr{S}_1)_{\Gamma_0(\mathfrak{n})}$*, and choose a set of points* $x(\mathbf{v}) \in \mathcal{O}_F^2$ *for the edges* $\mathbf{v} \in \mathrm{Supp}(\partial\xi)$ $\Gamma_0(\mathfrak{n})$*-equivariantly. Then*

$$\sum_{\mathbf{v} \in \mathrm{Supp}(\partial\xi)} \lambda_{\mathbf{u}}[v_1, v_2, x(\mathbf{v})] = 0 \pmod{\Gamma_0(\mathfrak{n})},$$

where $\mathbf{v} = [v_1, v_2]$ *is an edge of* $\mathbf{u} \in \mathrm{Supp}(\xi)$*.*

Proof. We use the notation established above. It suffices to show that for each representative $\mathbf{w}_i$, the chain

$$\nu_i = \sum_{\mathbf{v} \in \Gamma_0(\mathfrak{n})\mathbf{w}_i} \lambda_{\mathbf{u}}[v_1, v_2, x(\mathbf{v})]$$

vanishes modulo $\Gamma_0(\mathfrak{n})$. We consider the three separate cases:

Firstly, if $\mathbf{w}_i$ is degenerate, then by definition the point $x(\mathbf{v})$ for each $\mathbf{v} = [v_1, v_2] \in \Gamma_0(\mathfrak{n})\mathbf{w}_i$ lies in the same F-span as v_1 and v_2, so $[v_1, v_2, x(\mathbf{v})]$ is also degenerate. Thus ν_i, being a chain of degenerate sharblies, must vanish.

Secondly, if $\mathbf{w}_i$ is non-trivial, then we have

$$\begin{aligned}
\nu_i &= \sum_{\mathbf{v} \in \Gamma_0(\mathfrak{n})\mathbf{w}_i} \lambda_{\mathbf{u}}[v_1, v_2, x(\mathbf{v})] \\
&= \sum_{\mathbf{v} \in \Gamma_0(\mathfrak{n})\mathbf{w}_i} \epsilon_{\mathbf{v}} \lambda_{\mathbf{u}} \gamma_{\mathbf{v}}[w_1, w_2, x(\mathbf{w})] \\
&= \sum_{\mathbf{v} \in \Gamma_0(\mathfrak{n})\mathbf{w}_i} \epsilon_{\mathbf{v}} \lambda_{\mathbf{u}}[w_1, w_2, x(\mathbf{w})] \pmod{\Gamma}.
\end{aligned}$$

Thus, since

$$\sum_{\mathbf{v} \in \Gamma_0(\mathfrak{n})\mathbf{w}_i} \epsilon_{\mathbf{v}} \lambda_{\mathbf{u}} = 0,$$

ν_i must vanish modulo $\Gamma_0(\mathfrak{n})$.

Finally, if $\mathbf{w}_i$ is trivial, then by our definition of $\Gamma_0(\mathfrak{n})$-equivariance we have

$$\begin{aligned}
\sum_{\mathbf{v} \in \Gamma_0(\mathfrak{n})\mathbf{w}_i} \lambda_{\mathbf{u}}[v_1, v_2, x(\mathbf{v})] &= \tfrac{1}{2} \sum_{\mathbf{v} \in \Gamma_0(\mathfrak{n})\mathbf{w}_i} (\lambda_{\mathbf{u}} \gamma_{\mathbf{v}}[w_1, w_2, x(\mathbf{w}_i^+)] + \lambda_{\mathbf{u}} \gamma_{\mathbf{v}}[w_1, w_2, x(\mathbf{w}_i^-)]) \\
&= \tfrac{1}{2} \sum_{\mathbf{v} \in \Gamma_0(\mathfrak{n})\mathbf{w}_i} (\lambda_{\mathbf{u}} \gamma_{\mathbf{v}}[w_1, w_2, x(\mathbf{w}_i^+)] + \lambda_{\mathbf{u}} \gamma_{\mathbf{v}} \gamma_{\mathbf{w}}[w_2, w_1, x(\mathbf{w}_i^+)]).
\end{aligned}$$

Each pair of terms cancels, and thus ν_i vanishes modulo $\Gamma_0(\mathfrak{n})$, as required. □

Note that, since the notions of totally reduced, reduced and non-reduced sharblies are preserved under the action of $\mathrm{GL}_2(\mathcal{O}_F)$, **Proposition 5.2.3** applies equally well if we restrict our attention to the subset of edges of ξ which are not totally reduced.

Throughout our algorithm, we will require the existence of a $\Gamma_0(\mathfrak{n})$-equivariant set of reducing points for the edges of ξ. Since, by the nature of our algorithm, we will often be replacing sharblies in $\mathrm{Supp}(\xi)$ with sharblies that are "closer" to being reduced, we also need to ensure that reducing points chosen for any new edges that occur are also selected $\Gamma_0(\mathfrak{n})$-equivariantly. We do this by assigning to each non-reduced sharbly $\mathbf{v}$ a matrix $M_{\mathbf{v}}$, known as a *lift* of $\mathbf{v}$ (see **[Gun99], Definition 5.3**).

Our choice of lifts reflects our definition of $\Gamma_0(\mathfrak{n})$-equivariance. To begin with, we assign to each degenerate or non-trivial representative $\mathbf{w}_i = [w_1, w_2]$ the lift $M_{\mathbf{w}_i} = (\mathbf{w}_1|\mathbf{w}_2)$ (that is, the matrix with columns w_1 and w_2). For all other $\mathbf{v} \in \Gamma_0(\mathfrak{n})\mathbf{w}_i$, we write $\mathbf{v} = \epsilon_{\mathbf{v}}\gamma_{\mathbf{v}}\mathbf{w}_i$ for some $\gamma_{\mathbf{v}} \in \Gamma_0(\mathfrak{n})$, and give $\mathbf{v}$ the lift $\gamma_{\mathbf{v}}M_{\mathbf{w}_i}$. Note that, if $M_{\mathbf{v}} = (m_1|m_2)$, then the sharblies $\mathbf{v}$ and $[m_1, m_2]$ must be equal.

If $\mathbf{w}_i$ is trivial then, as in our definition, we rewrite it as $\mathbf{w}_i = \frac{1}{2}(\mathbf{w}_i^+ + \mathbf{w}_i^-)$, and define $M_{\mathbf{w}_i^+} = (w_1|w_2)$ and $M_{\mathbf{w}_i^-} = (w_2|w_1)$. Given $\mathbf{v} \in \Gamma_0(\mathfrak{n})\mathbf{w}_i$, we can find $\gamma_{\mathbf{v}} \in \Gamma_0(\mathfrak{n})$ such that $\mathbf{v} = \gamma_{\mathbf{v}}\mathbf{w}_i$; we then rewrite $\mathbf{v}$ as $\frac{1}{2}(\mathbf{v}^+ + \mathbf{v}^-)$, and define $M_{\mathbf{v}^+} = \gamma_{\mathbf{v}}M_{\mathbf{w}_i^+}$ and $M_{\mathbf{v}^-} = \gamma_{\mathbf{v}}M_{\mathbf{w}_i^-}$.

To ensure that our reducing points are chosen $\Gamma_0(\mathfrak{n})$-equivariantly, we store the lifts $M_{\mathbf{w}_i}$ of our representatives $\mathbf{w}_i$, and assign to each such edge a reducing point $x(\mathbf{w}_i)$. Then, given an arbitrary 1-sharbly $\mathbf{v}$ for which we want to select a reducing point, we check whether its lift $M_{\mathbf{v}}$ is equivalent to one of our representative lifts under the left action of $\Gamma_0(\mathfrak{n})$. If so, say $M_{\mathbf{v}} = \gamma_{\mathbf{v}}M_{\mathbf{w}_i}$, then we assign to $\mathbf{v}$ the reducing point $\gamma_{\mathbf{v}}x(\mathbf{w}_i)$. If $M_{\mathbf{v}}$ is inequivalent to all our representatives, we choose an arbitrary reducing point, and add $M_{\mathbf{v}}$ to our list of representatives.

We need a final word on how to select lifts for the new edges which arise during the course of our algorithm. Given a representative edge $\mathbf{w}_i = [w_1, w_2]$ and a point $x(\mathbf{w}_i)$ chosen $\Gamma_0(\mathfrak{n})$-equivariantly, the edge $\mathbf{w}_i$ is replaced during our algorithm by the edges $[w_1, x(\mathbf{w}_i)]$ and $[x(\mathbf{w}_i), w_2]$. Assign to these edges the lifts $(w_1|x(\mathbf{w}_i))$ and $(x(\mathbf{w}_i)|w_2)$ respectively.

If $\mathbf{v}$ is an arbitrary edge, with $\mathbf{v} = \epsilon_{\mathbf{v}}\gamma_{\mathbf{v}}\mathbf{w}_i$ for some $\gamma_{\mathbf{v}} \in \Gamma_0(\mathfrak{n})$, and the point $x(\mathbf{v})$ is chosen $\Gamma_0(\mathfrak{n})$-equivariantly, then we have

$$[v_1, x(\mathbf{v})] = \begin{cases} \gamma_{\mathbf{v}}[w_1, x(\mathbf{w}_i)], & \text{if } \epsilon_{\mathbf{v}} = 1, \\ \gamma_{\mathbf{v}}[w_2, x(\mathbf{w}_i)], & \text{if } \epsilon_{\mathbf{v}} = -1, \end{cases}$$

and similarly

$$[x(\mathbf{v}), v_2] = \begin{cases} \gamma_{\mathbf{v}}[x(\mathbf{w}_i), w_2], & \text{if } \epsilon_{\mathbf{v}} = 1, \\ \gamma_{\mathbf{v}}[x(\mathbf{w}_i), w_1], & \text{if } \epsilon_{\mathbf{v}} = -1. \end{cases}$$

Note that, if $\mathbf{v}$ has lift $M_{\mathbf{v}} = (m_1|m_2)$, then

$$[m_1, m_2] = \begin{cases} [v_1, v_2], & \text{if } \epsilon_{\mathbf{v}} = 1, \\ [v_2, v_1], & \text{if } \epsilon_{\mathbf{v}} = -1. \end{cases}$$

Thus, if the edge $\mathbf{v}$ has lift $M_{\mathbf{v}} = (m_1|m_2)$, the choice of lifts

$$M_{[v_1, x(\mathbf{v})]} = \begin{cases} (m_1|x(\mathbf{v})), & \text{if } [m_1, m_2] = [v_1, v_2], \\ (x(\mathbf{v})|m_2), & \text{if } [m_1, m_2] = [v_2, v_1], \end{cases}$$

and

$$M_{[x(\mathbf{v}), v_2]} = \begin{cases} (x(\mathbf{v})|m_2), & \text{if } [m_1, m_2] = [v_1, v_2], \\ (m_1|x(\mathbf{v})), & \text{if } [m_1, m_2] = [v_2, v_1], \end{cases}$$

ensure that any future points will also be selected $\Gamma_0(\mathfrak{n})$-equivariantly.

Finally, it is not hard to see that if $\{M_{\mathbf{v}}\}_{\mathbf{v} \in \mathrm{Supp}(\xi)}$ is a set of lifts of the edges $\mathbf{v}$ of ξ, and $\{\gamma_1, \ldots, \gamma_n\}$ denotes a set of representatives as in **Proposition 5.2.1**, then $\{\gamma_1 M_{\mathbf{v}}, \ldots, \gamma_n M_{\mathbf{v}}\}_{\mathbf{v} \in \mathrm{Supp}(\xi)}$ is a set of lifts of the edges of the chain $T_{\mathfrak{p}}(\xi)$, which are still $\Gamma_0(\mathfrak{n})$-equivariant.

Thus, in practice, we will choose a set of lifts for our chain ξ, apply the Hecke operator $T_{\mathfrak{p}}$, and give the cycle $T_{\mathfrak{p}}(\xi)$ the corresponding lifts. This cycle, together with the set of lifts, forms the input for our algorithm.

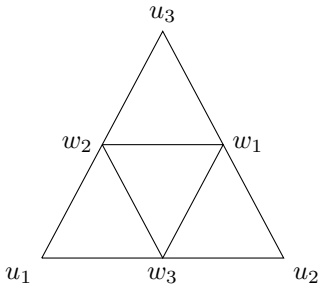
Before proceeding to discuss the algorithm in full, we establish an analogue of **Lemma 5.2.2**:

Lemma 5.2.4. *Let $\xi \in (\mathscr{S}_1)_{\Gamma_0(\mathfrak{n})}$ be a 1-sharbly cycle. Then we can find a chain*

$$\xi' = \sum \lambda_{\mathbf{v}} \mathbf{v}$$

of 1-sharblies $\mathbf{v} = [v_1, v_2, v_3]$ such that each $q(v_i)$ is a vertex of Π and ξ' is homologous to ξ.

Proof. For each edge $[u_1, u_2]$ of ξ, let $u_i = \binom{x_i}{y_i}$, $z_i = \gcd(x_i, y_i)$ and $w_i = z_i^{-1} u_i$, so that in particular $q(w_i)$ is a vertex of Π, and w_i lies in the same F-span as u_i. To each such edge, assign one of the w_i for which $q(u_i)$ is not a vertex of Π, and assign these points $\Gamma_0(\mathfrak{n})$-equivariantly (which is possible, since ξ is a cycle).



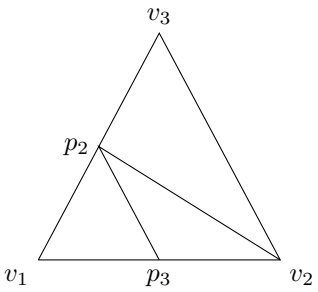
Now, given $\mathbf{u} = [u_1, u_2, u_3] \in \mathrm{Supp}(\xi)$, let w_1, w_2, w_3 be the points chosen for the edges $[u_2, u_3]$, $[u_3, u_1]$ and $[u_1, u_2]$ respectively. Define four tetrahedra $T_1 = [u_1, u_2, u_3, w_1]$, $T_2 = [u_3, u_1, w_1, w_2]$, $T_3 = [u_1, u_2, w_1, w_3]$ and $T_4 = [u_1, w_1, w_2, w_3]$. Then

$$\begin{aligned}
\partial T_1 &= [u_2, u_3, w_1]^* + [u_3, u_1, w_1] + [u_1, u_2, w_1] + [u_2, u_1, u_3], \\
\partial T_2 &= [u_1, w_1, w_2] + [w_1, u_3, w_2] + [u_3, u_1, w_2]^* + [u_1, u_3, w_1], \\
\partial T_3 &= [u_2, w_1, w_3] + [w_1, u_1, w_3] + [u_1, u_2, w_3]^* + [u_2, u_1, w_1], \\
\partial T_4 &= [w_1, w_2, w_3] + [w_2, u_1, w_3] + [u_1, w_1, w_3] + [w_1, u_1, w_2],
\end{aligned}$$

and $\mathbf{u} + \partial T_1 + \partial T_2 + \partial T_3 + \partial T_4$ is homologous to $\mathbf{u}$. By **Proposition 5.2.3**, the starred terms cancel when we consider the whole cycle ξ, so we replace $\mathbf{u}$ with

$$\mathbf{u} + \partial T_1 + \partial T_2 + \partial T_3 + \partial T_4 = [w_1, u_3, w_2] + [u_2, w_1, w_3] + [w_1, w_2, w_3] + [w_2, u_1, w_3].$$

Note in particular that each of the resulting sharblies contains at most one point which does not correspond to a vertex of Π. Let $\mathbf{v} = [v_1, v_2, v_3]$ be such a sharbly, and, after permuting if necessary, assume that $q(v_1)$ is not a vertex of Π. Let p_2 and p_3 be the points chosen for the edges $[v_3, v_1]$ and $[v_1, v_2]$ respectively, and note that p_2 and p_3 both lie in the same F-span as v_1.



Define two tetrahedra $T_1 = [v_1, v_2, v_3, p_3]$ and $T_2 = [v_3, v_1, p_3, p_2]$. Then

$$\partial T_1 = [v_2, v_3, p_3] + [v_3, v_1, p_3] + [v_1, v_2, p_3]^* + [v_2, v_1, v_3],$$
$$\partial T_2 = [v_1, p_3, p_2] + [p_3, v_3, p_2] + [v_3, v_1, p_2]^* + [v_1, v_3, p_3],$$

and $\mathbf{u} + \partial T_1 + \partial T_2$ is homologous to $\mathbf{u}$. As before, the starred terms cancel, so we replace $\mathbf{u}$ with

$$\mathbf{u} + \partial T_1 + \partial T_2 = [v_2, v_3, p_3] + [v_1, p_3, p_2] + [p_3, v_3, p_2].$$

Now, since p_2 and p_3 have been chosen to lie in the same F-span as v_1, the sharbly $[v_1, p_3, p_2]$ is degenerate, and the result follows. □

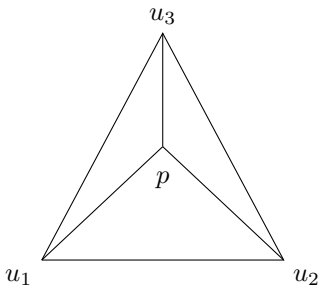
Thus we may, if we so choose, assume that all the sharblies in the support of our cycle ξ define a set of vertices of Π.

We now proceed to discuss the algorithm with which we reduce an arbitrary 1-sharbly cycle ξ. Given a 1-sharbly $\mathbf{u} = [u_1, u_2, u_3] \in \mathrm{Supp}(\xi)$, we perform one of the following steps, based on the *reduction type* of $\mathbf{u}$ (that is, based on the configuration of reduced and non-reduced edges of $\mathbf{u}$). Note that this algorithm is essentially the same as that found in, for example, **[GHY13]**, but we treat reduction types **III.i** and **V.ii** differently. As is the case in **[GHY13]**, we have no proof that the algorithm will terminate, but in practice it always does so.

Reduction Type I

If $\mathbf{u}$ is already totally reduced, we leave it untouched.

Reduction Type II



If all three edges of $\mathbf{u}$ are totally reduced, but $\mathbf{u}$ itself is *not* totally reduced, we begin by selecting a central point $p \in \mathcal{O}_F^2$ from among the vectors mapping to the vertices of $\mathcal{F}_{\mathbf{u}}$. We choose p such that the number of totally reduced sharblies in the set

$$\{[u_1, u_2, p_i],\ [u_2, u_3, p_i],\ [u_3, u_1, p_i]\}$$

is maximal among all such vectors.

Define a tetrahedron $T = [u_1, u_2, u_3, p]$. Then

$$\partial T = [u_2, u_3, p] + [u_3, u_1, p] + [u_1, u_2, p] + [u_2, u_1, u_3],$$

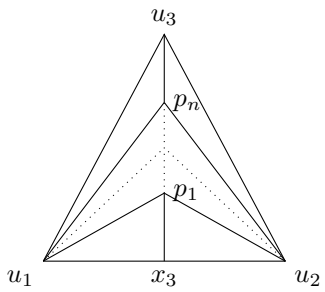
and $\mathbf{u} + \partial T$ is homologous to $\mathbf{u}$. We therefore replace $\mathbf{u}$ with

$$\mathbf{u} + \partial T = [u_2, u_3, p] + [u_3, u_1, p] + [u_1, u_2, p].$$

Reduction Type III

If **u** has one edge which is not totally reduced, then after cyclic permutation of the vectors u_i we may assume, without loss of generality, that the edge $[u_1, u_2]$ is not totally reduced. We select a reducing point x_3 for this edge, and consider the new edges $[u_1, x_3]$, $[u_2, x_3]$ and $[u_3, x_3]$. We have two separate cases:

Reduction Type III.i



If $[u_1, x_3]$ and $[u_2, x_3]$ are both totally reduced, but $[u_3, x_3]$ is *not* totally reduced, then we attempt to construct a chain of points $p_1, \ldots, p_n$ such that

- The 0-sharblies $[u_1, p_i]$ and $[u_2, p_i]$ are totally reduced for $i = 1, \ldots, n$;
- The 0-sharblies $[p_i, p_{i+1}]$ are totally reduced for $i = 1, \ldots, n-1$; and
- The 0-sharblies $[x_3, p_1]$ and $[u_3, p_n]$ are totally reduced.

Suppose we can find such a chain. Then, setting $p_0 = x_3$, and $p_{n+1} = u_3$, we define tetrahedra $T_0, \ldots, T_n$ by $T_i = [u_1, u_2, p_{i+1}, p_i]$. Then

$$\partial T_i = [u_2, p_{i+1}, p_i] + [p_{i+1}, u_1, p_i] + [u_1, u_2, p_i] + [u_2, u_1, p_{i+1}],$$

and so

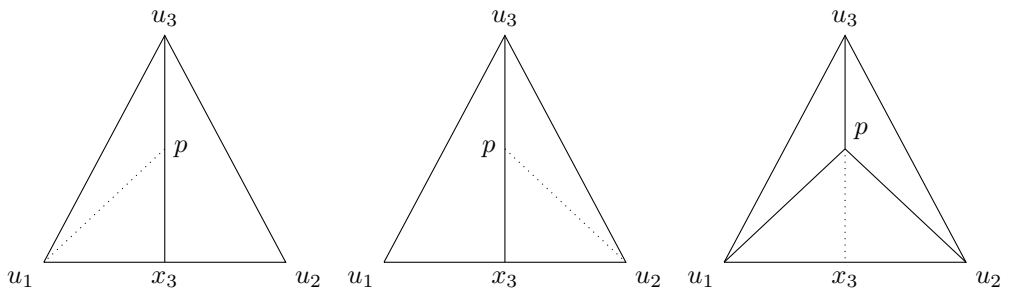
$$\sum_{i=0}^{n} \partial T_i = \sum_{i=0}^{n} ([u_2, p_{i+1}, p_i] + [p_{i+1}, u_1, p_i]) + [u_1, u_2, x_3]^* + [u_2, u_1, u_3].$$

By **Proposition 5.2.3** the starred term cancels when this reduction is performed across the whole chain ξ, so we replace **u** with

$$\mathbf{u} + \sum_{i=0}^{n} \partial T_i = \sum_{i=0}^{n} ([u_2, p_{i+1}, p_i] + [p_{i+1}, u_1, p_i]).$$

In practice, we were either able to find such a chain *or* find a vector $p \in \mathcal{O}_F^2$ mapping to a vertex of $\mathcal{F}_\Phi$ such that:

- Three of the 0-sharblies in
$$\{[u_1, p],\ [u_2, p],\ [u_3, p],\ [x_3, p]\}$$
were totally reduced;
- The single non-reduced sharbly in the above set was either $[u_1, p]$, $[u_2, p]$ or $[x_3, p]$; and
- We *were* able to find such a chain for the 1-sharbly $[u_3, u_1, x_3]$, $[u_2, u_3, x_3]$ or $[u_1, u_2, p]$ in each respective case.



If either $[u_1, p]$ or $[u_2, p]$ is non-reduced, define a tetrahedron $T = [u_1, u_2, u_3, x_3]$, so that

$$\partial T = [u_2, u_3, x_3] + [u_3, u_1, x_3] + [u_1, u_2, x_3]^* + [u_2, u_1, u_3].$$

As before, the starred term cancels, so we replace $\mathbf{u}$ with

$$\mathbf{u} + \partial T = [u_2, u_3, x_3] + [u_3, u_1, x_3].$$

Since each resulting 1-sharbly contains the edge $[u_3, x_3]$ with opposite orientations, it cancels upon applying the boundary map. Thus, assigning the point p as a reducing point for this edge in both 1-sharblies, we ensure that the terms $[u_3, x_3, p]$ still cancel, as per **Proposition 5.2.3**.

If $[x_3, p]$ is non-reduced, define a tetrahedron $T = [u_1, u_2, u_3, p]$, so that

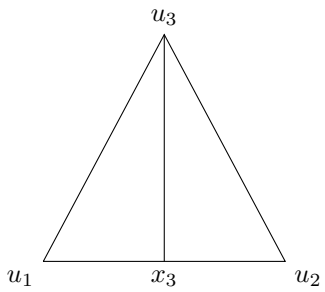
$$\partial T = [u_2, u_3, p] + [u_3, u_1, p] + [u_1, u_2, p] + [u_2, u_1, u_3].$$

We then replace $\mathbf{u}$ with

$$\mathbf{u} + \partial T = [u_2, u_3, p] + [u_3, u_1, p] + [u_1, u_2, p],$$

retaining the point x_3 as a reducing point for the edge $[u_1, u_2]$.

Reduction Type III.ii



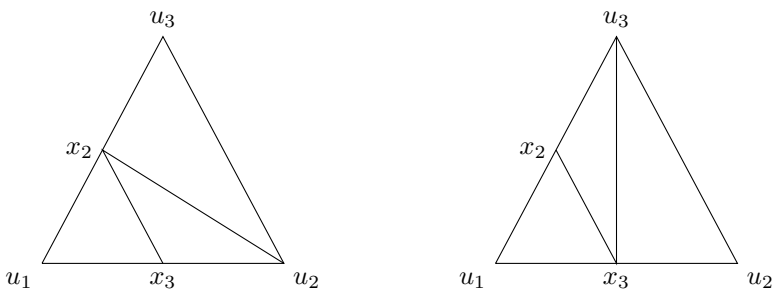
If $[u_3, x_3]$ is totally reduced, or at least one of $[u_1, x_3]$ and $[u_2, x_3]$ is not totally reduced, we define a single tetrahedron
$T = [u_1, u_2, u_3, x_3]$. Then

$$\partial T = [u_2, u_3, x_3] + [u_3, u_1, x_3] + [u_1, u_2, x_3]^* + [u_2, u_1, u_3],$$

and $\mathbf{u} + \partial T$ is homologous to $\mathbf{u}$. As before, the starred term cancels, so we replace $\mathbf{u}$ with

$$\mathbf{u} + \partial T = [u_2, u_3, x_3] + [u_3, u_1, x_3].$$

Reduction Type IV



If $\mathbf{u}$ has two edges which are not totally reduced then, after cyclic permutation of the vectors x_i, we may assume, without loss of generality, that the edges $[u_3, u_1]$ and $[u_1, u_2]$ are not totally reduced. We select reducing points x_2 and x_3 respectively for these edges.

We have a choice of decomposition. To decide which one to use, define new sharblies

$$\mathbf{w}_{11} = [x_2, x_3, u_3],\ \mathbf{w}_{12} = [x_3, u_2, u_3] \text{ and } \mathbf{w}_{21} = [x_3, u_2, x_2],\ \mathbf{w}_{22} = [u_2, u_3, x_2].$$

If $N(\mathbf{w}_{11}) + N(\mathbf{w}_{12}) \leq N(\mathbf{w}_{21}) + N(\mathbf{w}_{22})$, we define two tetrahedra $T_1 = [u_1, u_2, u_3, x_3]$ and $T_2 = [u_3, u_1, x_3, x_2]$. Then

$$\begin{aligned}\partial T_1 &= [u_2, u_3, x_3] + [u_3, u_1, x_3] + [u_1, u_2, x_3]^* + [u_2, u_1, u_3],\\ \partial T_2 &= [u_1, x_3, x_2] + [x_3, u_3, x_2] + [u_3, u_1, x_2]^* + [u_1, u_3, x_3],\end{aligned}$$

and $\mathbf{u} + \partial T_1 + \partial T_2$ is homologous to $\mathbf{u}$. As before, the starred terms cancel, so we replace $\mathbf{u}$ with

$$\mathbf{u} + \partial T_1 + \partial T_2 = [u_2, u_3, x_3] + [u_1, x_3, x_2] + [x_3, u_3, x_2].$$

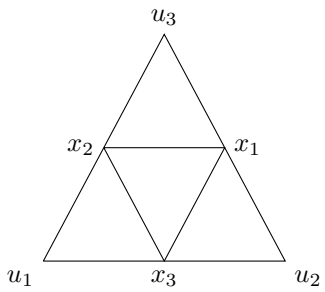
If $N(\mathbf{w}_{11}) + N(\mathbf{w}_{12}) > N(\mathbf{w}_{21}) + N(\mathbf{w}_{22})$, define two tetrahedra $T_1 = [u_1, u_2, u_3, x_2]$ and $T_2 = [u_1, u_2, x_2, x_3]$. Then

$$\begin{aligned}\partial T_1 &= [u_2, u_3, x_2] + [u_3, u_1, x_2]^* + [u_1, u_2, x_2] + [u_2, u_1, u_3],\\ \partial T_2 &= [u_2, x_2, x_3] + [x_2, u_1, x_3] + [u_1, u_2, x_3]^* + [u_2, u_1, x_2],\end{aligned}$$

and $\mathbf{u} + \partial T_1 + \partial T_2$ is homologous to $\mathbf{u}$. Once again, the starred terms cancel, so we replace $\mathbf{u}$ with

$$\mathbf{u} + \partial T_1 + \partial T_2 = [u_2, u_3, x_2] + [u_2, x_2, x_3] + [x_2, u_1, x_3].$$

Reduction Type V.i



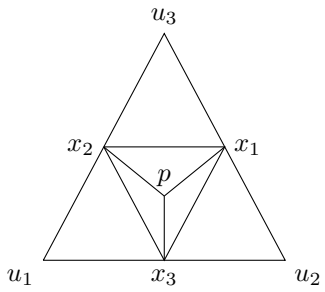
If all three edges $[u_2, u_3]$, $[u_3, u_1]$ and $[u_1, u_2]$ are not reduced, we choose reducing points x_1, x_2 and x_3 for these edges respectively. Define four tetrahedra $T_1 = [u_1, u_2, u_3, x_1]$, $T_2 = [u_3, u_1, x_1, x_2]$, $T_3 = [u_1, u_2, x_1, x_3]$ and $T_4 = [u_1, x_1, x_2, x_3]$. Then

$$\begin{aligned}
\partial T_1 &= [u_2, u_3, x_1]^* + [u_3, u_1, x_1] + [u_1, u_2, x_1] + [u_2, u_1, u_3], \\
\partial T_2 &= [u_1, x_1, x_2] + [x_1, u_3, x_2] + [u_3, u_1, x_2]^* + [u_1, u_3, x_1], \\
\partial T_3 &= [u_2, x_1, x_3] + [x_1, u_1, x_3] + [u_1, u_2, x_3]^* + [u_2, u_1, x_1], \\
\partial T_4 &= [x_1, x_2, x_3] + [x_2, u_1, x_3] + [u_1, x_1, x_3] + [x_1, u_1, x_2],
\end{aligned}$$

and $\mathbf{u} + \partial T_1 + \partial T_2 + \partial T_3 + \partial T_4$ is homologous to $\mathbf{u}$. As usual, the starred terms cancel, so we replace $\mathbf{u}$ with

$$\mathbf{u} + \partial T_1 + \partial T_2 + \partial T_3 + \partial T_4 = [x_1, u_3, x_2] + [u_2, x_1, x_3] + [x_1, x_2, x_3] + [x_2, u_1, x_3].$$

Reduction Type V.ii



If all three edges $[u_2, u_3]$, $[u_3, u_1]$ and $[u_1, u_2]$ are reduced, but not totally reduced, we proceed as above. However, if the resulting 1-sharbly $[x_1, x_2, x_3]$ has the properties that:

- The edges $[x_1, x_2]$, $[x_2, x_3]$ and $[x_3, x_1]$ are all reduced, but not totally reduced; and
- $\{\mathrm{Norm}_{F/\mathbb{Q}}(x_i|x_j);\ i < j\} = \{\mathrm{Norm}_{F/\mathbb{Q}}(u_i|u_j);\ i < j\}$,

then we perform an additional step. In this case, we choose a central point p for the 1-sharbly $[x_1, x_2, x_3]$ as for **Reduction Type II**, and define an additional tetrahedron $T_5 = [x_1, x_2, x_3, p]$, so that

$$\partial T_5 = [x_2, x_3, p] + [x_3, x_1, p] + [x_1, x_2, p] + [x_2, x_1, x_3].$$

We then proceed as in the previous case, except we replace the 1-sharbly $[x_1, x_2, x_3]$ with

$$[x_1, x_2, x_3] + \partial T_5 = [x_2, x_3, p] + [x_3, x_1, p] + [x_1, x_2, p].$$

5.3 Examples

The following pages give details of cuspidal Hecke eigenclasses defined over the fields F_1, F_2 and F_3. For the field F_1, we were able to provide an in-depth analysis, by investigating the cohomology $H^5(X_0(\mathfrak{n}), \mathbb{C})$ for all levels $\mathfrak{n}$ with norm at most 5500. Due to time constraints, however, we were unable to repeat this process for the fields F_2 and F_3, and instead focused on a restricted set of levels $\mathfrak{n}$.

In order to detect non-trivial cuspidal cohomology, we required data regarding the rank of the corresponding Eisenstein cohomology. This is provided in the following table, which collates heuristic data from **[GHY13]** (to determine these ranks, one observes that the Hecke operator T_v, where v does not divide the level $\mathfrak{n}$, acts on the Eisenstein subspace via multiplication by $\mathrm{Norm}_{F/\mathbb{Q}}(v)+1$):

Factorisation Type	$\mathfrak{p}$	$\mathfrak{p}^2$	$\mathfrak{p}^3$	$\mathfrak{p}^4$	$\mathfrak{p}^5$	$\mathfrak{p}^6$	$\mathfrak{pq}$
dim $H^5_{\mathrm{Eis}}(X_0(\mathfrak{n}), \mathbb{C})$	3	5	7	9	11	13	7
Factorisation Type	$\mathfrak{p}^2\mathfrak{q}$	$\mathfrak{p}^3\mathfrak{q}$	$\mathfrak{p}^4\mathfrak{q}$	$\mathfrak{p}^2\mathfrak{q}^2$	$\mathfrak{p}^3\mathfrak{q}^2$	$\mathfrak{pqr}$	$\mathfrak{p}^2\mathfrak{qr}$
dim $H^5_{\mathrm{Eis}}(X_0(\mathfrak{n}), \mathbb{C})$	11	15	19	17	23	15	23

Before proceeding to discuss each individual case, we make a mention of two ways in which cuspidal eigenclasses in $H^*(X_0(\mathfrak{n}), \mathbb{C})$ can arise from other cohomology groups, namely *level lifting* and *cyclic base change*, examples of which were observed for the field F_1.

Firstly, suppose that the level $\mathfrak{n} = \mathfrak{d}\mathfrak{m}$, for ideals $\mathfrak{d}$ and $\mathfrak{m}$ of F. The inclusion $K_0(\mathfrak{n}) \hookrightarrow K_0(\mathfrak{m})$ induces a map $H^*(X_0(\mathfrak{m}), \mathbb{C}) \to H^*(X_0(\mathfrak{n}), \mathbb{C})$ of cohomology groups. Consequently, one expects cuspidal eigenclasses at level $\mathfrak{m}$ to contribute to the cohomology at level $\mathfrak{n}$ (one draws an obvious analogy to classical modular forms, in which *oldforms* at level $n = dm$ are cuspidal eigenforms arising from the smaller level n).

Just as eigenclasses can arise from lower levels, so too can they arise from subfields of F. Let F/K be a *cyclic* extension of number fields of degree n, and let ω be a non-trivial character of $\mathrm{Gal}(F/K)$, which we can regard as a character of $\mathbb{A}_F^\times / F^\times$. Given an automorphic representation π of $\mathrm{Res}_{K/\mathbb{Q}}(\mathrm{GL}_2)$, the *base change* of π to F is an automorphic representation $\tilde{\pi}$ of $\mathrm{Res}_{F/\mathbb{Q}}(\mathrm{GL}_2)$, which satisfies the property

$$L(s, \tilde{\pi}) = \prod_{i=1} L(s, \omega^i \otimes \pi).$$

In particular, suppose that F/K is a quadratic extension, and observe that the non-trivial character $\omega \in \mathrm{Gal}(F/K)$ (viewed as a Hecke character) is defined locally at unramified non-archimedean places v by

$$\omega_v(\varpi) = \begin{cases} 1; & \text{if } v \text{ splits in } F, \\ -1; & \text{if } v \text{ is inert in } F, \end{cases}$$

where ϖ is a uniformiser of K_v.

If π is the automorphic representation associated to some automorphic form over K, then we have

$$L(s, \pi_v) = (1 - a_v(\pi)q^{-s} + q^{1-2s})^{-1},$$

where q denotes the size of the residue field of $\mathcal{O}_{K_v}$, and $a_v(\pi)$ denotes the eigenvalue of the Hecke operator T_v on the corresponding automorphic form. Then:

- If v splits in F, with corresponding places w_1, w_2, then

$$L(s, \tilde{\pi}_{w_1})L(s, \tilde{\pi}_{w_2}) = L(s, \pi_v)^2,$$

- If v is inert in F, with corresponding place w, then

$$L(s, \tilde{\pi}_w) = (1 - (a_v(\pi)^2 - 2q)q^{-2s} + q^{2-2s})^{-1}.$$

We therefore deduce that the Hecke eigenvalues on the corresponding eigenclass should be given by

$$a_w(\tilde{\pi}) = \begin{cases} a_v(\pi); & \text{if } v \text{ splits}, \\ a_v(\pi)^2 - 2q; & \text{if } v \text{ is inert}. \end{cases}$$

5.3.1 The Field F_1

Let $F = F_1 = \mathbb{Q}(t)$, where t denotes a primitive twelfth root of unity. We searched over a range of levels $\mathfrak{n}$ to detect those for which the cuspidal cohomology $H^5_{\mathrm{cusp}}(X_0(\mathfrak{n}), \mathbb{C})$ was non-trivial. As mentioned previously, we investigated all levels of norm at most 5500, of which there are 544, up to Galois conjugation. We discovered non-Eisenstein cohomology at 55 of these levels, with a total of 99 non-Eisenstein Hecke eigenclasses spread across these levels. Table 5.3.1.1 below lists a set of generators for the levels studied, together with their factorization type and the discrepancy d between the rank of $H_1((\mathscr{S}_*)_{\Gamma_0(\mathfrak{n})}, \mathbb{C})$ and the expected rank of the Eisenstein cohomology:

Level	Generator	Type	d	Level	Generator	Type	d
169	$2t^3 - 3t^2 - 3t + 2$	$\mathfrak{pq}$	1	3721a	$7t^3 - 6t^2 - t - 1$	$\mathfrak{pq}$	3
441	$5t^2 - 1$	$\mathfrak{pq}$	1	3721b	$6t^2 - 5t - 6$	$\mathfrak{pq}$	1
484	$t^3 + 4t^2 - 4t - 1$	$\mathfrak{pq}$	1	3844	$5t^3 - t^2 + t + 6$	$\mathfrak{pq}$	1
576	$2t^3 + 2t^2 + 2t - 4$	$\mathfrak{p}^3\mathfrak{q}$	1	3969	$9t^2 - 6$	$\mathfrak{p}^2\mathfrak{q}$	2
625	5	$\mathfrak{pq}$	2	4033a	$-8t^3 + 9t - 9$	$\mathfrak{pq}$	1
676	$3t^3 - t^2 + 3t$	$\mathfrak{pqr}$	2	4033b	$-11t^3 + 6t^2 + 5t - 9$	$\mathfrak{pq}$	1
1089	$-t^3 + 2t - 6$	$\mathfrak{pq}$	2	4057	$6t^3 + 2t^2 - 9t - 2$	$\mathfrak{p}$	1
1156	$3t^2 + 5t - 3$	$\mathfrak{pq}$	1	4069	$-7t^3 - 6t^2 + 6t + 2$	$\mathfrak{pq}$	1
1369	$2t^3 + 2t^2 + 3t - 5$	$\mathfrak{pq}$	2	4096	8	$\mathfrak{p}^6$	1
1521	$4t^3 + 4t^2 - 5t + 1$	$\mathfrak{pqr}$	2	4225a	$-5t^3 + 3t^2 + 9t - 3$	$\mathfrak{pqr}$	2
1764	$t^3 + 4t^2 + 4t - 5$	$\mathfrak{pqr}$	2	4225b	$-9t^3 + 3t^2 + 6t - 1$	$\mathfrak{p}^2\mathfrak{q}$	1
1936	$4t^3 - 4t^2 - 6t - 2$	$\mathfrak{p}^2\mathfrak{q}$	2	4225c	$-4t^3 + 7$	$\mathfrak{pqr}$	1
2041	$-t^3 + 6t^2 - t - 7$	$\mathfrak{pq}$	1	4356	$5t^3 + 3t^2 + 5t$	$\mathfrak{pqr}$	6
2116	$5t^3 - 5t^2 + t + 6$	$\mathfrak{pq}$	2	4516	$-4t^3 - 3t^2 + 9t + 1$	$\mathfrak{pq}$	1
2197a	$t^3 - 2t^2 + 3t + 7$	$\mathfrak{pqr}$	2	4624	$-8t^3 - 2$	$\mathfrak{p}^2\mathfrak{q}$	2
2197b	$t^3 + 2t^2 - 7t - 2$	$\mathfrak{p}^2\mathfrak{q}$	2	4672	$8t^3 + 6t^2 - 6t - 2$	$\mathfrak{p}^3\mathfrak{q}$	1
2209	$4t^3 - 8t - 1$	$\mathfrak{p}$	1	4761	$-7t^3 + 5t^2 + 2t + 2$	$\mathfrak{pq}$	3
2257	$-2t^3 + 6t^2 + 5t + 1$	$\mathfrak{pq}$	1	4852	$-4t^3 + 7t^2 + 3t + 1$	$\mathfrak{pq}$	1
2304	$8t^3 - 4t$	$\mathfrak{p}^4\mathfrak{q}$	2	5041	$-8t^3 + 3t^2 + 3t - 8$	$\mathfrak{p}$	2
2401	7	$\mathfrak{pq}$	3	5184	$-6t^2 + 6t + 6$	$\mathfrak{p}^3\mathfrak{q}^2$	2
2452	$-7t^3 + t^2 + t + 2$	$\mathfrak{pq}$	1	5317	$-7t^3 + 3t^2 - 2t - 4$	$\mathfrak{pq}$	1
2500a	$-t^3 - 7t^2 + t$	$\mathfrak{p}^2\mathfrak{q}$	1	5329a	$t^3 + 5t^2 + 3t - 9$	$\mathfrak{p}^2$	2
2500b	$5t^2 + 5t - 5$	$\mathfrak{pqr}$	4	5329b	$3t^3 - 8t^2 - 3t$	$\mathfrak{pq}$	2
2704	$-2t^3 - 6t^2 + 6t + 2$	$\mathfrak{p}^2\mathfrak{qr}$	4	5329c	$3t^3 - 6t - 10$	$\mathfrak{pq}$	4
2916	$3t^3 - 3t^2 + 3t + 6$	$\mathfrak{p}^3\mathfrak{q}$	2	5329d	$8t^3 - 9t$	$\mathfrak{pq}$	1
2977	$4t^3 + 2t^2 - 9t + 2$	$\mathfrak{pq}$	1	5473	$-9t - 8$	$\mathfrak{pq}$	1
3328	$4t^3 + 8t^2 - 4t - 4$	$\mathfrak{p}^4\mathfrak{q}$	1	5476	$-5t^2 - t - 5$	$\mathfrak{pqr}$	5
3481	$5t^3 - 5t^2 - 6t - 1$	$\mathfrak{p}$	2				

Table 5.3.1.1: Levels with non-Eisenstein cohomology classes

Of the 99 non-Eisenstein Hecke eigenclasses we detected:

- 68 admitted rational eigenvalues;
- 18 admitted eigenvalues lying in a quadratic extension of $\mathbb{Q}$;
- 9 admitted eigenvalues lying in a cubic extension of $\mathbb{Q}$; and
- 4 admitted eigenvalues lying in a quartic extension of $\mathbb{Q}$.

Of the 68 eigenclasses which admitted rational Hecke eigenvalues:

- 31 had eigenvalues matching an eigenclass appearing at a lower level;
- 15 had eigenvalues matching those expected from the base change of an automorphic form defined over a quadratic subfield of F;
- 2 had eigenvalues matching those from the Eisenstein cohomology, up to sign; and
- 20 classes could not be attributed to any of these phenomena, and we were able to find elliptic curves defined over F whose local data matched the eigenvalue data for each of these classes. We list these classes in Table 5.3.1.2 below, together with their Hecke eigenvalues for a number of primes of small norm, while the corresponding elliptic curves are listed in Table 5.3.1.10 (a discussion of how these curves were discovered can be found in **Section 6.6**).

Class	$\mathfrak{p}_2$	$\mathfrak{p}_3$	$\mathfrak{p}_{13,1}$	$\mathfrak{p}_{13,2}$	$\mathfrak{p}_{13,3}$	$\mathfrak{p}_{13,4}$	$\mathfrak{p}_{5,1}$	$\mathfrak{p}_{5,2}$
441	0	$*$	-6	4	4	-6	-4	-4
1156	$*$	0	4	4	-6	-6	6	6
2041	2	-2	2	2	$*$	-4	-4	-10
2257	-3	-4	-1	1	-6	-3	1	-8
2452	$*$	1	-4	-4	-4	5	-1	8
2500a	$*$	0	4	4	-1	-1	1	$*$
2977	2	4	2	-4	$*$	-4	2	-10
3328	$*$	2	-2	-2	6	$*$	2	-6
3721b	2	-2	-4	-4	2	2	8	8
3844	$*$	-5	-1	-6	-6	-1	1	1
4033a	-1	4	2	-4	2	2	2	-4
4033b	2	-2	-4	2	2	2	-4	2
4057	-3	-2	-4	-1	-4	1	-5	-2
4069	-3	-4	-3	1	$*$	-5	7	1
4225b	-2	-2	-4	$*$	-2	-6	$*$	4
4516	$*$	5	4	-1	-6	4	-4	6
4672	$*$	2	-2	-2	-2	6	-6	2
4852	$*$	-3	-1	-7	-2	-4	3	-8
5317	-3	2	-2	6	-2	$*$	2	2
5473	-1	-2	2	2	-4	$*$	2	8

Table 5.3.1.2: Rational Hecke eigenclasses over F_1

Table 5.3.1.3 below lists generators for the prime ideals of norm up to 25:

$\mathfrak{p}$	Generator	$\mathfrak{p}$	Generator
$\mathfrak{p}_2$	$-t^2+t+1$	$\mathfrak{p}_{13,3}$	$-t^3-t+1$
$\mathfrak{p}_3$	t^2+1	$\mathfrak{p}_{13,4}$	t^3+t^2+1
$\mathfrak{p}_{13,1}$	$-t^3+t^2+1$	$\mathfrak{p}_{5,1}$	$2t^2-t-2$
$\mathfrak{p}_{13,2}$	t^3+t+1	$\mathfrak{p}_{5,2}$	t^3-2t^2-t

Table 5.3.1.3: Generators for prime ideals of F_1 of small norm

In Table 5.3.1.4, we list the "old" classes we discovered: those which correspond to classes appearing at a lower level. We observe that in each case, the set of Hecke eigenvalues matches those of the original eigenclass. Lower case Roman numerals are used to denote each eigenclass.

Class	$\mathfrak{p}_2$	$\mathfrak{p}_3$	$\mathfrak{p}_{13,1}$	$\mathfrak{p}_{13,2}$	$\mathfrak{p}_{13,3}$	$\mathfrak{p}_{13,4}$	$\mathfrak{p}_{5,1}$	$\mathfrak{p}_{5,2}$	Original Class
676 (**i-ii**)	$*$	-4	0	$*$	0	$*$	-2	-2	169
1521 (**i-ii**)	-2	$*$	0	$*$	0	$*$	-2	-2	169
1764 (**i-ii**)	$*$	$*$	-6	4	4	-6	-4	-4	441
1936 (**i-ii**)	$*$	-5	-1	-1	-1	-1	-4	-4	484
2197a (**i-ii**)	-2	-4	0	$*$	$*$	$*$	-2	-2	169
2197b (**i-ii**)	-2	-4	0	$*$	0	$*$	-2	-2	169
2304 (**i-ii**)	$*$	$*$	-2	-2	-2	-2	-6	-6	576
2704 (**ii-iv**)	$*$	-4	0	$*$	0	$*$	-2	-2	169
3969 (**i-ii**)	0	$*$	-6	4	4	-6	-4	-4	441
4225a (**i-ii**)	-2	-4	0	$*$	0	$*$	-2	$*$	169
4356 (**i-ii**)	$*$	$*$	-2	6	-2	6	-6	-6	1089 (I)
4356 (**iii-iv**)	$*$	$*$	4	-6	4	-6	6	6	1089 (II)
4356 (**v-vi**)	$*$	$*$	-1	-1	-1	-1	-4	-4	484
4624 (**i-ii**)	$*$	0	4	4	-6	-6	6	6	1156
5184 (**i-ii**)	$*$	$*$	-2	-2	-2	-2	-6	-6	576

Table 5.3.1.4: "Old" cohomology classes

In Table 5.3.1.5 we list the eigenclasses which correspond to the base change of an automorphic representation π' defined over a subfield of F, such that the Hecke eigenvalues $a_{\mathfrak{p}}(\pi')$ are rational. For each of these classes, we were able to find an elliptic curve defined over the corresponding subfield whose local data matched these eigenvalues (listed in Table 5.3.1.11).

Class	$\mathfrak{p}_2$	$\mathfrak{p}_3$	$\mathfrak{p}_{13,1}$	$\mathfrak{p}_{13,2}$	$\mathfrak{p}_{13,3}$	$\mathfrak{p}_{13,4}$	$\mathfrak{p}_{5,1}$	$\mathfrak{p}_{5,2}$	Base Field
484	$*$	-5	-1	-1	-1	-1	-4	-4	$\mathbb{Q}(\sqrt{3})$
576	$*$	$*$	-2	-2	-2	-2	-6	-6	$\mathbb{Q}(\sqrt{3})$
1089 (**i**)	-3	$*$	-2	6	-2	6	-6	-6	$\mathbb{Q}(\sqrt{3})$
1089 (**ii**)	0	$*$	4	-6	4	-6	6	6	$\mathbb{Q}(\sqrt{3})$
2209	-3	-2	-6	0	-6	0	-6	-6	$\mathbb{Q}(\sqrt{3})$
2704 (**i**)	$*$	-2	2	$*$	2	$*$	2	2	$\mathbb{Q}(\sqrt{3})$
2916 (**i**)	$*$	$*$	5	-4	5	-4	-1	-1	$\mathbb{Q}(\sqrt{3})$
2916 (**ii**)	$*$	$*$	-4	5	-4	5	-1	-1	$\mathbb{Q}(\sqrt{3})$
4225c	-4	-2	$*$	$*$	-4	-4	$*$	-10	$\mathbb{Q}(\sqrt{-1})$
5041 (**i**)	0	5	-6	-1	-6	-1	1	1	$\mathbb{Q}(\sqrt{3})$
5041 (**ii**)	-4	5	2	-1	2	-1	-7	-7	$\mathbb{Q}(\sqrt{3})$
5329d	-1	-2	2	2	2	2	2	2	$\mathbb{Q}(\sqrt{-3})$
5476 (**i**)	$*$	-5	-4	-7	-4	-7	2	2	$\mathbb{Q}(\sqrt{3})$

Table 5.3.1.5: Base change from rational Hecke eigenclasses

In Table 5.3.1.6 we list the remaining eigenclasses which correspond to the base change of an automorphic representation π' defined over a subfield of F. In each case, the Hecke eigenvalues $a_{\mathfrak{p}}(\pi')$ lie in a quadratic extension of $\mathbb{Q}$, and so there is no elliptic curve defined over the corresponding subfield of F whose local data matches these eigenvalues. However, for each class, we were able to find an elliptic curve defined over F whose local data matched the eigenvalues $a_{\mathfrak{p}}(\pi)$ (listed in Table 5.3.1.12).

Class	$\mathfrak{p}_2$	$\mathfrak{p}_3$	$\mathfrak{p}_{13,1}$	$\mathfrak{p}_{13,2}$	$\mathfrak{p}_{13,3}$	$\mathfrak{p}_{13,4}$	$\mathfrak{p}_{5,1}$	$\mathfrak{p}_{5,2}$	Base Field
169	-2	-4	0	$*$	0	$*$	-2	-2	$\mathbb{Q}(\sqrt{3})$
4096	$*$	2	-2	-2	-2	-2	2	2	$\mathbb{Q}(\sqrt{3})$

Table 5.3.1.6: Base change from non-rational Hecke eigenclasses

In Table 5.3.1.7 we list the remaining two eigenclasses with rational Hecke eigenvalues, which match those of the Eisenstein cohomology, up to sign. We observe that the ray class group $Cl(\mathcal{O}_F, \mathfrak{n})$ of the corresponding level admits a single non-trivial quadratic character χ, and that the Hecke eigenvalues are given by

$$a_{\mathfrak{p}}(\pi) = \chi(\mathfrak{p})(\mathrm{Norm}_{F/\mathbb{Q}}(\mathfrak{p}) + 1).$$

Class	$\mathfrak{p}_2$	$\mathfrak{p}_3$	$\mathfrak{p}_{13,1}$	$\mathfrak{p}_{13,2}$	$\mathfrak{p}_{13,3}$	$\mathfrak{p}_{13,4}$	$\mathfrak{p}_{5,1}$	$\mathfrak{p}_{5,2}$	$\mathfrak{p}_{37,1}$	$\mathfrak{p}_{37,2}$	$\mathfrak{p}_{37,3}$	$\mathfrak{p}_{37,4}$
5329*a* (**i**)	-5	-10	14	-14	-14	-14	26	-26	-38	-38	38	38
5329*a* (**ii**)	-5	-10	14	-14	-14	-14	26	-26	-38	-38	38	38

Table 5.3.1.7: Remaining rational eigenclasses

In Tables 5.3.1.8 and 5.3.1.9 we list the remaining eigenclasses, whose eigenvalues lie in a proper extension of $\mathbb{Q}$. For the classes appearing in Table 5.3.1.8, the field $\mathbb{Q}(a_{\mathfrak{p}}(\pi))$ generated by these eigenvalues is a quadratic extension of $\mathbb{Q}$, and we list the pair of Galois conjugate eigenvalues for each prime. For the classes appearing in Table 5.3.1.9, the field $\mathbb{Q}(a_{\mathfrak{p}}(\pi))$ is either a cubic or a quartic extension of $\mathbb{Q}$, and for each prime we list the polynomial whose roots are the corresponding eigenvalues.

Class	$\mathfrak{p}_2$	$\mathfrak{p}_3$	$\mathfrak{p}_{13,1}$	$\mathfrak{p}_{13,2}$	$\mathfrak{p}_{13,3}$	$\mathfrak{p}_{13,4}$	$\mathbb{Q}(a_{\mathfrak{p}}(\pi))$
625 (**i-ii**)	$\frac{1\pm\sqrt{17}}{2}$	$-1 \pm \sqrt{17}$	$-1 \pm \sqrt{17}$	$-1 \pm \sqrt{17}$	$-1 \pm \sqrt{17}$	$-1 \pm \sqrt{17}$	$\mathbb{Q}(\sqrt{17})$
1369 (**i-ii**)	$\frac{-3\pm\sqrt{17}}{2}$	$\frac{-5\pm\sqrt{17}}{2}$	$\frac{3\pm\sqrt{17}}{2}$	$1 \pm \sqrt{17}$	$\frac{3\pm\sqrt{17}}{2}$	$1 \pm \sqrt{17}$	$\mathbb{Q}(\sqrt{17})$
2116 (**i-ii**)	$*$	$-2 \pm 2\sqrt{3}$	$-1 \pm 3\sqrt{3}$	$2 \pm 2\sqrt{3}$	$-1 \pm 3\sqrt{3}$	$2 \pm 2\sqrt{3}$	$\mathbb{Q}(\sqrt{3})$
2500*b* (**i-iv**)	$*$	$-1 \pm \sqrt{17}$	$-1 \pm \sqrt{17}$	$-1 \pm \sqrt{17}$	$-1 \pm \sqrt{17}$	$-1 \pm \sqrt{17}$	$\mathbb{Q}(\sqrt{17})$
3481 (**i-ii**)	$\frac{-5\pm\sqrt{5}}{2}$	$\frac{-5\pm3\sqrt{5}}{2}$	$-1 \pm 2\sqrt{5}$	$\frac{-7\pm3\sqrt{5}}{2}$	$-1 \pm 2\sqrt{5}$	$\frac{-7\pm3\sqrt{5}}{2}$	$\mathbb{Q}(\sqrt{5})$
5329*b* (**i-ii**)	$\pm\sqrt{7}$	$\pm2\sqrt{7}$	-4	-4	$1 \pm \sqrt{7}$	$1 \pm \sqrt{7}$	$\mathbb{Q}(\sqrt{7})$
5476 (**ii-v**)	$*$	$\frac{-5\pm\sqrt{17}}{2}$	$1 \pm \sqrt{17}$	$\frac{3\pm\sqrt{17}}{2}$	$1 \pm \sqrt{17}$	$\frac{3\pm\sqrt{17}}{2}$	$\mathbb{Q}(\sqrt{17})$

Table 5.3.1.8: Eigenclasses with eigenvalues lying in a quadratic extension of $\mathbb{Q}$

Class	$\mathfrak{p}_2$	$\mathfrak{p}_3$	$\mathbb{Q}(a_{\mathfrak{p}}(\pi))$
2401 (**i-iii**)	$x^3+2x^2-11x-20$	$x^3+2x^2-32x-80$	$\mathbb{Q}(x^3+x^2-8x-10)$
$3721a$ (**i-iii**)	x^3+2x^2-9x-6	x^3+5x^2-x-2	$\mathbb{Q}(x^3-x^2-9x+12)$
4761 (**i-iii**)	x^3+3x^2-4x-4	$*$	$\mathbb{Q}(x^3-x^2-4x+2)$
$5329c$ (**i-iv**)	$x^4+4x^3-3x^2-16x-8$	$x^4+8x^3+6x^2-48x-64$	$\mathbb{Q}(x^4-9x^2-2x+2)$

Table 5.3.1.9: Eigenclasses with eigenvalues lying in a cubic or quartic extension of $\mathbb{Q}$

In Table 5.3.1.10 (on the next page) we list the coefficients a_i of the Weierstrass polynomial

$$y^2+a_1xy+a_3y=x^3+a_2x^2+a_4x+6$$

defining the global minimal model of an elliptic curve E over F whose local data matches the Hecke eigenvalues of the classes appearing in Table 5.3.1.2.

In Table 5.3.1.11 (below) we list the coefficients a_i of the Weierstrass polynomial defining the global minimal model of an elliptic curve E over a subfield of F such that the Hecke eigenvalues of the classes appearing in Table 5.3.1.5 match the local data of the base change of E to F.

In Table 5.3.1.12 (on the next page) we list the coefficients of the Weierstrass polynomial defining the global minimal model of an elliptic curve E over F whose local data matches the Hecke eigenvalues of the classes appearing in Table 5.3.1.6.

Class	a_1	a_2	a_3	a_4	a_6
484	$\sqrt{3}$	$\sqrt{3}+1$	$\sqrt{3}$	$2\sqrt{3}+2$	$\sqrt{3}+1$
576	$\sqrt{3}+1$	$-\sqrt{3}+1$	0	$-5\sqrt{3}-6$	$3\sqrt{3}+6$
1089(**i**)	1	$-\sqrt{3}$	0	1	0
1089(**ii**)	$\sqrt{3}+1$	$-\sqrt{3}$	1	$5\sqrt{3}-9$	$-6\sqrt{3}+10$
2209	1	$-\sqrt{3}$	1	$-\sqrt{3}-1$	0
2704(**i**)	0	$\sqrt{3}-1$	0	2	$2\sqrt{3}+3$
2916(**i**)	1	-1	$\sqrt{3}+1$	$-23\sqrt{3}-41$	$217\sqrt{3}+377$
2916(**ii**)	1	-1	$\sqrt{3}+1$	$22\sqrt{3}-41$	$-218\sqrt{3}+377$
$4225c$	$\sqrt{-1}+1$	$-\sqrt{-1}$	$\sqrt{-1}$	1	0
5041(**i**)	0	-1	$\sqrt{3}$	$-2\sqrt{3}-4$	$3\sqrt{3}+5$
5041(**ii**)	0	1	$\sqrt{3}$	$\sqrt{3}+2$	$\sqrt{3}+1$
$5329d$	$3\sqrt{-3}$	$\sqrt{-3}+7$	$\frac{1}{2}(\sqrt{-3}-5)$	$4\sqrt{-3}+1$	$\frac{1}{2}(\sqrt{-3}-3)$
5476	1	$-\sqrt{3}+1$	$\sqrt{3}$	$-\sqrt{3}+1$	$-\sqrt{3}+1$

Table 5.3.1.11: Elliptic curves corresponding to the classes in Table 5.3.1.5

Class	a_1	a_2	a_3	a_4	a_6
441	$-3t^3-3t^2+3t$	$2t+2$	$5t^3-2t^2-4t-2$	$-t^3-12t^2-7t+9$	$6t^3+6t^2-9t-3$
1156	$-6t^3-6t^2+3$	$-13t^3-7t^2+20t+20$	$4t^3-7t^2-17t-13$	$-165t^3-66t^2+64t+11$	$235t^3-270t^2-288t+145$
2041	$-3t^3+3$	$-t^3-7t^2+2t+1$	$-t^3-9t^2-2t-1$	$-10t^3+28t^2+31t+15$	$-262t^3-262t^2+98t+219$
2257	$-3t^3-3t^2$	$-8t^3-7t^2+2t+7$	$9t^3+t^2-12t-13$	$-10t^3-29t^2-28t-14$	$68t^3+35t^2-65t-71$
2452	$3t^3-3t-3$	$2t^3+5t^2+3t-1$	$5t^3-12t-9$	$29t^3+17t^2-9t-17$	$41t^3+22t^2-39t-33$
2500a	$-3t^3-6t^2$	$-11t^3-13t^2+13t+14$	$4t^3-3t^2-8t-3$	$-15t^3-46t^2-11t+28$	$4t^3-11t^2-29t-3$
2977	$-3t^3+3$	$-t^3-3t^2+2t-1$	$-8t^2-t-6$	$-11t^3+8t^2+5$	$2t^3-29t^2-3t$
3328	$-3t^3+3t^2+3t$	$2t^3-9t-1$	$5t^2-3t-7$	$-50t^3+25t^2+54t-31$	$139t^3-87t^2-115t+121$
3721b	$-3t^3+3$	t^3-7t^2+t	$5t^3-8t^2-3t-4$	$-14t^3+23t^2-t-15$	$28t^3-21t^2-13t+21$
3844	$-3t^3-3t^2$	$-8t^3-7t^2+2t+8$	$8t^3-9t-7$	$-7399t^3-3866t^2+8173t+9088$	$-182355t^3-372229t^2-280418t-56472$
4033a	$-3t$	$-5t^2-t+1$	$5t^3+4t^2-7t$	$8t^3-2t^2-t-10$	$4t^3+2t^2+11t-7$
4033b	$-6t^3-3t^2+3t+3$	$-t^3+6t^2+7t$	$2t^3-5t^2-12t-2$	$-24t^3-28t^2+19t+37$	$-11t^3-24t^2-26t-20$
4057	$-6t^3-6t^2+3$	$-9t^3-7t^2+16t+17$	$14t^3+7t^2-16t-19$	$-53t^3-82t^2-41t-3$	$132t^3+106t^2-90t-130$
4069	$3t^3+3t^2+3$	$-11t^3-5t^2+9t+6$	$8t^2+4t-2$	$-17t^3-21t^2+19t+29$	$-15t^3-5t^2+14t+20$
4225b	$3t^2-3t-3$	t^3-t^2-2t	$-4t^3+4t^2+7t+2$	$-4t^3-2t^2+5t+16$	$-2t^3-6t^2-16t-8$
4516	$3t^3+3t^2-3$	t^3+4t^2+3t	t^3-3t^2-3t-1	$-5t^3+13t^2+5t-22$	$-16t^3+5t^2+10t-15$
4672	$3t^3+3$	$-9t^3+4t^2+10t+9$	$4t^3+8t^2+12t+14$	$130t^3-152t^2-30t+208$	$-514t^3-122t^2+1086t-764$
4852	$-3t^2-6t-3$	$-7t^3-13t^2-10t-1$	$-10t^3-9t^2+6t+7$	$-47t^3-29t^2+42t+52$	$16t^3+31t^2+24t+4$
5317	$-3t^2-3t$	$-4t^3-4t^2-3t+1$	$5t^3+6t^2-t-2$	$13t^3+13t^2-8t-15$	$-6t^3+13t+10$
5473	$3t^2$	$-2t^2+3t+3$	t^2+3t-1	$-20t^3+13t^2+58t+43$	$190t^3+188t^2-54t-144$

Table 5.3.1.10: Elliptic curves corresponding to the classes in Table 5.3.1.2

Class	a_1	a_2	a_3	a_4	a_6
169	$3t^3-3t^2-3t$	$-t^3+2t^2-3t-2$	$-2t^3+2t^2-t+2$	$-6t^3+t^2+9t-3$	$5t^3-3t^2-t+2$
4096	$2t+2$	$-t^2+t-1$	$2t^3+2$	$-2t^3+2t^2-2t$	0

Table 5.3.1.12: Elliptic curves corresponding to the classes in Table 5.3.1.6

5.3.2 The Field F_2

Let $F = F_2 = \mathbb{Q}(t)$, where t is a root of the polynomial $x^4 - x^3 + 2x^2 + x + 1$. As mentioned previously, due to time constraints we were unable to perform such an in-depth analysis as for the field F_1, so we restricted our attention to levels $\mathfrak{n}$ which were unfixed by the Galois group $\mathrm{Gal}(F/\mathbb{Q})$, as we expect that eigenclasses arising from such levels should not occur as a base change from a subfield.

We searched over all such levels of norm up to 2150, of which there are 196, up to Galois conjugation. We detected non-Eisenstein cohomology at 4 of these levels, with a total of 6 non-Eisenstein Hecke eigenclasses spread across these levels. Table 5.3.2.1 below lists a set of generators for the levels studied, together with their factorization type and the discrepancy d between the rank of $H_1((\mathscr{S}_*)_{\Gamma_0(\mathfrak{n})}, \mathbb{C})$ and the expected rank of the Eisenstein cohomology:

Level	Generator	Type	d	Level	Generator	Type	d
244	$-t^3 + 3t^2 - 6t + 2$	$\mathfrak{pq}$	1	976*b*	$t^3 - 2t^2 + 6t - 5$	$\mathfrak{pqr}$	2
976*a*	$3t^2 - 2t + 7$	$\mathfrak{p}^2\mathfrak{q}$	2	2071	$\frac{1}{2}(9t^3 - 16t^2 + 28t + 3)$	$\mathfrak{pq}$	1

Table 5.3.2.1: Levels with non-Eisenstein cohomology classes

Each of the 6 non-Eisenstein Hecke eigenclasses we detected admitted rational eigenvalues, of which:

- 4 had eigenvalues matching an eigenclass appearing at a lower level;
- 2 classes appear to be defined purely over F, and we were able to find elliptic curves defined over F whose local data matched the eigenvalue data for both of these classes. We list these classes in Table 5.3.2.2 below:

Class	$\mathfrak{p}_{2,1}$	$\mathfrak{p}_{2,2}$	$\mathfrak{p}_3$	$\mathfrak{p}_{19,1}$	$\mathfrak{p}_{19,2}$	$\mathfrak{p}_{19,3}$	$\mathfrak{p}_{19,4}$	$\mathfrak{p}_5$
244	$*$	$*$	-2	-4	-4	-4	8	2
2071	-1	-1	-2	2	$*$	2	2	8

Table 5.3.2.2: Rational Hecke eigenclasses over F_2

Table 5.3.2.3 below lists generators for the prime ideals of norm up to 25:

$\mathfrak{p}$	Generator	$\mathfrak{p}$	Generator
$\mathfrak{p}_{2,1}$	$\frac{1}{2}(-t^3 + 2t^2 - 4t - 1)$	$\mathfrak{p}_{19,2}$	$\frac{1}{2}(-t^3 + 2t^2 - 4t - 3)$
$\mathfrak{p}_{2,2}$	$t^3 - t^2 + 2t$	$\mathfrak{p}_{19,3}$	$\frac{1}{2}(-t^3 - 2t - 5)$
$\mathfrak{p}_3$	$\frac{1}{2}(t^3 - 2t^2 + 2t - 3)$	$\mathfrak{p}_{19,4}$	$t - 2$
$\mathfrak{p}_{19,1}$	$\frac{1}{2}(3t^3 - 4t^2 + 4t + 1)$	$\mathfrak{p}_5$	$\frac{1}{2}(-3t^3 + 2t^2 - 6t - 3)$

Table 5.3.2.3: Generators for prime ideals of F_2 of small norm

Table 5.3.2.4 lists the "old" classes we detected at the two levels of norm 976:

Class	$\mathfrak{p}_{2,1}$	$\mathfrak{p}_{2,2}$	$\mathfrak{p}_3$	$\mathfrak{p}_{19,1}$	$\mathfrak{p}_{19,2}$	$\mathfrak{p}_{19,3}$	$\mathfrak{p}_{19,4}$	Original Class
976a (**i-ii**)	$*$	$*$	-2	-4	-4	-4	8	244
976b(**i-ii**)	$*$	$*$	-2	-4	-4	-4	8	244

Table 5.3.2.4: "Old" cohomology classes

In Table 5.3.2.5 we list the coefficients a_i of the Weierstrass polynomial defining the global minimal model of an elliptic curve E over F whose local data matches the Hecke eigenvalues of the classes appearing in Table 5.3.2.1.

Class	a_1	a_2	a_3	a_4	a_6
244	$2t^2-3t$	t^3+3t^2-3t+3	$-t^3-t^2-t+1$	$-6t^3-t^2-8t-3$	$-t^3+6t^2+2t-1$
2071	t^3+t+1	$-2t^3+4t^2-6t-1$	$\frac{1}{2}(-3t^3-2t-1)$	$-3t^3-2t^2+t-5$	$3t^3-3t^2+2t$

Table 5.3.2.5: Elliptic curves corresponding to the classes in Table 5.3.2.2

5.3.3 The Field F_3

Let $F = F_3 = \mathbb{Q}(t)$, where t is a primitive eighth root of unity. As was the case for the field F_2, we restricted our attention to levels $\mathfrak{n}$ which were unfixed by the Galois group $\mathrm{Gal}(F/\mathbb{Q})$.

We searched over all such levels of norm up to 1000, of which there are 90, up to Galois conjugation. We detected non-Eisenstein cohomology at only a single level, which we list in Table 5.3.3.1 below:

Level	Generator	Type	d
881	$-4t^2 + 5t$	$\mathfrak{p}$	1

Table 5.3.3.1: Level with a non-Eisenstein cohomology class

This class did not appear to correspond to the base change of an automorphic representation over a subfield of F, and we were able to find an elliptic curve whose local data matched the Hecke eigenvalues for this class. We list these eigenvalues for a number of primes of small norm in Table 5.3.3.2.

Class	$\mathfrak{p}_2$	$\mathfrak{p}_{3,1}$	$\mathfrak{p}_{3,2}$	$\mathfrak{p}_{17,1}$	$\mathfrak{p}_{17,2}$	$\mathfrak{p}_{17,3}$	$\mathfrak{p}_{17,4}$	$\mathfrak{p}_{5,1}$	$\mathfrak{p}_{5,2}$
881	0	4	-2	-6	0	0	0	2	2

Table 5.3.3.2: Rational Hecke eigenclass over F_3

Table 5.3.3.3 below lists generators for the prime ideals of norm up to 25:

$\mathfrak{p}$	Generator	$\mathfrak{p}$	Generator
$\mathfrak{p}_2$	$t+1$	$\mathfrak{p}_{17,3}$	$2*t+1$
$\mathfrak{p}_{3,1}$	t^3+t^2-t	$\mathfrak{p}_{17,4}$	$2*t^3+1$
$\mathfrak{p}_{3,2}$	t^3-t^2-t	$\mathfrak{p}_{5,1}$	$2*t^3-t$
$\mathfrak{p}_{17,1}$	$t+2$	$\mathfrak{p}_{5,2}$	t^3-2*t
$\mathfrak{p}_{17,2}$	t^3+2		

Table 5.3.3.3: Generators for prime ideals of F_3 of small norm

In Table 5.3.3.4 we list the coefficients a_i of the Weierstrass polynomial defining the global minimal model of an elliptic curve E over F whose local data matches the Hecke eigenvalues of this class.

Class	a_1	a_2	a_3	a_4	a_6
881	$-2t^2-t-1$	$-7t^3-7t^2-2t+3$	$14t^3-2t^2-17t-22$	$55t^3-88t^2-75t+29$	$138t^3+192t^2-515t-81$

Table 5.3.3.4: Elliptic curve corresponding to the class in Table 5.3.3.2

5.4 Practical Considerations

We shall now briefly mention a few technical issues relating to our computation. To begin with, as per **[AGM02]**, we choose to work with the finite field $\mathbb{F}_{12379}$ rather than the complex numbers as our coefficient field. While this runs the risk of introducing additional cohomology classes (as would be the case if the torsion subgroup of the *integral* cohomology $H^*(\Gamma_0(\mathfrak{n}), \mathbb{C})$ had order divisible by 12379, this can be remedied by computing Betti numbers for various large primes, and ensuring that they match. Working with coefficients in a finite field makes several calculations both quicker and less susceptible to error, which we illustrate with the following example:

Let $\mathfrak{n}$ be the ideal of norm 2977 in F_1 generated by $4t^3+2t^2-9t+2$, where t is a primitive twelfth root of unity. To construct the homology $H_1((\mathscr{S})_{\Gamma_0(\mathfrak{n})}, \mathbb{F}_{12379})$, we first determine a set of representatives for the $\Gamma_0(\mathfrak{n})$-orbits of totally reduced sharblies (as per **[AGM02], Section 3**). We find that there are a total of 135 non-trivial $\Gamma_0(\mathfrak{n})$-orbits of totally reduced 0-sharblies (where by a non-trivial sharbly we mean one whose stabilizer in $\Gamma_0(\mathfrak{n})$ contains no orientation-reversing elements), 4024 non-trivial $\Gamma_0(\mathfrak{n})$-orbits of totally reduced 1-sharblies, and 20269 non-trivial $\Gamma_0(\mathfrak{n})$-orbits of totally reduced 2-sharblies.

We construct matrices D_1 and D_2 corresponding to the differentials

$$\partial_1 : (\mathscr{S}_1)_{\Gamma_0(\mathfrak{n})} \to (\mathscr{S}_0)_{\Gamma_0(\mathfrak{n})}$$

$$\partial_2 : (\mathscr{S}_2)_{\Gamma_0(\mathfrak{n})} \to (\mathscr{S}_1)_{\Gamma_0(\mathfrak{n})}.$$

Consequently, D_1 is a 135×4024 matrix, and D_2 is a 4024×20269 matrix. For such large matrices (and these are by no means the largest we will be dealing with) working with coefficients in a finite field is much more efficient.

Using MAGMA, we can compute the kernel of the matrix D_2 and the image of the matrix D_1, and then construct the quotient space $\ker(D_2)/\mathrm{Im}(D_1)$, which is isomorphic to the homology $H_1((\mathscr{S}_*)_{\Gamma_0(\mathfrak{n})}, \mathbb{F}_{12379})$ (we remark that this differs from the method outlined in **[AGM02], Section 5.2**, in which one instead constructs the kernel of the matrix

$$\mathcal{D} = \begin{pmatrix} D_1 \\ D_2^T \end{pmatrix},$$

which is also isomorphic to the homology of the sharbly complex. In practice, our method seems to yield a "better" choice of basis for the homology, in the sense that the resulting vectors have significantly fewer non-zero entries, meaning we have fewer sharblies to reduce in order to compute the Hecke action).

We can therefore construct a basis for the first homology group, which we find is an 8-dimensional space. Since the ideal $\mathfrak{n}$ is prime, this corresponds to the expected 7-dimensional Eisenstein space and a 1-dimensional cuspidal space.

The basis sharbly cycles $\xi_1, \ldots, \xi_8$ have, respectively, 55, 5, 66, 1, 2, 1, 1 and 1 non-trivial sharblies in their support. This is fairly typical, in our experience; quite often we can find basis sharbly cycles with both quite large and very small support.

The matrix for the action of the Hecke operator $T_{\mathfrak{p}_2}$, where $\mathfrak{p}_2$ lies above the rational prime 2, on this basis is given by

$$\begin{pmatrix} 10321 & 0 & 0 & 5158 & 0 & 5158 & 7221 & 7221 \\ 4120 & 5 & 0 & 2060 & 0 & 2060 & 10319 & 10319 \\ 4126 & 0 & 5 & 2063 & 0 & 2063 & 10316 & 10316 \\ 0 & 0 & 0 & 5 & 0 & 0 & 0 & 0 \\ 4123 & 0 & 0 & 8251 & 5 & 8251 & 4128 & 4128 \\ 0 & 0 & 0 & 0 & 0 & 5 & 0 & 0 \\ 8259 & 0 & 0 & 10319 & 0 & 10319 & 2065 & 2060 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 5 \end{pmatrix}$$

which we see has eigenvalues 5 (with multiplicity seven) and 2.

A basis for the Eisenstein subspace (with respect to our original basis $\xi_1, \ldots, \xi_8$) is then given by the vectors

$$\begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 2 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 12378 \end{pmatrix}$$

while the cuspidal cycle is given by

$$\begin{pmatrix} 1 \\ 12341 \\ 12377 \\ 0 \\ 12359 \\ 0 \\ 38 \\ 0 \end{pmatrix}.$$

In particular, if we denote by $\mathrm{Eis}_1, \ldots, \mathrm{Eis}_7$ the above basis for the Eisenstein subspace, and by Cusp the cuspidal cycle, we have

$$\mathrm{Cusp} = \mathrm{Eis}_1 + 12341\mathrm{Eis}_2 + 12377\mathrm{Eis}_3 + 12359\mathrm{Eis}_5 + 38\mathrm{Eis}_7 + 36\xi_8.$$

This is key to our ability to compute Hecke operators efficiently. Suppose, for example, that reducing a single 1-sharbly $\mathbf{u}$ (that is, applying the algorithm in the previous section as many times as necessary to produce a chain whose support is all totally reduced) were to take 15 seconds (in practice, some sharblies can take much, much longer to reduce, and the time increases with the size of the sharbly). The cycle Cusp has 79 sharblies in its support, so computing the Hecke operator $T_{\mathfrak{p}_2}$ would take 5925 seconds, or just under 1.6 hours. For a Hecke operator at a prime ideal of norm roughly 400, this increases to roughly 5.5 days.

Fortunately, in our case we can rapidly speed up proceedings. Indeed, since we can express Cusp in terms of Eisenstein cycles and the cycle ξ_8, we can (since we know the action of the Hecke operators on the Eisenstein cycles) compute the action of Cusp simply by computing the corresponding action on ξ_8, which has only a single sharbly in its support. In this case, computing a Hecke operator at a prime of ideal of norm roughly 400 will take only around 1.6 hours. For many of our examples, we were able to use this method to compute many more Hecke eigenvalues than would otherwise be possible.

Chapter 6

Proving Modularity of an Elliptic Curve

In this, the final chapter, we discuss a method for determining the equivalence of two Galois representations

$$\rho_1, \rho_2 : \mathrm{Gal}(\overline{F}/F) \to \mathrm{GL}_2(\mathbb{Q}_\ell),$$

subject to certain constraints. We begin in **Section 6.1** by discussing residual Galois representations, and show that the residual representation $\widetilde{\rho}$ of a representation ρ can be defined over any field which contains the coefficients of the characteristic polynomials of $\tilde{\rho}$ on Frobenius elements.

In **Section 6.2**, we recall the Galois representations that we wish to compare, namely those attached to elliptic curves defined over a number field F, and the representation presented in **Section 3.5** attached to certain cuspidal automorphic forms.

Section 6.3 is dedicated to the method of proving equivalence of the residual reprsentations $\widetilde{\rho_1}$ and $\widetilde{\rho_2}$. **Sections 6.4** discuss the method of Livné for proving equivalence of the original representations when the $\widetilde{\rho_i}$ are not absolutely irreducible, while **Section 6.5** discuss the method of Faltings and Serre for proving equivalence when the representations $\widetilde{\rho_i}$ are absolutely irreducible.

Finally, in **Sections 6.6** we apply these methods to prove modularity of all but one of the elliptic curves found in **Section 5.3**.

6.1 Residual Galois Representations

Let F be a number field, let G_F denote the absolute Galois group $\mathrm{Gal}(\overline{F}/F)$, and let $\rho : G_F \to \mathrm{GL}_2(\overline{\mathbb{Q}}_\ell)$ be a continuous ℓ-adic Galois representation. In this section we will show that one can define a *residual* representation

$$\tilde{\rho} : G_F \to \mathrm{GL}_2(\overline{\mathbb{F}}_\ell),$$

related to ρ, such that two isomorphic representations ρ_1, ρ_2 have isomorphic residual representations. Moreover, we shall show that the image of this representation is contained in the finite group $\mathrm{GL}_2(\mathbb{F}_{\ell^r})$, for some $r \geq 1$, which depends only on the coefficients of the characteristic polynomial of $\tilde{\rho}$ on Frobenius elements of G_F.

We begin with the following standard result, a proof of which we borrow from a note by C. Skinner (**[Ski09], Section 2**).

Proposition 6.1.1. *Let $\rho : G_F \to \mathrm{GL}_2(\overline{\mathbb{Q}}_\ell)$ be a continuous ℓ-adic Galois representation. Then there exists a finite extension V of $\mathbb{Q}_\ell$ such that the image of ρ is contained in $\mathrm{GL}_2(V)$.*

Proof. It is known (see, for example, **Chapter 3, Section 1.6** of **[Rob00]**) that for each positive integer n, there are only finitely many extensions of $\mathbb{Q}_\ell$ of degree n. The finite extensions W of $\mathbb{Q}_\ell$ contained in $\overline{\mathbb{Q}}_\ell$ therefore form a countable set, and for each such field W, $\mathrm{GL}_2(W)$ is closed in $\mathrm{GL}_2(\overline{\mathbb{Q}}_\ell)$. Since ρ is by definition continuous, the subgroups $G_W := \rho^{-1}(\mathrm{GL}_2(W))$ form a countable set of closed subgroups of G_F, whose union is G_F itself. Since G_F is compact, it carries a Haar measure with total measure finite and non-zero. In particular, since the countable union of measurable sets each having measure zero must also have measure zero, it follows that *some* G_W must have non-zero measure, and hence finite index in G_F. Write G_F as the disjoint union

$$G_F = \coprod_{i=1}^{n} g_i G_W$$

for some choice of coset representatives g_i. Then the image of ρ is contained in $\mathrm{GL}_2(V)$, where V is the finite extension of $\mathbb{Q}_\ell$ generated by W and the entries of the $\rho(g_i)$. □

To construct the residual representation, we first show that any representation $\rho : G_F \to \mathrm{GL}_2(V)$ with V a finite extension of $\mathbb{Q}_\ell$ fixes a lattice in V (that is, an $\mathcal{O}_V$-module Π such that $\Pi \otimes_{\mathcal{O}_V} V \simeq V^2$, where $\mathcal{O}_V$ is the valuation ring of V). We then show that the representation in fact factors through the group $\mathrm{GL}(\Pi)$, so that, up to isomorphism, we may consider ρ as a representation $\rho : G_F \to \mathrm{GL}_2(\mathcal{O}_V)$, which we may then compose with the reduction map from $\mathrm{GL}_2(\mathcal{O}_V)$ to $\mathrm{GL}_2(k_V)$, where k_V is the residue field of V.

Proposition 6.1.2. *Let $\rho : G_F \to \mathrm{GL}_2(V)$ be a Galois representation, with V a finite extension of $\mathbb{Q}_\ell$, and let $\mathcal{O}_V$ denote the valuation ring of V. Then, up to isomorphism, we may realise ρ as a representation $\rho : G_F \to \mathrm{GL}_2(\mathcal{O}_V)$.*

Proof. Let Λ be *any* lattice in V^2. Since Λ is open in V^2, the group $G_\Lambda := \{g \in \mathrm{GL}_2(V);\ g(\Lambda) = \Lambda\}$ is open in $\mathrm{GL}_2(V)$, and so $H_\Lambda := \rho(G) \cap G_\Lambda$ is open in $\rho(G)$. Since ρ is continuous, $\rho(G)$ is compact and thus H_Λ has finite index in $\rho(G)$.

Choose a set $\{g_1, \ldots, g_n\}$ of coset representatives of $\rho(G)/H_\Lambda$. Now, for each i, $g_i(\Lambda)$ has finite index in $\mathcal{O}_V^2$, and thus in particular

$$\Pi := \sum_{i=1}^{n} g_i(\Lambda)$$

is a lattice in V^2, which is G_F-stable by construction.

Since by definition $\Pi \otimes_{\mathcal{O}_V} V \simeq V^2$, any element $\rho(g) \in \mathrm{GL}_2(V)$ which acts trivially on Π must also act trivially on V^2, and so ρ factors through $\mathrm{GL}(\Pi)$. Since Π is of full rank, we can find some matrix in $\mathrm{GL}_2(V)$ which maps the generators of Π to the standard generators of $\mathcal{O}_V^2$, and thus after conjugation by this matrix we may assume that $\rho : G_F \to \mathrm{GL}_2(\mathcal{O}_V)$, as required. □

As mentioned previously, we then obtain a reduction $\tilde{\rho}$ by composing ρ with the homomorphism $\mathrm{GL}_2(\mathcal{O}_V) \to \mathrm{GL}_2(k_V)$ given by reducing the matrix coefficients. However, this particular reduction is dependent on our choice of lattice Λ in **Proposition 6.1.2**. Since any two choices of lattice differ by an element of $\mathrm{GL}_2(V)$, this means that our reduced representation is unique up to conjugation by an element of this group. As representations over k_V, however, they need not be isomorphic.

To remedy this, we want to fix a choice of representation, and call this our residual representation $\tilde{\rho}$. To this end, we will require some results from general representation theory, the statements of which we quote from G. Wiese's lecture notes (**[Wie08], Theorems 2.1.8, 2.4.6.**).

Theorem 6.1.3. (**Jordan-Hölder**) *Let k be a field, A a k-algebra, and $\mathcal{V}$ an A-module which is a finite-dimensional k-vector space. Then $\mathcal{V}$ has a composition series, i.e., a descending chain of submodules*

$$\mathcal{V} = \mathcal{V}_0 \supsetneq \mathcal{V}_1 \supsetneq \mathcal{V}_2 \supsetneq \ldots \supsetneq \mathcal{V}_n = 0,$$

such that all composition factors $\mathcal{V}_i/\mathcal{V}_{i+1}$ are simple.

Theorem 6.1.4. (**Brauer-Nesbitt**) *Let k be a field, A a k-algebra, and $\mathcal{V}, \mathcal{W}$ two A-modules which are finite-dimensional k-vector spaces. If for all $a \in A$, the characteristic polynomials on $\mathcal{V}$ and $\mathcal{W}$ are equal, then $\mathcal{V}$ and $\mathcal{W}$ have the same composition factors.*

We adapt this to our setting. Let ρ_1 and ρ_2 be two different realisations of our original representation ρ over $\mathcal{O}_V$ (so that $\rho_1(\sigma) = g\rho_2(\sigma)g^{-1}$ for all $\sigma \in G_F$, for some fixed element $g \in \mathrm{GL}_2(V)$). Since the characteristic polynomial of a matrix is invariant under conjugation, the characteristic polynomials of ρ_1 and ρ_2 must be identical on G_F. Moreover, since ρ_1 and ρ_2 take values in $\mathrm{GL}_2(\mathcal{O}_V)$, the coefficients of this polynomial are integral, and so the corresponding reductions also have equal characteristic polynomials. Applying **Brauer-Nesbitt** with $k = k_V$, $A = k[G_F]$, and $\mathcal{V}$ and $\mathcal{W}$ the vector space k^2 with $k[G_F]$ action defined by the reductions of ρ_1 and ρ_2 respectively, we deduce that the composition series have identical composition factors.

To this end, we now define the residual representation $\tilde{\rho}$ of the representation ρ to be the *semisimplification* of *any* of our previously obtained reductions, by which we mean the direct sum of the associated composition factors, which thus frees us from our choice of lattice, leaving us with a well-defined (up to isomorphism) representation

$$\tilde{\rho} : G_F \to \mathrm{GL}_2(k_V).$$

From this argument it is clear that isomorphic representations must have isomorphic residual representations, and thus, given two representations ρ_1 and ρ_2 which we suspect are isomorphic, it is natural to first look at their residual representations. Since this reduces to a finite problem, establishing isomorphism of the residual representations should be a simpler task than establishing isomorphism of the original representations. In fact, the methods we shall describe later for comparing the full representations will assume that their residual representations are isomorphic, so it is necessary for our purposes to develop tools for comparing these reductions.

Since this will result in a computational task, it is in our best interests to find as small a field as possible over which to define our residual representations. That is, given a representation $\rho : G_F \to \mathrm{GL}_2(V)$, for some finite extension V of $\mathbb{Q}_\ell$, we wish to find the smallest subfield k of the residue field k_V for which $\mathrm{GL}_2(k)$ contains the image of the reduction $\tilde{\rho}$.

In fact, we shall show that the residual representation may be defined over the field k_ρ, the subfield of k_V generated over $\mathbb{F}_\ell$ by the coefficients of the characteristic polynomials of $\tilde{\rho}(\mathrm{Frob}_v)$, for all finite places v of F. In particular, if the trace and determinant of our representation ρ are integer-valued, then $\tilde{\rho}$ is defined over $\mathbb{F}_\ell$.

To show this, we begin with a variant of a standard result from cohomological algebra. Given two groups G and X, with an action of G on X, we define the *first cohomology set* $H^1(G;X)$ to be the set of *cocycles* $\{\gamma : G \to X,\ \sigma \mapsto \gamma_\sigma\}$ satisfying $\gamma_{\sigma\tau} = \gamma_\sigma \cdot \sigma(\gamma_\tau)$ for all $\sigma, \tau \in G$, modulo the relation $\sim$, where $\gamma \sim \hat{\gamma}$ if, and only if, $\hat{\gamma}_\sigma = x \cdot \gamma_\sigma \cdot \sigma(x)^{-1}$ for all $\sigma \in G$, for some $x \in X$.

Theorem 6.1.5. (**Hilbert's Theorem 90**) *Let L/K be a finite Galois extension, and let $G = \mathrm{Gal}(L/K)$. Then $H^1(G, \mathrm{GL}_n(L))$ is trivial.*

We shall make use of the following result. While it is no doubt well-known to experts, we were unable to find a reference, and so we provide a full proof.

Proposition 6.1.6. *Let $\rho : G_F \to \mathrm{GL}_2(V)$ be a Galois representation, with V a finite extension of $\mathbb{Q}_\ell$, and let $\tilde{\rho} : G_F \to \mathrm{GL}_2(k_V)$ be its residual representation. Then $\tilde{\rho}$ may be realised over the subfield k_ρ of k_V generated over $\mathbb{F}_\ell$ by the coefficients of the characteristic polynomials of $\tilde{\rho}(\mathrm{Frob}_v)$, for all finite places v of F, in the sense that we may conjugate $\tilde{\rho}$ by some element of $\mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$ so that its image lies in $\mathrm{GL}_2(k_\rho)$.*

Proof. The group $\mathrm{Gal}(k_V/k_\rho)$ is cyclic, generated by the Frobenius element $\sigma : x \mapsto x^{\ell^{[k_\rho:\mathbb{F}_\ell]}}$. Since by definition σ fixes k_ρ, the representations $\tilde{\rho}$ and $\sigma \circ \tilde{\rho}$ have the same characteristic polynomial. Since $\tilde{\rho}$ (and thus $\sigma \circ \tilde{\rho}$) are semisimple, Brauer-Nesbitt implies that they must be isomorphic, and so there exists some element $s \in \mathrm{GL}_2(k_V)$ such that $\sigma(\tilde{\rho}(g)) = s^{-1}\tilde{\rho}(g)s$ for all $g \in G_F$.

Now, let $\pi_s = \mathrm{Norm}_{k_V/k_\rho}(s) = \prod_{i=1}^{[k_V:k_\rho]} \sigma^i(s)$. Since $\pi_s \in \mathrm{GL}_2(k_\rho)$, it must have finite order, r, say. Let k_r denote a field extension of k_V of degree r. Then $\mathrm{Norm}_{k_r/k_V}(\pi_s) = \pi_s^r = \mathrm{Id}$, and thus $\mathrm{Norm}_{k_r/k_\rho}(s) = \mathrm{Norm}_{k_r/k_V}(\pi_s) = \mathrm{Id}$.

Let $G = \mathrm{Gal}(k_r/k_\rho)$, and let τ be the generator of G, so that in particular $\tau|_{k_V} = \sigma$. Then the map

$$\gamma : G \to \mathrm{GL}_2(k_r);\ \tau^m \mapsto \gamma_{\tau^m} := \prod_{i=0}^{m-1} \tau^i(s)$$

is a G-cocycle, which can easily be deduced from the definition and the fact that $\gamma_{\tau^{|G|}} = \mathrm{Norm}_{k_r/k_\rho}(s) = \mathrm{Id}$.

By Hilbert's Theorem 90, $H^1(G, \mathrm{GL}_2(k_r))$ is trivial, so in particular (since $\gamma_\tau = s$) there exists some $t \in \mathrm{GL}_2(k_r)$ such that $ts\tau(t)^{-1} = \mathrm{Id}$, i.e., $s = t^{-1}\tau(t)$.

Embedding $\mathrm{GL}_2(k_V)$ into $\mathrm{GL}_2(k_r)$, we may view $\tilde{\rho}$ as a representation $\tilde{\rho} : G_F \to \mathrm{GL}_2(k_r)$, which is fixed by $\mathrm{Gal}(k_r/k_V)$. In particular,

$$\tau \circ \tilde{\rho} = \tilde{\rho}^{\tau|_{k_V}} = \sigma \circ \tilde{\rho}.$$

Then for each $g \in G_F$,

$$\tau(t\tilde{\rho}(g)t^{-1}) = \tau(t)\sigma(\tilde{\rho}(g))\tau(t)^{-1} = \tau(t)s^{-1}\tilde{\rho}(g)s\tau(t)^{-1} = t\tilde{\rho}(g)t^{-1},$$

and so the image of $t\tilde{\rho}t^{-1}$ is contained in $\mathrm{GL}_2(k_\rho)$, as required. □

In particular:

Corollary 6.1.7. *Let $\rho : G_F \to \mathrm{GL}_2(V)$ be a Galois representation, with V a finite extension of $\mathbb{Q}_\ell$, and let $\tilde{\rho} : G_F \to \mathrm{GL}_2(k_V)$ be its residual representation. If the coefficients of the characteristic polynomial of $\rho(\mathrm{Frob}_v)$ are rational for all finite places v of F, then we may realise $\tilde{\rho}$ over the field $\mathbb{F}_\ell$.*

6.2 Sources of Galois Representations

In this section we will provide a brief recap of the particular Galois representations with which we will be concerned, namely those arising from elliptic curves, and those arising from automorphic forms.

The Galois representation attached to an elliptic curve E over a number field F is constructed in the same manner as for rational elliptic curves (as in **Section 2.4**), namely by considering the action of G_F on the ℓ-adic Tate module. **Theorem 2.4.3** extends naturally to elliptic curves defined over number fields, and as a consequence we have the following result (see **[Wie08], Theorem 1.3.3**):

Theorem 6.2.1. *Let E be an elliptic curve over F, with conductor $\mathfrak{n}$, and let ℓ be a rational prime. Then the above action of G_F on Ta_ℓ defines an ℓ-adic Galois representation*

$$\rho_E : G_F \to \mathrm{GL}_2(\mathbb{Q}_\ell),$$

which is unramified at all finite places not dividing $\ell\mathfrak{n}$. At each such unramified place $\mathfrak{p}$, the characteristic polynomial of $\mathrm{Frob}_\mathfrak{p}$ is given by

$$\Phi_\mathfrak{p}(X) = X^2 - a_\mathfrak{p} X + \mathrm{Norm}_{F/\mathbb{Q}}(\mathfrak{p}),$$

where

$$a_\mathfrak{p} = \mathrm{Norm}_{F/\mathbb{Q}}(\mathfrak{p}) - |\widetilde{E}(\mathcal{O}_F/\mathfrak{p})| + 1,$$

where $\widetilde{E}(\mathcal{O}_F/\mathfrak{p})$ denotes the reduction of the curve E at the prime $\mathfrak{p} \subseteq \mathcal{O}_F$. Moreover, the determinant of ρ_E is given by the ℓ-adic cyclotomic character of F.

The residual representation $\widetilde{\rho_E}$ is straightforward to describe, it is the semisimplification of the representation induced by the action of G_F on the set of ℓ-torsion points $E(\overline{F})[\ell]$. In particular, if $\ell = 2$, then we can determine the image of $\widetilde{\rho}$, from the Weierstrass equation

$$E : y^2 = x^3 + ax + b.$$

Since $\mathrm{GL}_2(\mathbb{F}_2) \simeq S_3$, the image of $\widetilde{\rho_E}$ must be a subgroup of S_3. In fact, it must be either S_3 itself, the cyclic group C_3 or the trivial group $\{\mathrm{Id}\}$. Indeed, it is not hard to see that any representation with S_3- or C_3-image is irreducible, and thus unchanged by semisimplification. On the other hand, a representation with C_2-image is *not* irreducible (as $\mathbb{F}_2^2$ contains a line invariant under each subgroup of $\mathrm{GL}_2(\mathbb{F}_2)$ of order 2) and so has trivial image after semisimplification. To determine which image our residual representation has, it suffices to compute the splitting field of the cubic $x^3 + ax + b$, as the field $F(E[2])$ generated by the coefficients of the 2-torsion points of E is isomorphic to this field.

On the automorphic side, we use the representation presented in **Section 3.5**, which we recall below:

Theorem 3.5.1. *Let F be a CM field, and let π be a cuspidal automorphic representation of $\mathrm{Res}_{F/\mathbb{Q}}(\mathrm{GL}_2)$ of cohomological type, with trivial central character, and fix a prime ℓ. Then there exists an ℓ-adic Galois representation*

$$\rho_\pi : \mathrm{Gal}(\overline{F}/F) \to \mathrm{GL}_2(\overline{\mathbb{Q}}_\ell)$$

such that, for each place v of F not dividing ℓ, we have the local-to-global compatibility statement, up to semisimplification:

$$\mathrm{WD}(\rho_{\pi,v})^{ss} \simeq \mathscr{L}_v(\pi_v \otimes |\det|_v^{-\frac{1}{2}})^{ss}.$$

Furthermore, if π_v is not a twist of Steinberg (e.g., is an unramified principal series) then we have the full local-to-global compatibility statement, up to Frobenius semisimplification:

$$\mathrm{WD}(\rho_{\pi,v})_{\mathrm{Frob}} \simeq \mathscr{L}_v(\pi_v \otimes |\det|_v^{-\frac{1}{2}}).$$

In particular, we use the automorphic representation π corresponding to a cuspidal automorphic form of level $K_0(\mathfrak{n})$ attached to one of the cuspidal Hecke eigenclasses found in **Section 5.3**. In particular, we recall the following properties of ρ_π from **Section 3.5**:

- ρ_π is unramified at all primes not dividing $\ell\mathfrak{n}$;
- The determinant of ρ_π is equal to the ℓ-adic cyclotomic character of F;
- The traces $\rho_\pi(\mathrm{Frob}_v)$ of Frobenius elements at unramified primes are given by the eigenvalues of the Hecke operators T_v acting on the corresponding Hecke eigenclass.
- Since the eigenclasses we are interested in have *rational* eigenvalues, the residual representation $\widetilde{\rho_\pi}$ takes values in $\mathrm{GL}_2(\mathbb{F}_\ell)$ by **Proposition 6.1.6**.

We shall call an elliptic curve E defined over F *modular* if, for some prime ℓ, the representation ρ_E is equivalent to the representation ρ_π for some π, up to semisimplification (due to the compatibility of families of such representations, equivalence of ρ_E and ρ_ℓ for some prime ℓ implies equivalence for all but finitely many primes ℓ).

6.3 Comparing Residual Representations

Suppose now that we have 2-adic representations ρ_E and ρ_π, associated to an elliptic curve and an automorphic representation respectively, and we wish to check whether or not they are isomorphic.

We shall follow the spirit of [**DGP10**]. The first step we shall take is to determine whether or not the residual representations $\widetilde{\rho_E}$ and $\widetilde{\rho_\pi}$ are isomorphic, which we shall do by investigating the fields cut out by their respective kernels. More precisely, let L_E denote the fixed field $\overline{F}^{\ker(\widetilde{\rho_E})}$, and L_π the fixed field $\overline{F}^{\ker(\widetilde{\rho_\pi})}$, so that $\mathrm{Gal}(L_E/F) \simeq G_F/\ker(\widetilde{\rho_E}) \simeq \mathrm{Im}(\rho_E)$, and $\mathrm{Gal}(L_\pi/F) \simeq G_F/\ker(\widetilde{\rho_\pi}) \simeq \mathrm{Im}(\rho_\pi)$. Since the coefficients of the characteristic polynomials of each representation are rational, the residual representations can be assumed to take values in $\mathrm{GL}_2(\mathbb{F}_2)$, and thus their images are isomorphic to subgroups of S_3. Now, elements of $\mathrm{GL}_2(\mathbb{F}_2)$ of the same order share the same characteristic polynomial so, applying Brauer-Nesbitt, we see that if the images of the residual representations are isomorphic then in fact $\widetilde{\rho_E} \simeq \widetilde{\rho_\pi}$ as representations. Thus our task reduces to determining whether or not the fixed fields L_E and L_π are isomorphic, for which we can use class field theory, following the treatment established in [**DGP10**].

We begin by establishing an isomorphism between $\mathrm{GL}_2(\mathbb{F}_2)$ and S_3, which we shall use throughout the remaining discussion. This isomorphism is induced by the action of $\mathrm{GL}_2(\mathbb{F}_2)$ on the three elements of $\mathbb{P}^1(\mathbb{F}_2)$, and can be defined by the mapping

$$(12) \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \ (13) \mapsto \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}.$$

From the statements of the previous section, we are considering representations unramified outside of those places which divide the rational prime 2 and the conductor of the elliptic curve E (since we restrict our attention to F a CM field, all infinite places are unramified). Consequently, the fields L_E and L_π are also unramified outside of these primes (by definition, if a representation ρ is unramified at $\mathfrak{p}$, then the absolute inertia group $I_\mathfrak{p} \subset G_F$ lies in $\ker(\rho)$. If F_ρ denotes the fixed field $\overline{F}^{\ker(\rho)}$, then for any prime $\mathfrak{q} \subset \mathcal{O}_{F_\rho}$ above $\mathfrak{p}$ the elements of the inertia group $I_{\mathfrak{q}/\mathfrak{p}} \subset \mathrm{Gal}(F_\rho/F)$ lift to elements of the absolute inertia group, and thus act trivially on F_ρ, so $\mathfrak{p}$ has trivial inertia in F_ρ, and thus is unramified).

Our aim is to establish isomorphism of the fields L_E and L_π, which we do by building up these fields by abelian extensions of F, leading us to consider ideas from class field theory. Recall that, for an ideal $\mathfrak{m}$ in a number field K (known as a *modulus*), the *ray class group* $Cl(\mathcal{O}_K, \mathfrak{m})$ is defined to be the quotient group $I^{\mathfrak{m}}/P^{\mathfrak{m}}$, where $I^{\mathfrak{m}}$ denotes the group of fractional ideals of K coprime to $\mathfrak{m}$, and $P^{\mathfrak{m}}$ is the group of principal ideals of K generated by elements which are congruent to 1 modulo $\mathfrak{m}$ (while the notion of ray class groups can be extended to include behaviour at infinite places, we shall not require such a generalization).

The ray class group $Cl(\mathcal{O}_K, \mathfrak{m})$ is a finite abelian group, and it is known that there exists an abelian extension $K(\mathfrak{m})/K$, known as a *ray class field*, which is unramified away from the primes dividing $\mathfrak{m}$, and whose Galois group is isomorphic to $Cl(\mathcal{O}_K, \mathfrak{m})$. This isomorphism is established via the *Artin map* $\mathrm{Art}_{K(\mathfrak{m})/K}$, which is defined as follows: any element of $Cl(\mathcal{O}_K, \mathfrak{m})$ can be defined as the image of a product of integral powers of prime ideals of K, not dividing $\mathfrak{m}$. The Artin map sends the image of such a prime $\mathfrak{p}$ to the Frobenius element $\mathrm{Frob}_{K(\mathfrak{m})/K}(\mathfrak{p})$ in $\mathrm{Gal}(K(\mathfrak{m})/K)$, and is extended to the entire ray class group multiplicatively. Moreover, the Artin map establishes a correspondence between the subgroups of $Cl(\mathcal{O}_K, \mathfrak{m})$ and subextensions of $K(\mathfrak{m})/K$.

The following result states that, if K is a CM field, then every *cyclic* Galois extension of K of prime degree appears as a subextension of some $K(\mathfrak{m})/K$, for a prescribed choice of modulus $\mathfrak{m}$:

Theorem 6.3.1. *Let K be a CM field, and let L/K be an abelian Galois extension of prime degree p, unramified away from the finite set of primes $S = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$. Denote by $\mathfrak{m}$ the modulus*

$$\mathfrak{m} = \prod_{\mathfrak{p} \in S} \mathfrak{p}^{e(\mathfrak{p})},$$

where

$$e(\mathfrak{p}) = \begin{cases} 1; & \text{if } \mathfrak{p} \nmid p, \\ \lfloor \frac{pe(\mathfrak{p}/p)}{p-1} \rfloor + 1; & \text{if } \mathfrak{p} | p. \end{cases}$$

Then $\mathrm{Gal}(L/K)$ *is isomorphic to a subgroup of* $Cl(\mathcal{O}_K, \mathfrak{m})$.

Proof. See **[Coh00], Propositions 3.3.21** and **3.3.22**. □

Every cyclic order p subgroup of $Cl(\mathcal{O}_K, \mathfrak{m})$ defines a character χ of order p, and vice-versa. Thus we can identify degree p extensions L/K with characters of ray class groups, assigning to each such extension the character defined by the Galois group $\mathrm{Gal}(L/K)$. For example, if L/K is a quadratic extension whose Galois group is a subgroup of $Cl(\mathcal{O}_K, \mathfrak{m})$, evaluation of the Artin map shows that the corresponding character χ_L is defined on the image of a prime $\mathfrak{p}$ of K not dividing $\mathfrak{m}$ by

$$\chi_L(\mathfrak{p}) = \begin{cases} 0; & \text{if } \mathfrak{p} \text{ splits in } L, \\ 1; & \text{if } \mathfrak{p} \text{ is inert in } L. \end{cases}$$

The following result (an extension of **[DGP10], Proposition 5.4**) will be used regularly:

Proposition 6.3.2. *Let K be a number field, $\mathfrak{m}$ an ideal of K, and define an $(\mathbb{Z}/p\mathbb{Z})$-basis $\{\psi_1, \dots, \psi_s, \chi_1, \dots, \chi_t\}$ of the order p characters of $Cl(\mathcal{O}_K, \mathfrak{m})$ for some prime p. Then there exists a set $\{\mathfrak{p}_1, \dots, \mathfrak{p}_r\}$ of prime ideals of $\mathcal{O}_K$ such that $\psi_i(\mathfrak{p}_j) = 0$ for all i, j, and the vectors $(\chi_1(\mathfrak{p}_j), \dots, \chi_t(\mathfrak{p}_j))$ for $j = 1, \dots, r$ span $(\mathbb{Z}/p\mathbb{Z})^t$.*

Moreover, for any set $\{\mathfrak{p}_1, \dots, \mathfrak{p}_r\}$ of prime ideals of $\mathcal{O}_K$ satisfying the above conditions, if χ is a non-trivial order p character of $Cl(\mathcal{O}_K, \mathfrak{m})$ not lying completely in the span of the characters $\{\psi_1, \dots, \psi_s\}$, then $\chi(\mathfrak{p}_j) \neq 0$ for some ideal $\mathfrak{p}_j$.

Proof. The first statement follows from Chebotarev's density theorem. Indeed, let $K(\mathfrak{m})$ be the ray class field of K with respect to $\mathfrak{m}$, so that $Cl(\mathcal{O}_K, \mathfrak{m})$ is isomorphic to $\mathrm{Gal}(K(\mathfrak{m})/K)$. In particular, the latter group is abelian, and thus Chebotarev's theorem implies that it is covered by Frobenius elements $\mathrm{Frob}_{K(\mathfrak{m})/K}(\mathfrak{p})$, for the primes $\mathfrak{p}$ of K which do not divide $\mathfrak{m}$. For each character χ_i, it is possible to find an element of $Cl(\mathcal{O}_K, \mathfrak{m})$ which has trivial image under all other order p characters, and the corresponding element of $\mathrm{Gal}(K(\mathfrak{m})/K)$ is therefore of the form $\mathrm{Frob}_{K(\mathfrak{m})/K}(\mathfrak{p}_i)$ for some prime $\mathfrak{p}_i$ of K – the set $\{\mathfrak{p}_1, \dots, \mathfrak{p}_r\}$ satisfies the required conditions.

For the second statement, we may write χ in the form

$$\chi = \psi + \sum_{i=1}^{t} \epsilon_i \chi_i,$$

for some $\epsilon_i \in \mathbb{Z}/n\mathbb{Z}$, not all zero, and where ψ lies in the span of the characters $\{\psi_1, \dots, \psi_s\}$. Suppose then that $\chi(\mathfrak{p}_j) = 0$ for all $1 \leq j \leq r$. Since $\chi(\mathfrak{p}_i) = 0$ for each $\mathfrak{p}_i$, it follows that

$$\begin{pmatrix} \chi_1(\mathfrak{p}_1) & \cdots & \chi_t(\mathfrak{p}_1) \\ \vdots & \ddots & \vdots \\ \chi_1(\mathfrak{p}_r) & \cdots & \chi_t(\mathfrak{p}_r) \end{pmatrix} \begin{pmatrix} \epsilon_1 \\ \vdots \\ \epsilon_t \end{pmatrix} = 0.$$

Since the matrix $(\chi_i(\mathfrak{p}_j))_{ij}$ has maximal rank, it follows that $\epsilon_i = 0$ for all i, and $\chi = \psi$, contradicting our assumption. □

We now proceed to compare the residual representations, which we shall do on a case-by-case basis, depending on the image of $\widetilde{\rho_E}$.

Case 1: $\mathrm{Im}(\widetilde{\rho_E}) \simeq \{\mathrm{Id}\}$.

If $\widetilde{\rho_E}$ has trivial image, then it suffices to establish that $\widetilde{\rho_\pi}$ does not have image isomorphic to either C_3 or S_3. Suppose then that $\mathrm{Im}(\widetilde{\rho_\pi}) = C_3$ or S_3. We begin by noting that if this is the case, then the fixed field $L_\pi = \overline{F}^{\ker(\widetilde{\rho_\pi})}$ contains a subfield F_π such that $[L_\pi : F_\pi] = 3$ (if $\mathrm{Im}(\widetilde{\rho_\pi}) = C_3$, then F_π is simply F itself, while if $\mathrm{Im}(\widetilde{\rho_\pi}) = S_3$ then F_π is a quadratic extension of F). Let $\mathfrak{n}$ denote the conductor of the elliptic curve E, and denote by $\mathfrak{m}$ the modulus

$$\mathfrak{m} = \prod_{\mathfrak{p}|2\mathfrak{n}} \mathfrak{p}^{e(\mathfrak{p})},$$

where

$$e(\mathfrak{p}) = \begin{cases} 1; & \text{if } \mathfrak{p} \nmid 2, \\ 2e(\mathfrak{p}/2) + 1; & \text{if } \mathfrak{p}|2. \end{cases}$$

By **Theorem 6.3.1**, any quadratic extension of F unramified away from the primes dividing $2\mathfrak{n}$ (and, consequently, the extension F_π) must correspond to a quadratic character of $Cl(\mathcal{O}_F, \mathfrak{m})$.

Now, for each such character, we construct the corresponding field F_π, and let $\mathfrak{m}_\pi$ denote the modulus

$$\mathfrak{m}_\pi = \prod_{\mathfrak{q}|2\mathfrak{n}\mathcal{O}_{F_\pi}} \mathfrak{q}^{e(\mathfrak{q})},$$

where

$$e(\mathfrak{q}) = \begin{cases} 1; & \text{if } \mathfrak{q} \nmid 3, \\ 3\lfloor \frac{e(\mathfrak{q}/3)}{2} \rfloor + 1; & \text{if } \mathfrak{q}|3. \end{cases}$$

Since L_π is a cubic extension of F_π, **Theorem 6.3.1** implies that it corresponds to a cubic character χ_π of $Cl(\mathcal{O}_{F_\pi}, \mathfrak{m}_\pi)$. Let $\{\chi_1, \ldots, \chi_t\}$ denote a $(\mathbb{Z}/3\mathbb{Z})$-basis of these characters, let $\{\mathfrak{q}_1, \ldots, \mathfrak{q}_s\}$ be a set of prime ideals in $\mathcal{O}_{F_\pi}$ not dividing $\mathfrak{m}_\pi$ such that the vectors $(\chi_1(\mathfrak{q}_i), \ldots, \chi_t(\mathfrak{q}_i))$ span $(\mathbb{Z}/3\mathbb{Z})^t$, and let $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}$ denote the set of prime ideals in $\mathcal{O}_F$ lying below the $\mathfrak{q}_i$.

By **Proposition 6.3.2**, since χ_π is assumed non-trivial, there must be some prime $\mathfrak{q}_i$ for which $\chi_\pi(\mathfrak{q}_i) \neq 0$. We claim that this means that $\widetilde{\rho_\pi}(\mathrm{Frob}_\mathfrak{p})$ must have odd trace, where $\mathfrak{p}$ lies below $\mathfrak{q}_i$. Indeed, if $\chi_\pi(\mathfrak{q}_i)$ is non-trivial then it must have order 3 in $\mathbb{Z}/3\mathbb{Z}$, whence the image of $\mathrm{Frob}_\mathfrak{p}$ must also have odd order in $\mathrm{GL}_2(\mathbb{F}_2) \simeq S_3$. By observation, the only such elements of $\mathrm{GL}_2(\mathbb{F}_2)$ are those with trace equal to 1.

Thus if the traces of $\rho_\pi(\mathrm{Frob}_{\mathfrak{p}_i})$ are even for each $\mathfrak{p}_i$ defined above, then $\widetilde{\rho_\pi}$ has trivial image, while if any of these traces are odd, the character χ_π is non-trivial and thus L_π is not isomorphic to L_E.

Case 2: $\mathrm{Im}(\widetilde{\rho_E}) \simeq C_3$.

In this case, there are two steps: we first prove that the residual representation $\widetilde{\rho_\pi}$ has image isomorphic to C_3, which we do by showing that its image is non-trivial, and contains no order 2 elements. We then prove that its image factors through the extension L_E, which we do by looking at all possible cubic extensions of F and showing that L_π can only correspond to the character associated to L_E.

We will need to consider both quadratic and cubic extensions of L and so, guided by **Theorem 6.3.1**, we let $\mathfrak{m}$ denote the modulus

$$\mathfrak{m} = \prod_{\mathfrak{p}|2\mathfrak{n}} \mathfrak{p}^{e(\mathfrak{p})},$$

where

$$e(\mathfrak{p}) = \begin{cases} 1; & \text{if } \mathfrak{p} \nmid 6, \\ 2e(\mathfrak{p}/2) + 1; & \text{if } \mathfrak{p}|2, \\ 3\lfloor \frac{e(\mathfrak{p}/3)}{2} \rfloor + 1; & \text{if } \mathfrak{p}|3, \end{cases}$$

where $\mathfrak{n}$ denotes the conductor of the elliptic curve E as before.

Now, if $\widetilde{\rho_\pi}$ contains an order 2 element in its image, then there must be some quadratic extension F_π of F contained in L_π, which therefore corresponds to a quadratic character of $Cl(\mathcal{O}_F, \mathfrak{m})$. Now, suppose $\mathfrak{p} \subset \mathcal{O}_F$ is a prime which is inert in F_π. Since $\mathrm{Im}(\widetilde{\rho_\pi}) \subseteq S_3$, $\widetilde{\rho_\pi}(\mathrm{Frob}_\mathfrak{p})$ must have order exactly 2, and in particular has trace equal to 0.

Let $\{\chi_1, \ldots, \chi_t\}$ be a $(\mathbb{Z}/2\mathbb{Z})$-basis for the quadratic characters of $Cl(\mathcal{O}_F, \mathfrak{m})$, and let $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}$ be a set of prime ideals of $\mathcal{O}_F$ not dividing $\mathfrak{m}$, such that the vectors $(\chi_1(\mathfrak{p}_i), \ldots, \chi_t(\mathfrak{p}_i))$ span $(\mathbb{Z}/2\mathbb{Z})^t$. By **Proposition 6.3.2**, for any quadratic extension K of F unramified away from the primes dividing $2\mathfrak{n}$, there must be some prime $\mathfrak{p}_i$ that is inert in K. Thus if $\mathrm{Tr}(\rho_\pi(\mathrm{Frob}_{\mathfrak{p}_i}))$ is odd for all primes $\mathfrak{p}_i$, $\widetilde{\rho_\pi}$ can contain no order 2 elements. In addition, since the identity matrix has even trace, this implies that $\widetilde{\rho_\pi}$ must have C_3-image.

Next, let ψ_E denote the cubic character associated to the cubic extension L_E, and extend it to a $(\mathbb{Z}/3\mathbb{Z})$-basis $\{\psi_E, \chi_1, \ldots, \chi_t\}$ of the cubic characters of $Cl(\mathcal{O}_F, \mathfrak{m})$. Compute a second set $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_s\}$ of prime ideals of $\mathcal{O}_F$, not dividing $\mathfrak{m}$, such that $\psi_E(\mathfrak{p}_i) = 0$ for all i and the vectors $(\chi_1(\mathfrak{p}_i), \ldots, \chi_t(\mathfrak{p}_i))$ span $(\mathbb{Z}/2\mathbb{Z})^t$.

Let ψ_π be the cubic character of $Cl(\mathcal{O}_F, \mathfrak{m})$ corresponding to L_π, and write

$$\psi_\pi = \epsilon\psi_E + \sum_{i=1}^{t} \epsilon_i \chi_i, \ \epsilon, \epsilon_i \in \mathbb{Z}/3\mathbb{Z}.$$

If $\psi_\pi = \epsilon\psi_E$, then $L_\pi \simeq L_E$, so suppose $\psi_\pi \neq \epsilon\psi_E$. By **Proposition 6.3.2**, we must have $\psi_\pi(\mathfrak{p}_i) \neq 0$ for some prime $\mathfrak{p}_i$. In particular, $\widetilde{\rho_\pi}(\mathrm{Frob}_{\mathfrak{p}_i})$ must have odd order in S_3, while $\widetilde{\rho_E}(\mathrm{Frob}_{\mathfrak{p}_i})$ has even order, or is the trivial element. Thus $\mathrm{Tr}(\widetilde{\rho_\pi}(\mathrm{Frob}_{\mathfrak{p}_i})) \neq \mathrm{Tr}(\widetilde{\rho_E}(\mathrm{Frob}_{\mathfrak{p}_i}))$.

We therefore evaluate the traces of $\widetilde{\rho_\pi}$ and $\widetilde{\rho_E}$ on the Frobenius elements at the primes $\mathfrak{p}_i$ above. If these all coincide, then we indeed have $L_\pi \simeq L_E$, and so $\widetilde{\rho_\pi} \simeq \widetilde{\rho_E}$. If any of these traces differ, the residual representations are non-isomorphic.

Case 3: $\mathrm{Im}(\widetilde{\rho_E}) \simeq S_3$.

This case is slightly more involved than the previous two. We begin by noting that the group S_3 contains a unique (up to inner isomorphism) subgroup of order 2, and thus it follows that F has a unique quadratic extension F_E contained in L_E. We wish to show that L_π can contain no quadratic extension of F *other than* F_E.

As before, let $\mathfrak{m}$ denote the modulus

$$\mathfrak{m} = \prod_{\mathfrak{p}|2\mathfrak{n}} \mathfrak{p}^{e(\mathfrak{p})},$$

where

$$e(\mathfrak{p}) = \begin{cases} 1; & \text{if } \mathfrak{p} \nmid 6, \\ 2e(\mathfrak{p}/2) + 1; & \text{if } \mathfrak{p}|2, \\ 3\lfloor \frac{e(\mathfrak{p}/3)}{2} \rfloor + 1; & \text{if } \mathfrak{p}|3, \end{cases}$$

where once again $\mathfrak{n}$ denotes the conductor of the elliptic curve E.

Let ψ_{F_E} denote the quadratic character of $Cl(\mathcal{O}_F, \mathfrak{m})$ corresponding to F_E. After evaluating the Artin map, it is clear that

$$\psi_{F_E}(\mathfrak{p}) = \begin{cases} 0; & \text{if } \mathfrak{p} \text{ splits in } F_E, \\ 1; & \text{if } \mathfrak{p} \text{ is inert in } F_E. \end{cases}$$

Now, extend ψ_{F_E} to a $(\mathbb{Z}/2\mathbb{Z})$-basis $\{\psi_{F_E}, \chi_1, \ldots, \chi_t\}$ of the quadratic characters of $Cl(\mathcal{O}_F, \mathfrak{m})$, and let $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}$ be a set of prime ideals in $\mathcal{O}_F$, not dividing $\mathfrak{m}$, such that $\psi_{F_E}(\mathfrak{p}_i) = 0$ and the vectors $(\chi_1(\mathfrak{p}_i), \ldots, \chi_t(\mathfrak{p}_i))$ span $(\mathbb{Z}/2\mathbb{Z})^t$. To ensure that $\psi_{F_E}(\mathfrak{p}_i) = 0$, we can restrict our attention to primes with inertial degree 3 on L_E; any such prime must necessarily split on F_E. For any such prime $\mathfrak{p}_i$, $\widetilde{\rho_E}(\mathrm{Frob}_{\mathfrak{p}_i})$ must have order 3 in $\mathrm{GL}_2(\mathbb{F}_2)$, and thus must have trace equal to 1.

Let χ be a quadratic character of $Cl(\mathcal{O}_F, \mathfrak{m})$ corresponding to a subfield of L_π, and write

$$\chi = \epsilon\psi_{F_E} + \sum_{i=1}^{t} \epsilon_i \chi_i, \ \epsilon, \epsilon_i \in \mathbb{Z}/2\mathbb{Z}.$$

If $\chi = \epsilon\psi_{F_E}$, then χ corresponds to either F itself (if $\epsilon = 0$) or F_E (if $\epsilon = 1$). If $\chi \neq \epsilon\psi_{F_E}$, then L_π contains a quadratic extension of F not isomorphic to F_E, and we wish to prove that this is not possible. By **Proposition 6.3.2**, we must have $\chi(\mathfrak{p}_i) \neq 0$ for some $\mathfrak{p}_i$, so in particular $\mathfrak{p}_i$ must have even inertial degree in L_π, and the image of $\widetilde{\rho_\pi}(\mathrm{Frob}_{\mathfrak{p}_i})$ must have even order, and hence has trace equal to 0. Thus if $\mathrm{Tr}(\rho_\pi(\mathrm{Frob}_{\mathfrak{p}_i}))$ is odd for all primes $\mathfrak{p}_i$ above, L_π can contain no quadratic extension of F other than F_E. If any of these traces are even, we can immediately deduce that the residual representations are non-isomorphic.

We now wish to eliminate the possibility that $\mathrm{Im}(\widetilde{\rho_\pi}) \simeq C_3$. If this were the case, let χ_π denote one of the cubic characters of $Cl(\mathcal{O}_F, \mathfrak{m})$ associated to L_π, and let $\{\chi_1, \ldots, \chi_t\}$ be a $(\mathbb{Z}/3\mathbb{Z})$-basis of the cubic characters of $Cl(\mathcal{O}_F, \mathfrak{m})$. By Chebotarev, we can choose a set $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}$ of prime ideals of $\mathcal{O}_F$ which either split completely in L_E or are inert in the quadratic extension F_E of F mentioned above, such that the vectors $(\chi_1(\mathfrak{p}_i), \ldots, \chi_t(\mathfrak{p}_i))$ span $(\mathbb{Z}/3\mathbb{Z})^t$. Note that for any such prime $\mathfrak{p}_i$, $\widetilde{\rho_E}(\mathrm{Frob}_{\mathfrak{p}_i})$ has order at most 2 in $\mathrm{GL}_2(\mathbb{F}_2)$, and thus has trace equal to 0.

Since χ_π is non-trivial, by **Proposition 6.3.2** we must have $\chi_\pi(\mathfrak{p}_i) \neq 0$ for some prime $\mathfrak{p}_i$. Thus $\chi_\pi(\mathfrak{p}_i)$ has order 3 in $\mathbb{Z}/3\mathbb{Z}$, and subsequently so too must $\widetilde{\rho_\pi}(\mathrm{Frob}_{\mathfrak{p}_i})$ in $\mathrm{Gal}(L_\pi/F)$. It follows that $\rho_\pi(\mathrm{Frob}_{\mathfrak{p}_i})$ must have odd trace, so if $\mathrm{Tr}(\rho_\pi(\mathrm{Frob}_{\mathfrak{p}_i}))$ is even for all primes $\mathfrak{p}_i$, we know that L_π cannot be a C_3-extension. Since we know that the image of $\widetilde{\rho_\pi}$ is isomorphic to a subgroup of S_3, it follows that it must be S_3 itself.

If the residual representations have not yet been shown to be non-isomorphic, then we know that L_π is an S_3-extension, containing the same quadratic extension F_E of F as L_E. We therefore wish to ascertain that the only possible cubic extension of F_E contained in L_π is L_E itself. Using **Theorem 6.3.1** once more, we consider the ray class group $Cl(\mathcal{O}_{F_E}, \mathfrak{m}_E)$, where

$$\mathfrak{m}_E = \prod_{\mathfrak{q}|2\mathfrak{n}\mathcal{O}_{F_E}} \mathfrak{q}^{e(\mathfrak{q})},$$

where

$$e(\mathfrak{q}) = \begin{cases} 1; & \text{if } \mathfrak{q} \nmid 3, \\ 3\lfloor \frac{e(\mathfrak{q}/3)}{2} \rfloor + 1; & \text{if } \mathfrak{q}|3, \end{cases}$$

.

Denote by ψ_E one of the cubic characters of $Cl(\mathcal{O}_{F_E}, \mathfrak{m}_E)$ associated to the extension L_E, and extend it to a $(\mathbb{Z}/3\mathbb{Z})$-basis $\{\psi_E, \chi_1, \ldots, \chi_t\}$ of the cubic characters of $Cl(\mathcal{O}_{F_E}, \mathfrak{m}_E)$. Compute a set $\{\mathfrak{q}_1, \ldots, \mathfrak{q}_s\}$ of prime ideals of $\mathcal{O}_{F_E}$ such that $\psi_E(\mathfrak{q}_i) = 0$ for each i, and the vectors $(\chi_1(\mathfrak{q}_i), \ldots, \chi_t(\mathfrak{q}_i))$ span $(\mathbb{Z}/3\mathbb{Z})^t$, and let $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}$ denote the set of prime ideals of $\mathcal{O}_F$ lying beneath the $\mathfrak{q}_i$. Now, since $\psi_E(\mathfrak{q}_i) = 0$, each prime $\mathfrak{q}_i$ must split completely in L_E, so every prime $\mathfrak{p}_i$ has inertial degree at most 2 in L_E. Consequently, $\widetilde{\rho_E}(\mathfrak{p})$ has order at most 2 in $\mathrm{GL}_2(\mathbb{F}_2)$, and thus $\rho_E(\mathfrak{p})$ has even trace.

Let ψ_π be the cubic character of $Cl(\mathcal{O}_{F_E}, \mathfrak{m}_E)$ corresponding to L_π, and write

$$\psi_\pi = \epsilon\psi_E + \sum_{i=1}^{t} \epsilon_i \chi_i.\ \epsilon, \epsilon_i \in \mathbb{Z}/3\mathbb{Z}.$$

Now, if $\psi_\pi = \epsilon\psi_E$, then ψ_π and ψ_E must both correspond to the same extension, and thus $L_\pi \simeq L_E$, so suppose that this is not the case. Then by **Proposition 6.3.2** $\psi_\pi(\mathfrak{q}_i) \neq 0$ for some $\mathfrak{q}_i$, and so $\mathfrak{q}_i$ must have inertial degree 3 in L_π, and subsequently so too must the prime $\mathfrak{p}_i$ beneath $\mathfrak{q}_i$. Thus $\widetilde{\rho_\pi}(\mathrm{Frob}_{\mathfrak{p}_i})$ must have order 3 in $\mathrm{GL}_2(\mathbb{F}_2)$, and so $\rho_\pi(\mathrm{Frob}_{\mathfrak{p}_i})$ has odd trace. Thus if $\mathrm{Tr}(\rho_\pi(\mathrm{Frob}_{\mathfrak{p}_i}))$ is even for all primes $\mathfrak{p}_i$, we can conclude that the residual representations $\widetilde{\rho_\pi}$ and $\widetilde{\rho_E}$ are isomorphic.

6.4 Livné's Criterion

Having shown how to decide isomorphism of the residual representations, we are now in a position to determine whether or not the full representations ρ_E and ρ_π are isomorphic, up to semisimplification. We shall use one of two different approaches, depending on what the images of the residual representations look like. The first of these, using a result due to Livné, may be used in the cases where the residual images are either trivial or cyclic.

We begin by stating the main result:

Theorem 6.4.1. *Let F be a number field, and V_λ a finite extension of $\mathbb{Q}_2$ with ring of integers $\mathcal{O}_\lambda$ and maximal ideal λ. Let*

$$\rho_1, \rho_2 : G_F \to \mathrm{GL}_2(V_\lambda)$$

be two continuous representations unramified outside a finite set S of places of F, such that

$$\mathrm{Tr}(\widetilde{\rho_1}) \equiv \mathrm{Tr}(\widetilde{\rho_2}) \equiv 0 \pmod{\lambda}, \text{ and } \det(\widetilde{\rho_1}) \equiv \det(\widetilde{\rho_2}) \equiv 1 \pmod{\lambda}.$$

Let $F_{2,S}$ denote the compositum of all quadratic extensions of F unramified outside S, and suppose there exists a set of prime ideals T of $\mathcal{O}_F$, disjoint from S, such that:

(i) $\{\mathrm{Frob}_\mathfrak{p};\ \mathfrak{p} \in T\}$ *surjects onto* $\mathrm{Gal}(F_{2,S}/F)$*; and*

(ii) *The characteristic polynomials of ρ_1 and ρ_2 at the Frobenius elements $\{\mathrm{Frob}_\mathfrak{p};\ \mathfrak{p} \in T\}$ are equal.*

Then ρ_1 and ρ_2 have isomorphic semisimplifications.

Proof. See **[Liv87]** (our statement of the theorem comes from **[Chê08], Theorem 5.4.9**). □

If both $\widetilde{\rho_\pi}$ and $\widetilde{\rho_E}$ have trivial image, we may use **Theorem 6.4.1** immediately. The Galois group $\mathrm{Gal}(F_{2,S}/F)$ may be identified with the subgroup of quadratic characters of $Cl(\mathcal{O}_F, \mathfrak{m})$ from **Section 6.3, Case 1**, where S is the set of prime ideals of $\mathcal{O}_F$ dividing $2\mathfrak{n}$.

Let $\{\chi_1, \ldots, \chi_t\}$ be a $(\mathbb{Z}/2\mathbb{Z})$-basis of the quadratic characters of $Cl(\mathcal{O}_F, \mathfrak{m})$. Then any set $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}$ of primes for which the vectors $(\chi_1(\mathfrak{p}_i), \ldots, \chi_t(\mathfrak{p}_i))$ *cover* $(\mathbb{Z}/2\mathbb{Z})^t \setminus \{0\}$ satisfies the criterion. Given such a set of primes, we check for equality of the characteristic polynomials of $\rho_\pi(\mathrm{Frob}_{\mathfrak{p}_i})$ and $\rho_E(\mathrm{Frob}_{\mathfrak{p}_i})$ for all $\mathfrak{p}_i$. If we have equality for each such prime, the representations are equal.

If both $\widetilde{\rho_\pi}$ and $\widetilde{\rho_E}$ have image isomorphic to C_3, the matter is slightly more complicated, as the traces of the residual representations are no longer identically zero. However, we make the following observation: if we define the fixed field $L = \overline{F}^{\ker(\widetilde{\rho})}$ (where $\widetilde{\rho}$ is isomorphic to both our residual representations), then L/F is a cubic Galois extension, and G_L is a normal subgroup of G_F. If ρ'_E and ρ'_π denote the restrictions of our original representations to G_L, then the corresponding residual representations are trivial, and thus we can use **Theorem 6.4.1** to determine isomorphism of ρ'_E and ρ'_π (as usual, up to semisimplification).

If we impose the additional restriction that the base change of the elliptic curve E to the field L does not possess complex multiplication, then the representation ρ'_E (and thus also ρ'_π) is in fact irreducible. By Schur's lemma, $\mathrm{Hom}_{G_L}(\rho'_E, \rho'_\pi)$ contains a copy of V_λ on which G_L acts trivially, and thus $\mathrm{Hom}_{G_L}(\mathbf{1}, (\rho_E \otimes \rho_\pi^\vee)|_{G_L})$ is non-trivial (where $\mathbf{1}$ denotes the trivial representation). Frobenius reciprocity implies that the latter group is isomorphic to $\mathrm{Hom}_{G_F}(\mathrm{Ind}_{G_L}^{G_F}(\mathbf{1}), \rho_E \otimes \rho_\pi^\vee)$, which decomposes as a direct sum

$$\mathrm{Hom}_{G_F}(\mathrm{Ind}_{G_L}^{G_F}(\mathbf{1}), \rho_E \otimes \rho_\pi^\vee) \simeq \bigoplus_{\chi|_{G_L}=\mathbf{1}} \mathrm{Hom}_{G_F}(\rho_\pi \otimes \chi, \rho_E).$$

Invoking Schur's lemma once more, we observe that one of these summands must be non-trivial, and that $\rho_E \simeq \rho_\pi \otimes \chi$ for some character χ of G_F whose restriction to G_L is non-trivial. One can then determine whether this character is trivial, by finding a prime $\mathfrak{p}$ of F which is inert in L. In this case, $\mathrm{Frob}_\mathfrak{p}$ is non-trivial, and so χ is completely determined by the value it takes on this Frobenius element. In particular, if $\mathrm{Tr}(\rho_\pi(\mathrm{Frob}_\mathfrak{p})) = \mathrm{Tr}(\rho_E(\mathrm{Frob}_\mathfrak{p}))$, then $\chi(\mathrm{Frob}_\mathfrak{p}) = 1$, χ is trivial, and ρ_π and ρ_E have isomorphic semisimplifications, as required.

6.5 The Faltings-Serre Method

This section concerns the remaining case: if the residual representations $\widetilde{\rho_E}$ and $\widetilde{\rho_\pi}$ are isomorphic and both have full image in $\mathrm{GL}_2(\mathbb{F}_2)$, how can we determine whether the full representations ρ_E and ρ_π are also isomorphic (as usual, up to semisimplification)?

The Faltings-Serre method gives us a means to answer this. We follow the spirit of **[DGP10], Section 4.1**. Let F be a number field, and suppose that

$$\rho_1, \rho_2 : G_F \to \mathrm{GL}_2(\mathbb{Z}_2)$$

are two representations such that:

- ρ_1 and ρ_2 have the same determinant;
- ρ_1 and ρ_2 are unramified outside a finite set S of primes of F;
- The residual representations $\widetilde{\rho_1}$ and $\widetilde{\rho_2}$ are absolutely irreducible and isomorphic.

If ρ_1 and ρ_2 were not isomorphic, then by Brauer-Nesbitt there must exist some prime $\mathfrak{p}$ in F such that $\mathrm{Tr}(\rho_1(\mathrm{Frob}_\mathfrak{p})) \neq \mathrm{Tr}(\rho_2(\mathrm{Frob}_\mathfrak{p}))$. The Faltings-Serre method will allow us to construct a *finite* set of candidate prime ideals that will contain such a prime, should it exist.

We will apply this to our representations ρ_E and ρ_π. While it is clear that ρ_E is defined over $\mathbb{Z}_2$, we need to show that ρ_π is. For this, we use the following result (adapted from **[Car94], Theorem 2**):

Theorem 6.5.1. *Let V, W be finite extensions of $\mathbb{Q}_2$, with rings of integers $\mathcal{O}_V$ and $\mathcal{O}_W$, and suppose that $W \supset V$. If*

$$\rho_W : G \to \mathrm{GL}_2(W)$$

is a representation of some group G such that the traces $\mathrm{Tr}(\rho_W(g))$ lie in V for all $g \in G$, and the residual representation $\widetilde{\rho_W}$ is absolutely irreducible, then ρ_W is equivalent to a representation

$$\rho_V : G \to \mathrm{GL}_2(V).$$

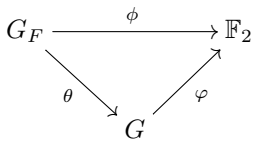
Since the two-dimensional irreducible representation of S_3 is in fact absolutely irreducible over any field of characteristic 2 (see, for example, **[LP10], Example 1.3.5**), we can apply **Theorem 6.5.1** to ρ_π, and deduce that it is indeed equivalent to a representation defined over $\mathbb{Z}_2$.

We now return to our original situation. Since the traces of ρ_1 and ρ_2 are non-equal, there must be a maximal $r \in \mathbb{N}$ for which $\mathrm{Tr}(\rho_1) \equiv \mathrm{Tr}(\rho_2) \pmod{2^r}$ (if this were not so, then the traces, being defined over $\mathbb{Z}_2$, would necessarily be equal). Thus we can define a non-trivial map $\phi : G_F \to \mathbb{F}_2$ by

$$\phi(\sigma) = \frac{\mathrm{Tr}(\rho_1(\sigma)) - \mathrm{Tr}(\rho_2(\sigma))}{2^r} \pmod 2.$$

Now, $\phi(\mathrm{Frob}_{\mathfrak{p}}) = 1$ precisely when the traces of $\rho_i(\mathrm{Frob}_{\mathfrak{p}})$ differ, so we wish to find some prime $\mathfrak{p}$ such that $\mathrm{Frob}_{\mathfrak{p}}$ has non-trivial image under ϕ. The difficulty lies in the fact that the group G_F is too large for us to approach directly, so we would like to factor the map ϕ through some *finite* group G.

More precisely, we wish to find a factorisation $\phi = \varphi \circ \theta$, with θ a group homomorphism, such that the following diagram commutes:



Thus ϕ is non-trivial if, and only if, φ is non-trivial on $\mathrm{Im}(\theta)$, so we may restrict our attention to the finite group G.

Now, we can associate a field F_θ to the map θ by defining $F_\theta := \overline{F}^{\ker(\theta)}$, in which case F_θ/F is a Galois extension, with

$$\mathrm{Gal}(F_\theta/F) \simeq G_F/\ker(\theta) \simeq \mathrm{Im}(\theta).$$

If we can choose θ appropriately, so as to control ramification in F_θ, then, since F_θ must be a Galois extension of F with a finite number of potential Galois groups, we can hope to use class field theory to determine a finite list of candidates for F_θ. For each possible field, we can determine which elements of $\mathrm{Gal}(F_\theta/F)$ can have non-trivial image under φ. If, for each possible F_θ, we can then find a set of prime ideals $\mathfrak{p} \in \mathcal{O}_F$ such that the images $\theta(\mathrm{Frob}_{\mathfrak{p}})$ cover this set, then $\phi(\mathrm{Frob}_{\mathfrak{p}})$ should be non-trivial for at least one of them. The union of all these primes thus gives us our desired set of candidates.

We now describe how we do this in practice. Since the residual representations $\widetilde{\rho_1}$ and $\widetilde{\rho_2}$ are isomorphic, we shall henceforth assume that $\widetilde{\rho_1} = \widetilde{\rho_2} = \widetilde{\rho}$, say. We note the following result (see **[Car94], Theorem 1**):

Theorem 6.5.2. *Let A be a local ring, R an A-algebra, and let ρ, ψ be two representations of R of the same dimension n. Suppose that the residual representation $\widetilde{\rho}$ is absolutely irreducible, and that ρ and ψ have the same trace. Then ρ and ψ are equivalent.*

We apply this as follows: let A be the local ring $A = \mathbb{Z}_2/2^r\mathbb{Z}_2$, and let ρ and ψ be the compositions of ρ_1 and ρ_2 with the projection $\mathbb{Z}_2 \to \mathbb{Z}_2/2^r\mathbb{Z}_2$. In particular, the residual representations $\widetilde{\rho}$ and $\widetilde{\psi}$ are equivalent to $\widetilde{\rho_1}$ and $\widetilde{\rho_2}$. Since we have assumed the representations to be absolutely irreducible, and that the traces of ρ_1 and ρ_2 are equal modulo 2^r, it follows that the representations ρ_1 and ρ_2 are in fact isomorphic modulo 2^r.

We can therefore define a map $\mu : G_F \to M_2(\mathbb{F}_2)$ by setting

$$\rho_1(\sigma) = (1 + 2^r\mu(\sigma))\rho_2(\sigma),$$

so that

$$\phi(\sigma) \equiv \mathrm{Tr}(\widetilde{\rho}(\sigma)\mu(\sigma)) \pmod 2.$$

Note that

$$\rho_1(\sigma\tau) = (1 + 2^r\mu(\sigma\tau))\rho_2(\sigma\tau),$$

but also

$$\rho_1(\sigma\tau) = \rho_1(\sigma)\rho_1(\tau) = (1 + 2^r\mu(\sigma))\rho_2(\sigma)(1 + 2^r\mu(\tau))\rho_2(\tau).$$

Equating the two, we observe that

$$\mu(\sigma\tau) \equiv \mu(\sigma) + \widetilde{\rho}(\sigma)\mu(\tau)\widetilde{\rho}(\sigma)^{-1} \pmod 2,$$

and so we may define a homomorphism $\theta : G_F \mapsto \mathrm{Im}(\widetilde{\rho}) \ltimes M_2(\mathbb{F}_2)$ by setting

$$\theta(\sigma) \equiv (\widetilde{\rho}(\sigma), \mu(\sigma)) \pmod 2.$$

Note that $\ker(\theta) = \{\sigma \in G_F, \mu(\sigma) = 0 \pmod 2\} \cap \ker(\widetilde{\rho})$. In particular, $\phi(\sigma) = 0$ for all $\sigma \in \ker(\theta)$, and so ϕ factors through $\mathrm{Im}(\widetilde{\rho}) \ltimes M_2(\mathbb{F}_2)$ as $\phi = \varphi \circ \theta$, where (by definition of ϕ) we find $\varphi : \mathrm{Im}(\widetilde{\rho}) \ltimes M_2(\mathbb{F}_2) \to \mathbb{F}_2$ is defined by

$$\varphi((M_1, M_2)) := \mathrm{Tr}(M_1M_2).$$

Let $\widetilde{\mu}$ denote the reduction of μ modulo 2. Since

$$\begin{aligned}\det(\rho_1(\sigma)) &= \det(1 + 2^r\mu(\sigma))\det(\rho_2(\sigma)) \\ &= (1 + 2^r\mathrm{Tr}(\mu(\sigma)) + 2^{2r}\det(\mu(\sigma)))\det(\rho_2(\sigma)) \\ &\equiv (1 + 2^r\mathrm{Tr}(\mu(\sigma)))\det(\rho_2(\sigma)) \pmod{2^{r+1}},\end{aligned}$$

equality of the determinants of ρ_1 and ρ_2 implies that

$$\mathrm{Im}(\widetilde{\mu}) \subset M_2^0(\mathbb{F}_2) := \{M \in M_2(\mathbb{F}_2), \mathrm{Tr}(M) = 0 \pmod 2\},$$

and hence has at most order 2^3. Thus we may take the group G mentioned previously to be $\mathrm{Im}(\widetilde{\rho}) \ltimes M_2^0(\mathbb{F}_2)$.

Since the residual representations have S_3-image, we are interested in the structure of the group $S_3 \ltimes M_2^0(\mathbb{F}_2)$. The following result will be useful:

Lemma 6.5.3. *We have an isomorphism $S_3 \ltimes M_2^0(\mathbb{F}_2) \simeq S_4 \times C_2$.*

Proof. Recall our previous identification of S_3 with $\mathrm{GL}_2(\mathbb{F}_2)$, given by:

$$(12) \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \ (13) \mapsto \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}.$$

Now, $M_2^0(\mathbb{F}_2) \simeq (\mathbb{Z}/2\mathbb{Z})^3$, where we may choose our generators to be

$$v_1 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \ v_2 = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \ v_3 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

and the group action corresponds to matrix addition. The action of S_3 on $M_2^0(\mathbb{F}_2)$ is given by the usual conjugation of matrices.

It is clear that under this action, the generator v_3 is fixed by all elements of S_3, and so we have an isomorphism $S_3 \ltimes M_2^0(\mathbb{F}_2) \simeq (S_3 \ltimes V_4) \times C_2$, where V_4 is the Klein group generated by v_1 and v_2. A quick check reveals that the S_3-action induces a permutation on the set $\{v_1, v_2, v_1 + v_2\}$. More precisely, if we set $u_1 = v_1$, $u_2 = v_2$, $u_3 = v_1 + v_2$, then the action of S_3 on $\{u_1, u_2, u_3\}$ is given by

$$\sigma(u_i) = u_{\sigma(i)},$$

corresponding to the action of S_3 on the subgroup $V_4 = \langle (14)(23), (13)(24) \rangle$ of S_4 (where we identify $S_3 \subset S_4$ as the set of permutations fixing the element 4). Indeed, the identification

$$v_1 \mapsto (14)(23), \ v_2 \mapsto (13)(24)$$

gives a concrete isomorphism $S_3 \ltimes \langle v_1, v_2 \rangle \simeq S_4$, and the result follows. □

As per our previous discussion, this means we may restrict our attention to Galois extensions L/F with $\mathrm{Gal}(L/F) \subset S_4 \times C_2$. This still gives us an infinite choice, so we attempt to control ramification in the field L. This turns out to be straightforward: we claim that the only primes of $\mathcal{O}_F$ which can ramify in L are those lying in the finite set S. Indeed, if $\mathfrak{p}$ is a prime *not* contained in the set S, then ρ_1 and ρ_2 are unramified at $\mathfrak{p}$, so in particular $\mathrm{Frob}_{\mathfrak{p}} \in \ker(\theta)$. It therefore follows that $\mathfrak{p}$ must be unramified in the field $L = F_\theta$. Restricting ramification in this manner results in a finite number of possible extensions. We may reduce this even further by noting that F_θ must also contain the fixed field $F_\rho := \overline{F}^{\ker(\widetilde{\rho})}$.

As stated previously, we wish to know which elements of $\mathrm{Im}(\widetilde{\rho}) \ltimes M_2^0(\mathbb{F}_2)$ have non-trivial image under the map φ. A simple check reveals that the elements of $S_4 \times C_2$ with non-trivial image are precisely those of order 4 or 6. These elements split into three conjugacy classes: if we choose elements σ_3 and σ_4 of order 3 and 4 in S_4 respectively, and let τ be the generator of C_2, then representatives of these conjugacy classes are (σ_4, id), (σ_4, τ) and (σ_3, τ).

Thus for each extension L of F as described above, we need to find primes $\mathfrak{p}_L$ in $\mathcal{O}_F$ whose Frobenius elements correspond to these conjugacy classes in $\mathrm{Gal}(L/F)$, and compare the traces of ρ_1 and ρ_2 on $\mathrm{Frob}_{\mathfrak{p}_L}$. Since we are looking for elements of order 4 or 6, and since $\mathrm{Gal}(L/F)$ must contain $\mathrm{Im}(\widetilde{\rho}) \simeq S_3$, we may restrict our attention to extensions L/F with Galois group isomorphic to $S_3 \times C_2$, S_4, or $S_4 \times C_2$.

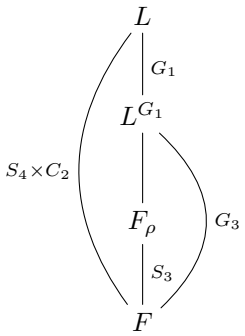
In fact, we may make things even easier than this, by considering only those extensions with Galois group $S_3 \times C_2$ or S_4. First of all, note that $S_4 \times C_2$ fits into the exact sequences

$$1 \longrightarrow V_4 \longrightarrow S_4 \times C_2 \longrightarrow S_3 \times C_2 \longrightarrow 1,$$

$$1 \longrightarrow C_2 \longrightarrow S_4 \times C_2 \longrightarrow S_4 \longrightarrow 1.$$

In the first sequence the map $V_4 \longrightarrow S_4 \times C_2$ is given by embedding the Klein group V_4 naturally into S_4, while the map $S_4 \times C_2 \to S_3 \times C_2$ is given by the isomorphism $S_4 \times C_2 \simeq (S_3 \ltimes V_4) \times C_2$, followed by the projection $((\sigma, \tau), \mu) \mapsto (\sigma, \mu)$. The maps in the second sequence are the obvious choices. Also, every order 4 element of $S_4 \times C_2$ maps to an order 4 element in S_4, while every order 6 element of $S_4 \times C_2$ maps to an order 6 element of $S_3 \times C_2$ under these surjections.

How does this help us? Suppose that L/F is an $(S_4 \times C_2)$-extension, such that L contains F_ρ as a subfield. Then, denoting by G_1 and G_3 the first and third non-trivial groups in either sequence respectively, we have the following situation:



Since we wish to consider primes $\mathfrak{p} \in \mathcal{O}_K$ whose Frobenius elements have order 4 or 6 in $S_4 \times C_2$, and each such element maps to an element of order 4 or 6 in G_3, we may instead consider the extension L^{G_1}/F. As such, we shall henceforth assume that $\mathrm{Gal}(L/F) \simeq S_4$ or $S_3 \times C_2$. Since these groups have only a single conjugacy class of order 4 and order 6 elements respectively, this means that for each such extension, we need only find a single prime $\mathfrak{p}$ of inertial degree either 4 or 6 in L.

We have therefore significantly reduced the number of cases we need to consider, but there are still some fairly substantial difficulties which we need to circumvent. Most notably, the groups $S_3 \times C_2$ and S_4, while small, are non-abelian, and thus do not fall under the remit of class field theory, which we would hope to use to characterize extensions of F. However, the extension L/F_ρ is much smaller, and will prove more tractable. Indeed, we shall show that L is the normal closure of a quadratic extension of F_ρ.

Let $\mathfrak{m}_\rho$ be a modulus in F_ρ invariant under the action of $\mathrm{Gal}(F_\rho/F)$. Then $\mathrm{Gal}(F_\rho/F)$ acts on the ray class group $Cl(\mathcal{O}_{F_\rho}, \mathfrak{m}_\rho)$, and thus induces an action on the additive characters of the group, given by $\psi^\sigma = \psi \circ \sigma$, for a character ψ and $\sigma \in \mathrm{Gal}(F_\rho/F)$.

Lemma 6.5.4. *Let ψ be a character of $Cl(\mathcal{O}_{F_\rho}, \mathfrak{m}_\rho)$, corresponding to the quadratic extension $F_\rho(\sqrt{\alpha})$, and let $\sigma \in \mathrm{Gal}(F_\rho/F)$. Then $\psi^{\sigma^{-1}}$ corresponds to the quadratic extension $F_\rho(\sqrt{\sigma(\alpha)})$.*

Proof. Any character is completely defined by its values on non-ramified prime ideals of F_ρ. Precisely, if $\mathfrak{p} \subset \mathcal{O}_{F_\rho}$, then

$$\psi(\mathfrak{p}) = \begin{cases} 0; & \text{if } \mathfrak{p} \text{ splits,} \\ 1; & \text{if } \mathfrak{p} \text{ is inert.} \end{cases}$$

If $\mathfrak{p}$ does not divide the fractional ideal α, then $\mathfrak{p}$ splits if, and only if, α is a square modulo $\mathfrak{p}$, which holds if, and only if, $\sigma(\alpha)$ is a square modulo $\sigma(\mathfrak{p})$, and the result is clear. □

We will need the following result:

Proposition 6.5.5. *Let L/F be a Galois extension, with $\mathrm{Gal}(L/F) = V_4$, and let L_1, L_2 and L_3 denote the three intermediate quadratic extensions of F. Then for any prime $\mathfrak{p} \subset \mathcal{O}_F$ which does not ramify in L, $\mathfrak{p}$ either has inertial degree 2 in precisely two of the L_i, or splits completely in L.*

Proof. Since V_4 is a 2-group, any such prime $\mathfrak{p}$ has either inertial degree 2 in L or splits completely, so we consider only the former case. Let $\mathrm{Gal}(L/F) = \langle \sigma, \tau \rangle$, and suppose $\mathfrak{p}\mathcal{O}_L = \mathfrak{r}_1\mathfrak{r}_2$, where $D(\mathfrak{r}_i|\mathfrak{p}) \simeq C_2$. Without loss of generality, $\mathfrak{r}_1$ is fixed by σ, and, after reordering, we may assume that $L_1 = L^{\langle \sigma \rangle}$, and thus

$$\mathrm{Gal}(L/L_k) \cap D(\mathfrak{r}_i|\mathfrak{p}) = \begin{cases} D(\mathfrak{r}_i|\mathfrak{p}); & \text{if } k = 1, \\ \{\mathrm{Id}\}; & \text{if } k = 2, 3. \end{cases}$$

Therefore, given a prime $\mathfrak{q}_k \subset \mathcal{O}_{L_i}$ above $\mathfrak{p}$, we see that

$$D(\mathfrak{r}_i|\mathfrak{q}_k) = \begin{cases} D(\mathfrak{r}_i|\mathfrak{p}); & \text{if } k = 1, \\ \{\mathrm{Id}\}; & \text{if } k = 2, 3, \end{cases}$$

and the result follows. □

Proposition 6.5.6. *Let F_ρ/F be a Galois S_3-extension, and let ψ be a quadratic character of $Cl(\mathcal{O}_{F_\rho}, \mathfrak{m}_\rho)$, where $\mathfrak{m}_\rho$ is a $\mathrm{Gal}(F_\rho/F)$-invariant modulus in L. Then:*

(i) *The quadratic extension of F_ρ corresponding to ψ is Galois over F if, and only if, $\psi^\sigma = \psi$ for all $\sigma \in \mathrm{Gal}(F_\rho/F)$;*

(ii) *The quadratic extension of F_ρ corresponding to ψ has normal closure over F with Galois group isomorphic to S_4 if, and only if, the elements fixing ψ form an order 2 subgroup, and $\psi + \psi^\sigma = \psi^{\sigma^2}$, where σ is any order 3 element of $\mathrm{Gal}(F_\rho/F)$.*

Proof. Let $F_\rho(\sqrt{\alpha})$ be a quadratic extension of F_ρ. Its normal closure over F is the compositum

$$L = \prod_{\sigma \in \mathrm{Gal}(F_\rho/F)} F_\rho(\sqrt{\sigma(\alpha)}),$$

and so in particular $\mathrm{Gal}(L/F_\rho)$ is an abelian 2-group. By the previous lemma, if $F_\rho(\sqrt{\alpha})$ corresponds to the character ψ, then the fields $F_\rho(\sqrt{\sigma(\alpha)})$ correspond to the characters ψ^σ, for $\sigma \in \mathrm{Gal}(F_\rho/F)$, and so statement (i) is clear.

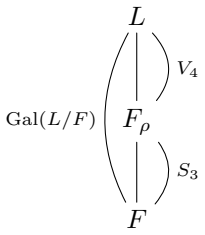
We therefore consider the second statement. Suppose first that the stabilizer of ψ in $\mathrm{Gal}(F_\rho/F)$ is a 2-group, and that $\psi+\psi^\sigma = \psi^{\sigma^2}$, for σ an order 3 element of $\mathrm{Gal}(F_\rho/F)$. The condition on the stabilizer of ψ implies that

$$L = F_\rho(\sqrt{\alpha}) \cdot F_\rho(\sqrt{\gamma(\alpha)}) \cdot F_\rho(\sqrt{\gamma^2(\alpha)}),$$

for some order 3 element $\gamma \in \mathrm{Gal}(F_\rho/F)$.

Let $\sigma = \gamma^{-1}$, so that the corresponding quadratic characters are given by ψ, ψ^σ and ψ^{σ^2}. Consider the compositum $F_\rho(\sqrt{\alpha}) \cdot F_\rho(\sqrt{\gamma(\alpha)})$. By **Proposition 6.5.5**, the field corresponding to the character $\varphi = \psi + \psi^\sigma$ is a quadratic subfield of this compositum. However, the conditions in the statement imply that $\varphi = \psi^{\sigma^2}$, and so $L = F_\rho(\sqrt{\alpha}) \cdot F_\rho(\sqrt{\gamma(\alpha)})$.

As a result, $[L : F_\rho] = 4$, and $\mathrm{Gal}(L/F_\rho) \simeq V_4$, and the situation is summed up by the following diagram:



We therefore have a short exact sequence

$$1 \longrightarrow V_4 \xrightarrow{\iota} \mathrm{Gal}(L/F) \longrightarrow S_3 \longrightarrow 1,$$

and so $\mathrm{Gal}(L/F) \simeq S_3 \ltimes V_4$, with the action of S_3 on V_4 given by

$$\tau^\sigma = \iota^{-1}(\sigma\iota(\tau)\sigma^{-1}),\ \sigma \in S_3,\ \tau \in V_4,$$

where we embed S_3 into $\mathrm{Gal}(L/F)$ via the inclusion $\mathrm{Gal}(F_\rho/F) \hookrightarrow \mathrm{Gal}(L/F)$.

We claim that this action induces a right action of $\mathrm{Gal}(F_\rho/F) \simeq S_3$ on the quadratic characters of $Cl(\mathcal{O}_{F_\rho}, \mathfrak{m}_\rho)$, given by $\psi \cdot \sigma = \sigma^{-1} \cdot \psi$. Indeed, suppose we embed $V_4 \hookrightarrow \mathrm{Gal}(L/F)$ via the map ι. Each non-trivial element $\tau \in V_4$ gives rise to a quadratic extension of F_ρ, namely $L^{\langle\tau\rangle}$. Say $L^{\langle\tau\rangle} = F_\rho(\sqrt{\beta})$ for some $\beta \in F_\rho$. Then $L^{\langle\tau^\sigma\rangle} = F_\rho(\sigma(\sqrt{\beta})) = F_\rho(\sqrt{\sigma(\beta)})$ for any $\sigma \in S_3$. Associating quadratic characters of $Cl(\mathcal{O}_{F_\rho}, \mathfrak{m}_\rho)$ with quadratic extensions of F_ρ as before, the previous lemma confirms our claim.

As a result, the assumption (ii) means that, in the action of S_3 on V_4, any order 3 element of S_3 must act non-trivially (as the stabilizer of our character ψ is a 2-group). Identifying V_4 with a 2-dimensional $\mathbb{F}_2$-vector space, this S_3-action gives a morphism

$$\alpha : S_3 \to \mathrm{GL}_2(\mathbb{F}_2),$$

whose image must therefore contain an order 3 element. Since the kernel of α must be a normal subgroup of S_3 containing no order 3 elements, it is trivial, and thus α is an automorphism of $\mathrm{GL}_2(\mathbb{F}_2)$. Now, there is a unique such automorphism (up to inner automorphisms, which will not change the isomorphism class of $S_3 \ltimes V_4$) and so $\mathrm{Gal}(L/F) \simeq S_4$, as claimed.

Conversely, if $\mathrm{Gal}(L/F) \simeq S_4$ then $\mathrm{Gal}(L/F_\rho) \simeq V_4$. Thus there are precisely 3 intermediate quadratic extensions, so the stabilizer of ψ is a 2-group. Moreover, since $L = L_1 \cdot L_2$ for any pair L_1, L_2 of these intermediate fields, the relation $\psi \cdot \psi^\sigma = \psi^{\sigma^2}$ must hold for any $\sigma \in S_3$ of order 3. □

In summary, to find our list of primes we need to compute all Galois extensions L/F which are unramified outside of S, which contain F_ρ as a subfield, and for which $\mathrm{Gal}(L/F) \simeq S_3 \times C_2$ or S_4. Having found these, we need to find a prime $\mathfrak{p}$ for which $\mathrm{Frob}_\mathfrak{p}$ has maximal order in $\mathrm{Gal}(L/F)$, and compare the traces of ρ_1 and ρ_2 on $\mathrm{Frob}_\mathfrak{p}$. By **Proposition 6.5.6**, it is enough to find all quadratic extensions of F_ρ which satisfy either criterion (i) or (ii), and then compute their normal closures.

Since we have already determined whether the residual representations are isomorphic, we may use the Faltings-Serre method to determine whether the representations themselves are isomorphic. We need to find all possible Galois $(S_3 \times C_2)$- or S_4-extensions L of F, and compare the traces of ρ_π and ρ_E at Frobenius elements of maximal order in each extension. We do this by considering the Galois closures of quadratic extensions of $L_E \simeq L_\pi$. Using **Theorem 6.3.1** once again, we consider the ray class group $Cl(\mathcal{O}_{L_E}, \mathfrak{m}_{L_E})$, where

$$\mathfrak{m}_{L_E} = \prod_{\mathfrak{q} | 2\mathfrak{n}\mathcal{O}_{L_E}} \mathfrak{q}^{e(\mathfrak{q})},$$

where

$$e(\mathfrak{q}) = \begin{cases} 1; & \text{if } \mathfrak{q} \nmid 2, \\ 2e(\mathfrak{q}/2) + 1; & \text{if } \mathfrak{p} | 2. \end{cases}$$

Then any quadratic extension of L_E corresponds to a quadratic character of $Cl(\mathcal{O}_{L_E}, \mathfrak{m}_{L_E})$. For the rest of this section, fix a basis $\{\chi_1, \ldots, \chi_t\}$ of these characters, and a basis $\{\mathfrak{a}_1, \ldots, \mathfrak{a}_t\}$ of even-order elements of $Cl(\mathcal{O}_{L_E}, \mathfrak{m}_{L_E})$, such that $\chi_i(\mathfrak{a}_j) = \delta_{ij}$.

We begin by considering the $(S_3 \times C_2)$-extensions. By **Proposition 6.5.6**.(i), we know that such extensions correspond to quadratic characters ψ which are fixed by $\mathrm{Gal}(L_E/F)$ or, equivalently, that $\psi + \psi^\sigma = 0$ for all $\sigma \in \mathrm{Gal}(L_E/F)$. In other words, writing $\psi = \sum \epsilon_i \chi_i$, we are looking for exponents ϵ_i for which

$$\sum \epsilon_i(\chi_i(\mathfrak{a}) + \chi_i(\sigma(\mathfrak{a}))) = 0$$

for all ideals $\mathfrak{a}$.

Fixing an order 3 element σ and an order 2 element τ of $\mathrm{Gal}(L_E/F)$, we therefore find the kernels V_σ and V_τ of the homogeneous systems

$$\begin{pmatrix} \chi_1(\mathfrak{a}_1) + \chi_1(\gamma(\mathfrak{a}_1)) & \dots & \chi_t(\mathfrak{a}_1) + \chi_t(\gamma(\mathfrak{a}_1)) \\ \vdots & \ddots & \vdots \\ \chi_1(\mathfrak{a}_1) + \chi_1(\gamma(\mathfrak{a}_1)) & \dots & \chi_t(\mathfrak{a}_t) + \chi_t(\gamma(\mathfrak{a}_t)) \end{pmatrix}, \ \gamma \in \{\sigma, \tau\}$$

and intersect them. The corresponding characters give rise to all $(S_3 \times C_2)$-extensions of F containing L_E.

Let $\{\psi_1, \dots, \psi_s\}$ be a $(\mathbb{Z}/2\mathbb{Z})$-basis of $V_\sigma \cap V_\tau$, and let $\{\mathfrak{p}_1, \dots, \mathfrak{p}_r\}$, be a set of primes of $\mathcal{O}_F$ with inertial degree 3 in L_E, such that the vectors $(\psi_1(\mathfrak{q}_i), \dots, \psi_s(\mathfrak{q}_i))$ span $(\mathbb{Z}/2\mathbb{Z})^s$, where $\mathfrak{q}_i$ is any prime in $\mathcal{O}_{L_E}$ above $\mathfrak{p}_i$.

Now, for any Galois $(S_3 \times C_2)$-extension L of F containing L_E, let ψ_L be the corresponding quadratic character on $Cl(\mathcal{O}_{L_E}, \mathfrak{m}_{L_E})$. By **Proposition 6.3.2**, we know that $\psi_L(\mathfrak{q}_i)$ is non-trivial for some prime $\mathfrak{q}_i$, and so $\mathfrak{q}_i$ has inertial degree 2 in L. By our choice of $\mathfrak{p}_i$, this means that $\mathfrak{p}_i$ has inertial degree 6 in L, as required. If the traces of Frobenius elements at the primes $\mathfrak{p}_i$ are equivalent then, if the two representations were non-isomorphic, the map ϕ must factor through an S_4-extension.

Our last step is to eliminate this possibility. By **Proposition 6.5.6**, we know that any S_4-extension L of F containing L_E arises as the normal closure of a quadratic extension of L_E such that, denoting by ψ_L the corresponding quadratic character of $Cl(\mathcal{O}_{L_E}, \mathfrak{m}_{L_E})$, the stabilizer of ψ_L in $\mathrm{Gal}(L_E/F)$ is an order 2 subgroup, and $\psi_L + \psi_L^\sigma = \psi_L^{\sigma^2}$, where σ is any order 3 element of $\mathrm{Gal}(L_E/F)$.

Since the stabilizer of any such character has order 2, σ cannot act trivially, and thus ψ, ψ^σ and ψ^{σ^2} are three distinct characters with these properties, and all give the same normal closure. Thus, if we let $\mathcal{S}$ denote the set of all characters with these properties, we see that we can write $\mathcal{S}$ as the union of three disjoint sets.

Moreover, since σ acts transitively by right multiplication on the order 2 elements of S_3, we see that

$$\mathcal{S} = V_\tau \cup V_{\tau\sigma} \cup V_{\tau\sigma^2},$$

where V_τ denotes the quadratic characters belonging to $\mathcal{S}$ invariant under the action of an order 2 element τ and the union is disjoint. Thus each of these sets is in bijection with all extensions L of L_E whose normal closure $\widetilde{L}$ satisfies $\mathrm{Gal}(\widetilde{L}/F) \simeq S_4$.

Analogously to the previous case, we are searching for characters $\psi = \sum \epsilon_i \chi_i$ whose exponents satisfy

$$\sum \epsilon_i(\chi_i(\mathfrak{a}) + \chi_i(\sigma(\mathfrak{a})) + \chi_i(\sigma^2(\mathfrak{a}))) = 0$$

and

$$\sum \epsilon_i(\chi_i(\mathfrak{a}) + \chi_i(\tau(\mathfrak{a}))) = 0$$

for some order 3 and order 2 element σ and $\tau \in \mathrm{Gal}(L_E/F)$. Fixing σ, we compute the kernel W_σ to the homogeneous system

$$\begin{pmatrix} \chi_1(\mathfrak{a}_1) + \chi_1(\sigma(\mathfrak{a}_1)) + \chi_1(\sigma^2(\mathfrak{a}_1)) & \dots & \chi_t(\mathfrak{a}_1) + \chi_t(\sigma(\mathfrak{a}_1)) + \chi_t(\sigma^2(\mathfrak{a}_1)) \\ \vdots & \ddots & \vdots \\ \chi_1(\mathfrak{a}_t) + \chi_1(\sigma(\mathfrak{a}_t)) + \chi_1(\sigma^2(\mathfrak{a}_t)) & \dots & \chi_t(\mathfrak{a}_t) + \chi_t(\sigma(\mathfrak{a}_t)) + \chi_t(\sigma^2(\mathfrak{a}_t)) \end{pmatrix},$$

and intersect it with the kernel V_τ obtained previously. The corresponding characters give rise to all quadratic extensions of L_E whose normal closure over F is an S_4-extension.

Let $\{\psi_1, \dots, \psi_s\}$ be a $(\mathbb{Z}/2\mathbb{Z})$-basis of $W_\sigma \cap V_\tau$, and let $\{\mathfrak{p}_1, \dots, \mathfrak{p}_r\}$ be a set of primes of $\mathcal{O}_F$ with inertial degree 2 in L_E, such that the vectors $(\psi_1(\mathfrak{q}_i), \dots, \psi_s(\mathfrak{q}_i))$, $(\psi_1(\sigma(\mathfrak{q}_i)), \dots, \psi_s(\sigma(\mathfrak{q}_i)))$ and $(\psi_1(\sigma^2(\mathfrak{q}_i)), \dots, \psi_s(\sigma^2(\mathfrak{q}_i)))$ span $(\mathbb{Z}/2\mathbb{Z})^s$, where $\mathfrak{q}_i$ is any prime in $\mathcal{O}_{L_E}$ above $\mathfrak{p}_i$.

Now, for any Galois S_4-extension $\widetilde{L}$ of F containing L_E, let L be the quadratic extension of L_E contained within, and let ψ_L be the corresponding quadratic character on $Cl(\mathcal{O}_{L_E}, \mathfrak{m}_{L_E})$. By **Proposition 6.3.2**, we know that $\psi_L(\mathfrak{q}_i)$ is non-trivial for some prime $\mathfrak{q}_i$, and so $\mathfrak{q}_i$ has inertial degree 2 in L. By our choice of $\mathfrak{p}_i$, this means that $\mathfrak{p}_i$ has inertial degree 4 in L, as required. If the traces of Frobenius elements at the primes $\mathfrak{p}_i$ are equivalent then we can conclude that the semisimplifications of our two representations are isomorphic.

6.6 Examples

In this section we provide examples of elliptic curves corresponding to each of the cohomology classes listed in **Section 5.3**, and aim to prove that the Galois representation ρ_E arising from each curve is isomorphic to the representation ρ_π attached to each cuspidal eigenclass (in the sense of **Section 3.5**).

For each isomorphism class of curves over F, we present a global minimal model - an integral element of the isomorphism class whose discriminant has minimal valuation at all prime ideals dividing it. Since each field we consider has trivial class group, such a model is guaranteed to exist.

The elliptic curves were found using MAGMA - once a candidate cuspidal eigenclass in $H^*(\Gamma_0(\mathfrak{n}), \mathbb{C})$ had been identified for a particular level $\mathfrak{n}$, we were able to search for elliptic curves of conductor $\mathfrak{n}$ using Steve Donnelly's EllipticCurveSearch routine. This process was accelerated by computing a number of Hecke eigenvalues, and providing these as input for the routine. In all cases, with the exception of the class labelled 4516 over the field F_1, this method yielded the correct curve.

To find this remaining curve, we made use of an idea presented in **[DGKY14], Section 3.3**, which involves considering the possible torsion subgroups of the curve E. Noting that the groups of points on the reduced curves $\widetilde{E}(\mathcal{O}_F/\mathfrak{p})$ have order divisible by 5, we posit that the torsion subgroup of $E(F)$ is isomorphic to $\mathbb{Z}/5\mathbb{Z}$ (since for any prime $\mathfrak{p}$ of good reduction, the torsion subgroup of $E(F)$ injects into $\widetilde{E}(\mathcal{O}_F/\mathfrak{p})$, so the order of this torsion subgroup must divide 5).

According to **[Kub76], Table 3**, any *rational* elliptic curve E with 5-torsion is isogenous to a curve E' with a parametrization of the form

$$E' : y^2 + (1-r)xy - ry = x^3 - rx^2, \ r \in \mathbb{Z}.$$

Inspired by this, we performed a search over values of $r \in \mathcal{O}_F$, which yielded the required curve with the value $r = t^3 + t^2 - 4t + 3$, where t denotes a primitive twelfth root of unity.

For each curve, we compute, using the ideas of the previous sections, a finite set $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$ of primes of F such that equality of the traces of $\rho_E(\mathrm{Frob}_{\mathfrak{p}_i})$ and $\rho_\pi(\mathrm{Frob}_{\mathfrak{p}_\pi})$ for each prime $\mathfrak{p}_i$ implies isomorphism of ρ_E and ρ_π. We then compute the eigenvalues for the Hecke operators $T_{\mathfrak{p}_i}$ for each of these primes to ascertain the isomorphism.

We found that none of the curves had complex multiplication. In particular, if the residual representation $\widetilde{\rho_E}$ has S_3-image, this implies absolute irreducibility, allowing us to apply the Faltings-Serre method.

Of these curves, there are several that cannot be isogenous to the base change of an elliptic curve defined over a subfield. We note that, in each of our examples, if the conductor $\mathfrak{n}$ of the given curve is not of the form $\mathfrak{n}_0\mathcal{O}_F$, for some ideal $\mathfrak{n}_0$ contained in a proper subfield of F, then we can find a rational prime p which splits completely over the field F as $p\mathcal{O}_F = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4$, such that the traces of the Hecke operators $T_{\mathfrak{p}_i}$ take on at least three distinct values. In particular, the local L-factor at p has at least three distinct factors. By contrast, the L-factors of a curve defined over a subfield K_0 would have at most two distinct factors, since such a curve is invariant under any element of $\mathrm{Gal}(F/K_0)$. Since isogeny preserves L-factors, the result is clear.

Computations to determine the set of primes as described in the previous sections were performed with PARI ([**PAR14**]). For each of the elliptic curves we discovered, the corresponding residual representation was either trivial, or had image isomorphic to S_3. For ease of reference, we shall briefly summarize the methods of **Sections 6.3**, **6.4** and **6.5** for determining isomorphism in these two cases:

If $\widetilde{\rho_E}$ has trivial image, then:

- We compute the ray class group $Cl(\mathcal{O}_F, \mathfrak{m})$ from **Section 6.3, Case 1**, whose quadratic characters correspond to quadratic extensions of F unramified away from the primes dividing $2\mathfrak{n}$.
- For each quadratic character of this group, we construct the corresponding field F_π, and compute the ray class group $Cl(\mathcal{O}_{F_\pi}, \mathfrak{m}_\pi)$, again from **Section 6.3, Case 1**. We compute a $(\mathbb{Z}/3\mathbb{Z})$-basis $\{\chi_1, \ldots, \chi_t\}$ of the cubic characters of this group, and determine a set of primes $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}$ of F such that the vectors $(\chi_1(\mathfrak{q}_i), \ldots, \chi_t(\mathfrak{q}_i))$ span $(\mathbb{Z}/3\mathbb{Z})^t$, where $\mathfrak{q}_i$ is a prime of F_π lying above $\mathfrak{p}_i$.
- If $\mathrm{Tr}(\rho_\pi(\mathrm{Frob}_{\mathfrak{p}_i}))$ is even for each of these primes (running over all choices of F_π) then the residual representations are isomorphic.
- If this is the case, then we compute a $(\mathbb{Z}/2\mathbb{Z})$-basis $\{\chi_1, \ldots, \chi_t\}$ of the quadratic characters of the ray class group $Cl(\mathcal{O}_F, \mathfrak{m})$, and determine a set $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}$ of primes of F for which the vectors $(\chi_1(\mathfrak{p}_i), \ldots, \chi_t(\mathfrak{p}_i))$ cover $(\mathbb{Z}/2\mathbb{Z})^t \setminus \{0\}$.
- If $\mathrm{Tr}(\rho_\pi(\mathrm{Frob}_{\mathfrak{p}_i})) = \mathrm{Tr}(\rho_E(\mathrm{Frob}_{\mathfrak{p}_i}))$ for each of these primes, then the representations ρ_π and ρ_E are isomorphic.

If $\widetilde{\rho_E}$ has image isomorphic to S_3, then:

- We compute the ray class group $Cl(\mathcal{O}_F, \mathfrak{m})$ from **Section 6.3, Case 3**, whose quadratic and cubic characters correspond to quadratic and cubic extensions of F unramified away from the primes dividing $2\mathfrak{n}$.

- We compute the quadratic character ψ_{F_E} of $Cl(\mathcal{O}_F, \mathfrak{m})$ corresponding to the unique quadratic extension of F contained in L_E, extend this to a $(\mathbb{Z}/2\mathbb{Z})$-basis $\{\psi_{F_E}, \chi_1, \ldots, \chi_t\}$ of the quadratic characters of this group, and determine a set of primes $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}$ of F such that $\psi_{F_E}(\mathfrak{p}_i) = 0$ and the vectors $(\chi_1(\mathfrak{p}_i), \ldots, \chi_t(\mathfrak{p}_i))$ span $(\mathbb{Z}/2\mathbb{Z})^t$.

- If $\mathrm{Tr}(\rho_\pi(\mathrm{Frob}_{\mathfrak{p}_i}))$ is even for any of these primes, then we deduce that the residual representations are non-isomorphic, otherwise, we deduce that the field L_π can contain no quadratic extension of F other than F_E.

- In this case, we compute a $(\mathbb{Z}/3\mathbb{Z})$-basis $\{\chi_1, \ldots, \chi_t\}$ of the cubic characters of $Cl(\mathcal{O}_F, \mathfrak{m})$, and determine a set of primes $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}$ of F which are either inert in F_E, or split completely in L_E, such that the vectors $(\chi_1(\mathfrak{p}_i), \ldots, \chi_t(\mathfrak{p}_i))$ span $(\mathbb{Z}/3\mathbb{Z})^t$.

- If $\mathrm{Tr}(\rho_\pi(\mathrm{Frob}_{\mathfrak{p}_i}))$ is odd for any of these primes, then we deduce that the residual representations are non-isomorphic, otherwise, we deduce that L_π cannot be a cubic extension of F.

- If this is the case, we compute the ray class group $Cl(\mathcal{O}_{F_E}, \mathfrak{m}_E)$, again from **Section 6.3, Case 3**, whose cubic characters correspond to cubic extensions of the subfield F_E of L_E.

- We determine a cubic character ψ_E of $Cl(\mathcal{O}_{F_E}, \mathfrak{m}_E)$ corresponding to the extension L_E, extend it to a $(\mathbb{Z}/3\mathbb{Z})$-basis $\{\psi_E, \chi_1, \ldots, \chi_t\}$ of all such cubic characters, and determine a set $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}$ of primes of F such that $\psi_E(\mathfrak{q}_i) = 0$, and the vectors $(\chi_1(\mathfrak{q}_i), \ldots, \chi_t(\mathfrak{q}_i))$ span $(\mathbb{Z}/3\mathbb{Z})^t$, where $\mathfrak{q}_i$ is a prime of F_E lying above $\mathfrak{p}_i$.

- If $\mathrm{Tr}(\rho_\pi(\mathrm{Frob}_{\mathfrak{p}_i}))$ is even for each of these primes, we deduce that the residual representations are isomorphic.

- If this is the case, we then compute the ray class group $Cl(\mathcal{O}_{L_E}, \mathfrak{m}_{L_E})$ from **Section 6.5**, whose quadratic characters correspond to quadratic extensions of L_E unramified away from the primes dividing $2\mathfrak{n}$. We fix a $(\mathbb{Z}/2\mathbb{Z})$-basis $\{\chi_1, \ldots, \chi_t\}$ of these characters, and a basis $\{\mathfrak{a}_1, \ldots, \mathfrak{a}_t\}$ of even-order elements of $Cl(\mathcal{O}_{L_E}, \mathfrak{m}_{L_E})$ such that $\chi_i(\mathfrak{a}_j) = \delta_{ij}$.

- We compute the kernels V_σ, V_τ and W_σ of the homogeneous systems described in **Section 6.5**, where σ and τ are elements of the Galois group $\mathrm{Gal}(L_E/F)$ of order 3 and 2 respectively.

- We compute a $(\mathbb{Z}/2\mathbb{Z})$-basis $\{\psi_1, \ldots, \psi_s\}$ of $V_\sigma \cap V_\tau$, and a set of primes $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}$ of F with inertial degree 3 in L_E, such that the set of vectors of the form $(\psi_1(\mathfrak{q}_i), \ldots, \psi_s(\mathfrak{q}_i))$ span $(\mathbb{Z}/2\mathbb{Z})^s$, where $\mathfrak{q}_i$ lies above $\mathfrak{p}_i$.

- Next, we compute a $(\mathbb{Z}/2\mathbb{Z})$-basis $\{\psi_1, \ldots, \psi_s\}$ of $W_\sigma \cap V_\tau$, and a set of primes $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}$ of F with inertial degree 2 in L_E, such that the set of vectors of the form $(\psi_1(\mathfrak{q}_i), \ldots, \psi_s(\mathfrak{q}_i))$, $(\psi_1(\sigma(\mathfrak{q}_i)), \ldots, \psi_s(\sigma(\mathfrak{q}_i)))$ and $(\psi_1(\sigma^2(\mathfrak{q}_i)), \ldots, \psi_s(\sigma^2(\mathfrak{q}_i)))$ span $(\mathbb{Z}/2\mathbb{Z})^s$, where $\mathfrak{q}_i$ lies above $\mathfrak{p}_i$.

- If $\mathrm{Tr}(\rho_\pi(\mathrm{Frob}_{\mathfrak{p}_i})) = \mathrm{Tr}(\rho_E(\mathrm{Frob}_{\mathfrak{p}_i}))$ for the primes $\mathfrak{p}_i$ in each of these sets, then we deduce that the representations ρ_π and ρ_E are isomorphic.

6.6.1 The Field F_1

Let $F = F_1$, which we recall is defined to be $\mathbb{Q}(t)$, where t is a primitive twelfth root of unity. The table below gives a list of the prime ideals of F of norm at most 650, together with a generator for each ideal:

$\mathfrak{p}$	Generator	$\mathfrak{p}$	Generator	$\mathfrak{p}$	Generator
$\mathfrak{p}_2$	$-t^2+t+1$	$\mathfrak{p}_{181,3}$	$4t^3+t^2-t-2$	$\mathfrak{p}_{397,1}$	$-4t^3-2t^2+3t-1$
$\mathfrak{p}_3$	t^2+1	$\mathfrak{p}_{181,4}$	$2t^3+t^2-t-4$	$\mathfrak{p}_{397,2}$	t^3+3t^2+2t-4
$\mathfrak{p}_{13,1}$	$-t^3+t^2+1$	$\mathfrak{p}_{193,1}$	$-t^3+t^2+4t-1$	$\mathfrak{p}_{397,3}$	$-t^3+3t^2-2t-4$
$\mathfrak{p}_{13,2}$	t^3+t+1	$\mathfrak{p}_{193,2}$	$3t^2-t-4$	$\mathfrak{p}_{397,4}$	$-t^3+3t^2+4t-2$
$\mathfrak{p}_{13,3}$	$-t^3-t+1$	$\mathfrak{p}_{193,3}$	$3t^2+t-4$	$\mathfrak{p}_{409,1}$	$-5t^3+t^2+t-1$
$\mathfrak{p}_{13,4}$	t^3+t^2+1	$\mathfrak{p}_{193,4}$	t^3+t^2-4t-1	$\mathfrak{p}_{409,2}$	$-t^3+t^2+t-5$
$\mathfrak{p}_{5,1}$	$2t^2-t-2$	$\mathfrak{p}_{229,1}$	$-3t^3+2t^2+3t+1$	$\mathfrak{p}_{409,3}$	$-3t^3+4t^2-t-4$
$\mathfrak{p}_{5,2}$	t^3-2t^2-t	$\mathfrak{p}_{229,2}$	$-t^3+3t^2-2t-3$	$\mathfrak{p}_{409,4}$	$4t^3-5t-1$
$\mathfrak{p}_{37,1}$	$2t^3+t^2-2$	$\mathfrak{p}_{229,3}$	$2t^3-3t^2-3t$	$\mathfrak{p}_{421,1}$	$3t^3+t^2-2t-5$
$\mathfrak{p}_{37,2}$	t^3-2t^2-2t	$\mathfrak{p}_{229,4}$	$-3t^3-2t^2+3t-1$	$\mathfrak{p}_{421,2}$	$2t^3+4t^2-3t-5$
$\mathfrak{p}_{37,3}$	t^3+t^2-t-3	$\mathfrak{p}_{241,1}$	$4t^3-4t-1$	$\mathfrak{p}_{421,3}$	$5t^3-3t-2$
$\mathfrak{p}_{37,4}$	$3t^3+t^2-t-1$	$\mathfrak{p}_{241,2}$	$-t^3+4t^2-4$	$\mathfrak{p}_{421,4}$	$-3t^3+t^2+2t-5$
$\mathfrak{p}_{7,1}$	$2t^3-3t$	$\mathfrak{p}_{241,3}$	t^3-t-4	$\mathfrak{p}_{433,1}$	$-3t^3+2t^2+t-5$
$\mathfrak{p}_{7,2}$	t^3-3t	$\mathfrak{p}_{241,4}$	$-4t^3+t^2-1$	$\mathfrak{p}_{433,2}$	$5t^3+t^2-2t-3$
$\mathfrak{p}_{61,1}$	$-t^3+t^2+3t-1$	$\mathfrak{p}_{277,1}$	$3t^2+2t-4$	$\mathfrak{p}_{433,3}$	t^3-2t^2-5t
$\mathfrak{p}_{61,2}$	$2t^2-t-3$	$\mathfrak{p}_{277,2}$	$2t^3-t^2-3t-4$	$\mathfrak{p}_{433,4}$	$3t^3+2t^2-t-5$
$\mathfrak{p}_{61,3}$	$2t^2+t-3$	$\mathfrak{p}_{277,3}$	t^3+2t^2-4t-2	$\mathfrak{p}_{457,1}$	$3t^2+3t-4$
$\mathfrak{p}_{61,4}$	t^3+t^2-3t-1	$\mathfrak{p}_{277,4}$	$2t^3-4t^2+t-1$	$\mathfrak{p}_{457,2}$	$-3t^3-3t^2+3t-1$
$\mathfrak{p}_{73,1}$	$-t^3-3t^2$	$\mathfrak{p}_{17,1}$	$4t^2-t-4$	$\mathfrak{p}_{457,3}$	$3t^3-3t^2-3t-1$
$\mathfrak{p}_{73,2}$	$2t^3+2t^2-3$	$\mathfrak{p}_{17,2}$	t^3-4t^2-t	$\mathfrak{p}_{457,4}$	t^3+3t^2+3t-3
$\mathfrak{p}_{73,3}$	$-2t^3+2t^2-3$	$\mathfrak{p}_{313,1}$	$-t^3+2t^2+3t-5$	$\mathfrak{p}_{23,1}$	$2t^3+3t^2-2t-6$
$\mathfrak{p}_{73,4}$	$-t^3+3t^2+t-3$	$\mathfrak{p}_{313,2}$	t^3-4t^2-2t	$\mathfrak{p}_{23,2}$	$-2t^3+3t^2+2t-6$
$\mathfrak{p}_{97,1}$	$2t^3+t^2-2t-4$	$\mathfrak{p}_{313,3}$	$3t^3+3t^2-t-5$	$\mathfrak{p}_{541,1}$	$-2t^3+2t-5$
$\mathfrak{p}_{97,2}$	$-2t^3+4t^2-1$	$\mathfrak{p}_{313,4}$	t^3+2t^2-3t-5	$\mathfrak{p}_{541,2}$	$5t^3-3t-3$
$\mathfrak{p}_{97,3}$	$-2t^3-4t^2+1$	$\mathfrak{p}_{337,1}$	$5t^3+t^2-2t-2$	$\mathfrak{p}_{541,3}$	$5t^3-5t-2$
$\mathfrak{p}_{97,4}$	$-2t^3+t^2+2t-4$	$\mathfrak{p}_{337,2}$	$-2t^3+2t^2+t-5$	$\mathfrak{p}_{541,4}$	$-5t^2-2t$
$\mathfrak{p}_{109,1}$	t^3+t^2-2t-4	$\mathfrak{p}_{337,3}$	$2t^3+2t^2-t-5$	$\mathfrak{p}_{577,1}$	$-2t^3+3t^2-2t-4$
$\mathfrak{p}_{109,2}$	$-2t^3-2t^2+2t-1$	$\mathfrak{p}_{337,4}$	$-t^3+3t^2+2t-5$	$\mathfrak{p}_{577,2}$	$-4t^3-2t^2+3t-2$
$\mathfrak{p}_{109,3}$	$2t^3-2t^2-2t-1$	$\mathfrak{p}_{349,1}$	$-2t^3+3t-5$	$\mathfrak{p}_{577,3}$	$4t^3-2t^2-3t-2$
$\mathfrak{p}_{109,4}$	$-t^3+t^2+2t-4$	$\mathfrak{p}_{349,2}$	$4t^3-t^2-2t-2$	$\mathfrak{p}_{577,4}$	$2t^3-4t^2-4t+1$
$\mathfrak{p}_{11,1}$	$-3t^3+t^2+t-3$	$\mathfrak{p}_{349,3}$	t^3+2t^2+2t-4	$\mathfrak{p}_{601,1}$	$5t^3-5t-1$
$\mathfrak{p}_{11,2}$	t^3+2t^2-3t-3	$\mathfrak{p}_{349,4}$	$2t^3-3t-5$	$\mathfrak{p}_{601,2}$	$-t^3+5t^2-5$
$\mathfrak{p}_{157,1}$	$-4t^3+2t-1$	$\mathfrak{p}_{19,1}$	$2t^3-5t$	$\mathfrak{p}_{601,3}$	t^3-t-5
$\mathfrak{p}_{157,2}$	$-t^3+2t^2-4$	$\mathfrak{p}_{19,2}$	$3t^3-5t$	$\mathfrak{p}_{601,4}$	$-5t^3+t^2-1$
$\mathfrak{p}_{157,3}$	t^3+2t^2-4	$\mathfrak{p}_{373,1}$	$4t^3+2t^2-2t-5$	$\mathfrak{p}_{613,1}$	t^3+2t^2-5t-2
$\mathfrak{p}_{157,4}$	$4t^3-2t-1$	$\mathfrak{p}_{373,2}$	$2t^3+3t^2-4t-5$	$\mathfrak{p}_{613,2}$	$4t^2-2t-5$
$\mathfrak{p}_{181,1}$	$-2t^3+t^2+t-4$	$\mathfrak{p}_{373,3}$	$5t^3-3t-1$	$\mathfrak{p}_{613,3}$	$4t^2+2t-5$
$\mathfrak{p}_{181,2}$	t^3-2t^2-4t	$\mathfrak{p}_{373,4}$	$3t^3+t^2-5t-1$	$\mathfrak{p}_{613,4}$	$-t^3+2t^2+5t-2$

The following pages provide, for each of the cuspidal classes with rational eigenvalues found in **Section 5.3.1**, a list of primes which suffice to prove modularity of the corresponding elliptic curve, using the techniques of the previous sections. For each example, we then list the Hecke eigenvalues $a_{\mathfrak{p}}(\pi)$ for these primes, and are therefore able to prove that each of these curves is indeed modular.

Class 441

- The level $\mathfrak{n} = \mathfrak{p}_3\mathfrak{p}_{7,2}$, and the residual representation attached to the corresponding elliptic curve has trivial image.
- The modulus $\mathfrak{m} = \mathfrak{p}_2^5\mathfrak{p}_3\mathfrak{p}_{7,2}$, and the corresponding ray class group $Cl(\mathcal{O}_F, \mathfrak{m})$ is isomorphic to $\mathbb{Z}/24\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z})^3$.
- The primes $\{\mathfrak{p}_{13,1}, \mathfrak{p}_{13,2}, \mathfrak{p}_{13,3}, \mathfrak{p}_{13,4}, \mathfrak{p}_{5,1}, \mathfrak{p}_{5,2}, \mathfrak{p}_{37,1}, \mathfrak{p}_{37,2}, \mathfrak{p}_{37,3}, \mathfrak{p}_{7,1}, \mathfrak{p}_{61,2}, \mathfrak{p}_{73,1}\}$ suffice to prove isomorphism of the residual representations.
- The primes $\{\mathfrak{p}_{13,1}, \mathfrak{p}_{13,2}, \mathfrak{p}_{13,3}, \mathfrak{p}_{13,4}, \mathfrak{p}_{5,1}, \mathfrak{p}_{37,1}, \mathfrak{p}_{37,2}, \mathfrak{p}_{37,3}, \mathfrak{p}_{37,4}, \mathfrak{p}_{7,1}, \mathfrak{p}_{61,2}, \mathfrak{p}_{61,3}, \mathfrak{p}_{73,1}, \mathfrak{p}_{73,2}, \mathfrak{p}_{97,1}, \mathfrak{p}_{97,2}, \mathfrak{p}_{109,2}, \mathfrak{p}_{109,3}, \mathfrak{p}_{11,1}, \mathfrak{p}_{181,2}, \mathfrak{p}_{181,3}, \mathfrak{p}_{193,1}, \mathfrak{p}_{17,1}, \mathfrak{p}_{313,1}, \mathfrak{p}_{337,1}, \mathfrak{p}_{349,1}, \mathfrak{p}_{349,4}, \mathfrak{p}_{19,1}, \mathfrak{p}_{409,2}, \mathfrak{p}_{23,1}, \mathfrak{p}_{601,2}\}$ satisfy the conditions for Livné's theorem, and therefore suffice to prove isomorphism of the full representations.

Class 1156

- The level $\mathfrak{n} = \mathfrak{p}_2\mathfrak{p}_{17,2}$, and the residual representation attached to the corresponding elliptic curve has trivial image.
- The modulus $\mathfrak{m} = \mathfrak{p}_2^5\mathfrak{p}_{17,2}$, and the corresponding ray class group $Cl(\mathcal{O}_F, \mathfrak{m})$ is isomorphic to $\mathbb{Z}/32\mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z})^3$.
- The prime $\mathfrak{p}_{13,1}$ suffices to prove isomorphism of the residual representations.
- The primes $\{\mathfrak{p}_3, \mathfrak{p}_{13,1}, \mathfrak{p}_{13,2}, \mathfrak{p}_{13,3}, \mathfrak{p}_{13,4}, \mathfrak{p}_{5,1}, \mathfrak{p}_{37,1}, \mathfrak{p}_{37,3}, \mathfrak{p}_{7,1}, \mathfrak{p}_{73,1}, \mathfrak{p}_{73,3}, \mathfrak{p}_{97,3}, \mathfrak{p}_{109,2}, \mathfrak{p}_{109,4}, \mathfrak{p}_{457,1}\}$ satisfy the conditions for Livné's theorem, and therefore suffice to prove isomorphism of the full representations.

Class 2041

- The level $\mathfrak{n} = \mathfrak{p}_{13,3}\mathfrak{p}_{157,3}$, and the residual representation attached to the corresponding elliptic curve has trivial image.
- The modulus $\mathfrak{m} = \mathfrak{p}_2^5\mathfrak{p}_{13,3}\mathfrak{p}_{157,3}$, and the corresponding ray class group $Cl(\mathcal{O}_F, \mathfrak{m})$ is isomorphic to $\mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z})^3$.
- The prime $\mathfrak{p}_{13,1}$ suffices to prove isomorphism of the residual representations.
- The primes $\{\mathfrak{p}_3, \mathfrak{p}_{13,1}, \mathfrak{p}_{13,2}, \mathfrak{p}_{13,4}, \mathfrak{p}_{5,1}, \mathfrak{p}_{5,2}, \mathfrak{p}_{37,1}, \mathfrak{p}_{37,2}, \mathfrak{p}_{37,3}, \mathfrak{p}_{37,4}, \mathfrak{p}_{61,1}, \mathfrak{p}_{61,2}, \mathfrak{p}_{61,3}, \mathfrak{p}_{73,1}, \mathfrak{p}_{73,3}, \mathfrak{p}_{73,4}, \mathfrak{p}_{97,1}, \mathfrak{p}_{97,2}, \mathfrak{p}_{97,4}, \mathfrak{p}_{109,1}, \mathfrak{p}_{109,2}, \mathfrak{p}_{109,4}, \mathfrak{p}_{181,1}, \mathfrak{p}_{193,1}, \mathfrak{p}_{229,3}, \mathfrak{p}_{17,1}, \mathfrak{p}_{313,1}, \mathfrak{p}_{313,4}, \mathfrak{p}_{373,1}, \mathfrak{p}_{409,1}, \mathfrak{p}_{1321,1}\}$, where $\mathfrak{p}_{1321,1}$ is generated by the element $-3t^3 - 8t^2 - t + 3$, satisfy the conditions for Livné's theorem, and therefore suffice to prove isomorphism of the full representations.

Class 2257

- The level $\mathfrak{n} = \mathfrak{p}_{37,1}\mathfrak{p}_{61,2}$, and the residual representation attached to the corresponding elliptic curve has image isomorphic to S_3.
- The modulus $\mathfrak{m} = \mathfrak{p}_2^5\mathfrak{p}_{37,1}\mathfrak{p}_{61,2}$, and the corresponding ray class group $Cl(\mathcal{O}_F, \mathfrak{m})$ is isomorphic to $\mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z})^3$.
- The primes $\{\mathfrak{p}_{13,1}, \mathfrak{p}_{13,2}, \mathfrak{p}_{13,4}, \mathfrak{p}_{5,1}\}$ suffice to show that L_π can contain no quadratic extension of F other than F_E, while the prime $\mathfrak{p}_3$ suffices to show that L_π cannot be a cubic extension of F.
- The modulus $\mathfrak{m}_E = \mathfrak{q}_2\mathfrak{q}_{37}\mathfrak{q}_{61}$, where the primes $\mathfrak{q}_i$ divide $2\mathfrak{n}\mathcal{O}_{F_E}$, and the corresponding ray class group $Cl(\mathcal{O}_{F_E}, \mathfrak{m}_E)$ is isomorphic to $(\mathbb{Z}/3\mathbb{Z})^3$.
- The prime $\mathfrak{p}_3$ suffices to deduce that the residual representations are isomorphic.
- The modulus $\mathfrak{m}_{L_E} = \mathfrak{r}_{2,1}^9\mathfrak{r}_{2,2}^9\mathfrak{r}_{2,3}^9\mathfrak{r}_{37,1}\mathfrak{r}_{37,2}\mathfrak{r}_{37,3}\mathfrak{r}_{61,1}\mathfrak{r}_{61,2}\mathfrak{r}_{61,3}$, where the primes $\mathfrak{r}_{i,j}$ divide $2\mathfrak{n}\mathcal{O}_{L_E}$, and the corresponding ray class group $Cl(\mathcal{O}_{L_E}, \mathfrak{m}_{L_E})$ is isomorphic to $\mathbb{Z}/24\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z} \times (\mathbb{Z}/4\mathbb{Z})^5 \times (\mathbb{Z}/2\mathbb{Z})^{14}$.
- The kernels V_σ, V_τ and W_σ are 14-, 9-, and 7-dimensional respectively, and the intersections $V_\sigma \cap V_\tau$ and $W_\sigma \cap V_\tau$ are a 5- and a 7-dimensional subspace of $(\mathbb{Z}/2\mathbb{Z})^{21}$ respectively. The set of primes $\{\mathfrak{p}_3,\ \mathfrak{p}_{13,1},\ \mathfrak{p}_{13,2},\ \mathfrak{p}_{13,3},\ \mathfrak{p}_{13,4},\ \mathfrak{p}_{5,1},\ \mathfrak{p}_{37,3},\ \mathfrak{p}_{61,1},\ \mathfrak{p}_{97,1},\ \mathfrak{p}_{97,3},\ \mathfrak{p}_{109,3},\ \mathfrak{p}_{193,1}\}$ suffice to prove isomorphism of the full representations.

Class 2452

- The level $\mathfrak{n} = \mathfrak{p}_2\mathfrak{p}_{613,3}$, and the residual representation attached to the corresponding elliptic curve has image isomorphic to S_3.
- The modulus $\mathfrak{m} = \mathfrak{p}_2^5\mathfrak{p}_{613,3}$, and the corresponding ray class group $Cl(\mathcal{O}_F, \mathfrak{m})$ is isomorphic to $\mathbb{Z}/12\mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z})^3$.
- The primes $\{\mathfrak{p}_3, \mathfrak{p}_{13,1}, \mathfrak{p}_{5,2}\}$ suffice to show that L_π can contain no quadratic extension of F other than F_E, while the prime $\mathfrak{p}_{13,1}$ suffices to show that L_π cannot be a cubic extension of F.
- The modulus $\mathfrak{m}_E = \mathfrak{q}_2\mathfrak{q}_{613,1}\mathfrak{q}_{613,2}$, where the primes $\mathfrak{q}_i$ divide $2\mathfrak{n}\mathcal{O}_{F_E}$, and the corresponding ray class group $Cl(\mathcal{O}_{F_E}, \mathfrak{m}_E)$ is isomorphic to $\mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.
- The prime $\mathfrak{p}_{13,3}$ suffices to deduce that the residual representations are isomorphic.

- The modulus $\mathfrak{m}_{L_E} = \mathfrak{r}_{2,1}^9\mathfrak{r}_{2,2}^9\mathfrak{r}_{2,3}^9\mathfrak{r}_{613,1}\mathfrak{r}_{613,2}$, where the primes $\mathfrak{r}_{i,j}$ divide $2\mathfrak{n}\mathcal{O}_{L_E}$, and the corresponding ray class group $Cl(\mathcal{O}_{L_E}, \mathfrak{m}_{L_E})$ is isomorphic to $\mathbb{Z}/12\mathbb{Z} \times (\mathbb{Z}/4\mathbb{Z})^3 \times (\mathbb{Z}/2\mathbb{Z})^{13}$.
- The kernels V_σ, V_τ and W_σ are 10-, 8-, and 7-dimensional respectively, and the intersections $V_\sigma \cap V_\tau$ and $W_\sigma \cap V_\tau$ are a 4- and a 5-dimensional subspace of $(\mathbb{Z}/2\mathbb{Z})^{17}$ respectively. The set of primes $\{\mathfrak{p}_3,\ \mathfrak{p}_{13,1},\ \mathfrak{p}_{13,3},\ \mathfrak{p}_{5,2},\ \mathfrak{p}_{37,2},\ \mathfrak{p}_{37,3},\ \mathfrak{p}_{7,1},\ \mathfrak{p}_{7,2},\ \mathfrak{p}_{61,3}\}$ suffice to prove isomorphism of the full representations.

Class 2500a

- The level $\mathfrak{n} = \mathfrak{p}_2\mathfrak{p}_{5,1}^2$, and the residual representation attached to the corresponding elliptic curve has image isomorphic to S_3.
- The modulus $\mathfrak{m} = \mathfrak{p}_2^5\mathfrak{p}_{5,1}$, and the corresponding ray class group $Cl(\mathcal{O}_F, \mathfrak{m})$ is isomorphic to $\mathbb{Z}/8\mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z})^3$.
- The primes $\{\mathfrak{p}_{13,3}, \mathfrak{p}_{13,4}, \mathfrak{p}_{37,1}\}$ suffice to show that L_π can contain no quadratic extension of F other than F_E. Since the ray class group admits no cubic characters, L_π cannot be a cubic extension of F.
- The modulus $\mathfrak{m}_E = \mathfrak{q}_2\mathfrak{q}_{5,1}\mathfrak{q}_{5,2}$, where the primes $\mathfrak{q}_i$ divide $2\mathfrak{n}\mathcal{O}_{F_E}$, and the corresponding ray class group $Cl(\mathcal{O}_{F_E}, \mathfrak{m}_E)$ is isomorphic to $\mathbb{Z}/3\mathbb{Z}$.
- Since this class group admits only a single cubic character, the only possible cubic extension of F_π must be L_E, and we deduce that the residual representations are isomorphic.
- The modulus $\mathfrak{m}_{L_E} = \mathfrak{r}_{2,1}^9\mathfrak{r}_{2,2}^9\mathfrak{r}_{2,3}^9\mathfrak{r}_{5,1}\mathfrak{r}_{5,2}$, where the primes $\mathfrak{r}_{i,j}$ divide $2\mathfrak{n}\mathcal{O}_{L_E}$, and the corresponding ray class group $Cl(\mathcal{O}_{L_E}, \mathfrak{m}_{L_E})$ is isomorphic to $\mathbb{Z}/8\mathbb{Z} \times (\mathbb{Z}/4\mathbb{Z})^3 \times (\mathbb{Z}/2\mathbb{Z})^{13}$.
- The kernels V_σ, V_τ and W_σ are 10-, 7-, and 7-dimensional respectively, and the intersections $V_\sigma \cap V_\tau$ and $W_\sigma \cap V_\tau$ are a 4- and a 6-dimensional subspace of $(\mathbb{Z}/2\mathbb{Z})^{13}$ respectively. The set of primes $\{\mathfrak{p}_{13,1},\ \mathfrak{p}_{13,3},\ \mathfrak{p}_{5,2},\ \mathfrak{p}_{37,1},\ \mathfrak{p}_{37,2},\ \mathfrak{p}_{37,3},\ \mathfrak{p}_{61,3}\}$ suffice to prove isomorphism of the full representations.

Class 2977

- The level $\mathfrak{n} = \mathfrak{p}_{13,3}\mathfrak{p}_{229,4}$, and the residual representation attached to the corresponding elliptic curve has trivial image.
- The modulus $\mathfrak{m} = \mathfrak{p}_2^5\mathfrak{p}_{13,3}\mathfrak{p}_{229,4}$, and the corresponding ray class group $Cl(\mathcal{O}_F, \mathfrak{m})$ is isomorphic to $\mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z})^3$.
- The primes $\{\mathfrak{p}_{13,1}, \mathfrak{p}_{13,2}, \mathfrak{p}_{5,2}\}$ suffice to prove isomorphism of the residual representations.

- The primes $\{\mathfrak{p}_3,\ \mathfrak{p}_{13,1},\ \mathfrak{p}_{13,2},\ \mathfrak{p}_{13,4},\ \mathfrak{p}_{5,1},\ \mathfrak{p}_{5,2},\ \mathfrak{p}_{37,1},\ \mathfrak{p}_{37,2},\ \mathfrak{p}_{37,3},\ \mathfrak{p}_{37,4},\ \mathfrak{p}_{7,2},\ \mathfrak{p}_{61,1},\ \mathfrak{p}_{61,2},\ \mathfrak{p}_{73,1},\ \mathfrak{p}_{73,2},\ \mathfrak{p}_{73,3},\ \mathfrak{p}_{97,1},\ \mathfrak{p}_{97,2},\ \mathfrak{p}_{109,2},\ \mathfrak{p}_{109,3},\ \mathfrak{p}_{157,2},\ \mathfrak{p}_{157,4},\ \mathfrak{p}_{229,1},\ \mathfrak{p}_{229,2},\ \mathfrak{p}_{241,3},\ \mathfrak{p}_{17,1},\ \mathfrak{p}_{313,1},\ \mathfrak{p}_{19,1},\ \mathfrak{p}_{397,3},\ \mathfrak{p}_{409,2},\ \mathfrak{p}_{409,3}\}$ satisfy the conditions for Livné's theorem, and therefore suffice to prove isomorphism of the full representations.

Class 3328

- The level $\mathfrak{n} = \mathfrak{p}_2^4\mathfrak{p}_{13,4}$, and the residual representation attached to the corresponding elliptic curve has trivial image.
- The modulus $\mathfrak{m} = \mathfrak{p}_2^5\mathfrak{p}_{13,4}$, and the corresponding ray class group $Cl(\mathcal{O}_F, \mathfrak{m})$ is isomorphic to $\mathbb{Z}/4\mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z})^3$.
- For each possible extension F_π of F corresponding to a quadratic character of $Cl(\mathcal{O}_F, \mathfrak{m})$, the ray class group $Cl(\mathcal{O}_{F_\pi}, \mathfrak{m}_\pi)$ admits no cubic characters, and thus we immediately deduce that the residual representations are isomorphic.
- The primes $\{\mathfrak{p}_3,\ \mathfrak{p}_{13,1},\ \mathfrak{p}_{13,2},\ \mathfrak{p}_{13,3},\ \mathfrak{p}_{5,1},\ \mathfrak{p}_{5,2},\ \mathfrak{p}_{37,1},\ \mathfrak{p}_{37,2},\ \mathfrak{p}_{37,4},\ \mathfrak{p}_{61,1},\ \mathfrak{p}_{61,2},\ \mathfrak{p}_{73,1},\ \mathfrak{p}_{73,4},\ \mathfrak{p}_{97,1},\ \mathfrak{p}_{17,1}\}$ satisfy the conditions for Livné's theorem, and therefore suffice to prove isomorphism of the full representations.

Class 3721b

- The level $\mathfrak{n} = \mathfrak{p}_{61,1}\mathfrak{p}_{61,2}$, and the residual representation attached to the corresponding elliptic curve has trivial image.
- The modulus $\mathfrak{m} = \mathfrak{p}_2^5\mathfrak{p}_{61,1}\mathfrak{p}_{61,2}$, and the corresponding ray class group $Cl(\mathcal{O}_F, \mathfrak{m})$ is isomorphic to $\mathbb{Z}/60\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z})^3$.
- The primes $\{\mathfrak{p}_{13,1}, \mathfrak{p}_{13,3}\}$ suffice to prove isomorphism of the residual representations.
- The primes $\{\mathfrak{p}_3,\ \mathfrak{p}_{13,1},\ \mathfrak{p}_{13,2},\ \mathfrak{p}_{13,3},\ \mathfrak{p}_{13,4},\ \mathfrak{p}_{5,1},\ \mathfrak{p}_{37,1},\ \mathfrak{p}_{37,3},\ \mathfrak{p}_{7,1},\ \mathfrak{p}_{7,2},\ \mathfrak{p}_{61,3},\ \mathfrak{p}_{61,4},\ \mathfrak{p}_{73,1},\ \mathfrak{p}_{73,2},\ \mathfrak{p}_{97,1},\ \mathfrak{p}_{97,2},\ \mathfrak{p}_{109,1},\ \mathfrak{p}_{109,3},\ \mathfrak{p}_{157,1},\ \mathfrak{p}_{157,3},\ \mathfrak{p}_{181,1},\ \mathfrak{p}_{181,2},\ \mathfrak{p}_{181,3},\ \mathfrak{p}_{181,4},\ \mathfrak{p}_{193,1},\ \mathfrak{p}_{17,1},\ \mathfrak{p}_{337,1},\ \mathfrak{p}_{19,1},\ \mathfrak{p}_{409,1},\ \mathfrak{p}_{409,3},\ \mathfrak{p}_{601,3}\}$ satisfy the conditions for Livné's theorem, and therefore suffice to prove isomorphism of the full representations.

Class 3844

- The level $\mathfrak{n} = \mathfrak{p}_2\mathfrak{p}_{31,2}$, and the residual representation attached to the corresponding elliptic curve has image isomorphic to S_3.
- The modulus $\mathfrak{m} = \mathfrak{p}_2^5\mathfrak{p}_{31,2}$, and the corresponding ray class group $Cl(\mathcal{O}_F, \mathfrak{m})$ is isomorphic to $\mathbb{Z}/120\mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z})^3$.
- The primes $\{\mathfrak{p}_3, \mathfrak{p}_{13,3}, \mathfrak{p}_{73,2}\}$ suffice to show that L_π can contain no quadratic extension of F other than F_E, while the prime $\mathfrak{p}_{13,1}$ suffices to show that L_π cannot be a cubic extension of F.
- The modulus $\mathfrak{m}_E = \mathfrak{q}_2\mathfrak{q}_{31,1}\mathfrak{q}_{31,2}$, where the primes $\mathfrak{q}_i$ divide $2\mathfrak{n}\mathcal{O}_{F_E}$, and the corresponding ray class group $Cl(\mathcal{O}_{F_E}, \mathfrak{m}_E)$ is isomorphic to $\mathbb{Z}/360\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.
- The prime $\mathfrak{p}_{13,1}$ suffices to deduce that the residual representations are isomorphic.
- The modulus $\mathfrak{m}_{L_E} = \mathfrak{r}_{2,1}^9\mathfrak{r}_{2,2}^9\mathfrak{r}_{2,3}^9\mathfrak{r}_{31,1}\mathfrak{r}_{31,2}$, where the primes $\mathfrak{r}_{i,j}$ divide $2\mathfrak{n}\mathcal{O}_{L_E}$, and the corresponding ray class group $Cl(\mathcal{O}_{L_E}, \mathfrak{m}_{L_E})$ is isomorphic to $\mathbb{Z}/1440\mathbb{Z} \times \mathbb{Z}/48\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z})^{14}$.
- The kernels V_σ, V_τ and W_σ are 10-, 8-, and 7-dimensional respectively, and the intersections $V_\sigma \cap V_\tau$ and $W_\sigma \cap V_\tau$ are a 4- and a 5-dimensional subspace of $(\mathbb{Z}/2\mathbb{Z})^{17}$ respectively. The set of primes $\{\mathfrak{p}_3, \mathfrak{p}_{13,1}, \mathfrak{p}_{13,2}, \mathfrak{p}_{5,1}, \mathfrak{p}_{37,2}, \mathfrak{p}_{61,1}, \mathfrak{p}_{73,2}\}$ suffice to prove isomorphism of the full representations.

Class 4033a

- The level $\mathfrak{n} = \mathfrak{p}_{37,4}\mathfrak{p}_{109,4}$, and the residual representation attached to the corresponding elliptic curve has trivial image.
- The modulus $\mathfrak{m} = \mathfrak{p}_2^5\mathfrak{p}_{37,4}\mathfrak{p}_{109,4}$, and the corresponding ray class group $Cl(\mathcal{O}_F, \mathfrak{m})$ is isomorphic to $\mathbb{Z}/36\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z})^3$.
- The prime $\mathfrak{p}_{13,1}$ suffices to prove isomorphism of the residual representations.
- The primes $\{\mathfrak{p}_3, \mathfrak{p}_{13,1}, \mathfrak{p}_{13,2}, \mathfrak{p}_{13,3}, \mathfrak{p}_{13,4}, \mathfrak{p}_{5,1}, \mathfrak{p}_{5,2}, \mathfrak{p}_{37,1}, \mathfrak{p}_{37,2}, \mathfrak{p}_{37,3}, \mathfrak{p}_{7,1}, \mathfrak{p}_{61,1}, \mathfrak{p}_{61,3}, \mathfrak{p}_{61,4}, \mathfrak{p}_{73,1}, \mathfrak{p}_{73,2}, \mathfrak{p}_{73,3}, \mathfrak{p}_{73,4}, \mathfrak{p}_{97,1}, \mathfrak{p}_{97,2}, \mathfrak{p}_{97,3}, \mathfrak{p}_{109,1}, \mathfrak{p}_{109,2}, \mathfrak{p}_{157,4}, \mathfrak{p}_{277,1}, \mathfrak{p}_{17,1}, \mathfrak{p}_{17,2}, \mathfrak{p}_{337,4}, \mathfrak{p}_{349,2}, \mathfrak{p}_{373,1}, \mathfrak{p}_{409,3}\}$ satisfy the conditions for Livné's theorem, and therefore suffice to prove isomorphism of the full representations.

Class 4033b

- The level $\mathfrak{n} = \mathfrak{p}_{37,4}\mathfrak{p}_{109,3}$, and the residual representation attached to the corresponding elliptic curve has trivial image.
- The modulus $\mathfrak{m} = \mathfrak{p}_2^5\mathfrak{p}_{37,4}\mathfrak{p}_{109,3}$, and the corresponding ray class group $Cl(\mathcal{O}_F, \mathfrak{m})$ is isomorphic to $\mathbb{Z}/36\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z})^3$.
- The primes $\{\mathfrak{p}_3, \mathfrak{p}_{13,2}\}$ suffice to prove isomorphism of the residual representations.
- The primes $\{\mathfrak{p}_3,\ \mathfrak{p}_{13,1},\ \mathfrak{p}_{13,2},\ \mathfrak{p}_{13,3},\ \mathfrak{p}_{13,4},\ \mathfrak{p}_{5,1},\ \mathfrak{p}_{5,2},\ \mathfrak{p}_{37,1},\ \mathfrak{p}_{37,2},\ \mathfrak{p}_{37,3},\ \mathfrak{p}_{7,1},\ \mathfrak{p}_{61,1},\ \mathfrak{p}_{61,2},\ \mathfrak{p}_{61,3},\ \mathfrak{p}_{61,4},\ \mathfrak{p}_{73,1},\ \mathfrak{p}_{73,2},\ \mathfrak{p}_{73,3},\ \mathfrak{p}_{73,4},\ \mathfrak{p}_{97,1},\ \mathfrak{p}_{97,2},\ \mathfrak{p}_{97,3},\ \mathfrak{p}_{109,1},\ \mathfrak{p}_{109,2},\ \mathfrak{p}_{109,4},\ \mathfrak{p}_{157,4},\ \mathfrak{p}_{17,2},\ \mathfrak{p}_{313,4},\ \mathfrak{p}_{373,1},\ \mathfrak{p}_{409,2},\ \mathfrak{p}_{409,3}\}$ satisfy the conditions for Livné's theorem, and therefore suffice to prove isomorphism of the full representations.

Class 4057

- The level $\mathfrak{n} = \mathfrak{p}_{4057,1}$, which is generated by the element $6t^3 + 2t^2 - 9t - 2$, and the residual representation attached to the corresponding elliptic curve has image isomorphic to S_3.
- The modulus $\mathfrak{m} = \mathfrak{p}_2^5\mathfrak{p}_{4057,1}$, and the corresponding ray class group $Cl(\mathcal{O}_F, \mathfrak{m})$ is isomorphic to $\mathbb{Z}/8\mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z})^3$.
- The primes $\{\mathfrak{p}_{13,1}, \mathfrak{p}_{13,3}, \mathfrak{p}_{5,2}\}$ suffice to show that L_π can contain no quadratic extension of F other than F_E. Since the ray class group admits no cubic characters, L_π cannot be a cubic extension of F.
- The modulus $\mathfrak{m}_E = \mathfrak{q}_2\mathfrak{q}_{4057,1}\mathfrak{q}_{4057,2}$, where the primes $\mathfrak{q}_i$ divide $2\mathfrak{n}\mathcal{O}_{F_E}$, and the corresponding ray class group $Cl(\mathcal{O}_{F_E}, \mathfrak{m}_E)$ is isomorphic to $\mathbb{Z}/6\mathbb{Z}\times$ $\mathbb{Z}/2\mathbb{Z}$.
- Since this class group admits only a single cubic character, the only possible cubic extension of F_π must be L_E, and we deduce that the residual representations are isomorphic.
- The modulus $\mathfrak{m}_{L_E} = \mathfrak{r}_{2,1}^9\mathfrak{r}_{2,2}^9\mathfrak{r}_{2,3}^9\mathfrak{r}_{4057,1}\mathfrak{r}_{4057,2}$, where the primes $\mathfrak{r}_{i,j}$ divide $2\mathfrak{n}\mathcal{O}_{L_E}$, and the corresponding ray class group $Cl(\mathcal{O}_{L_E}, \mathfrak{m}_{L_E})$ is isomorphic to $(\mathbb{Z}/8\mathbb{Z})^2 \times (\mathbb{Z}/4\mathbb{Z})^4 \times (\mathbb{Z}/2\mathbb{Z})^{11}$.
- The kernels V_σ, V_τ and W_σ are 10-, 8-, and 7-dimensional respectively, and the intersections $V_\sigma \cap V_\tau$ and $W_\sigma \cap V_\tau$ are a 4- and a 5-dimensional subspace of $(\mathbb{Z}/2\mathbb{Z})^{17}$ respectively. The set of primes $\{\mathfrak{p}_3,\ \mathfrak{p}_{13,1},\ \mathfrak{p}_{13,2},\ \mathfrak{p}_{13,3},\ \mathfrak{p}_{5,1},\ \mathfrak{p}_{5,2},\ \mathfrak{p}_{37,2},\ \mathfrak{p}_{61,2},\ \mathfrak{p}_{61,4}\}$ suffice to prove isomorphism of the full representations.

Class 4069

- The level $\mathfrak{n} = \mathfrak{p}_{13,3}\mathfrak{p}_{313,4}$, and the residual representation attached to the corresponding elliptic curve has image isomorphic to S_3.
- The modulus $\mathfrak{m} = \mathfrak{p}_2^5\mathfrak{p}_{13,3}\mathfrak{p}_{313,4}$, and the corresponding ray class group $Cl(\mathcal{O}_F, \mathfrak{m})$ is isomorphic to $\mathbb{Z}/24\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z})^3$.
- The primes $\{\mathfrak{p}_{13,1}, \mathfrak{p}_{13,2}, \mathfrak{p}_{13,4}, \mathfrak{p}_{5,2}\}$ suffice to show that L_π can contain no quadratic extension of F other than F_E, while the prime $\mathfrak{p}_{37,2}$ suffices to show that L_π cannot be a cubic extension of F.
- The modulus $\mathfrak{m}_E = \mathfrak{q}_2\mathfrak{q}_{13}\mathfrak{q}_{313}$, where the primes $\mathfrak{q}_i$ divide $2\mathfrak{n}\mathcal{O}_{F_E}$, and the corresponding ray class group $Cl(\mathcal{O}_{F_E}, \mathfrak{m}_E)$ is isomorphic to $(\mathbb{Z}/3\mathbb{Z})^2$.
- The prime $\mathfrak{p}_{37,2}$ suffices to deduce that the residual representations are isomorphic.
- The modulus $\mathfrak{m}_{L_E} = \mathfrak{r}_{2,1}^9\mathfrak{r}_{2,2}^9\mathfrak{r}_{2,3}^9\mathfrak{r}_{13,1}\mathfrak{r}_{13,2}\mathfrak{r}_{13,3}\mathfrak{r}_{313,1}\mathfrak{r}_{313,2}\mathfrak{r}_{313,3}$, where the primes $\mathfrak{r}_{i,j}$ divide $2\mathfrak{n}\mathcal{O}_{L_E}$, and the corresponding ray class group $Cl(\mathcal{O}_{L_E}, \mathfrak{m}_{L_E})$ is isomorphic to $\mathbb{Z}/24\mathbb{Z} \times (\mathbb{Z}/8\mathbb{Z})^3 \times (\mathbb{Z}/4\mathbb{Z})^3 \times (\mathbb{Z}/2\mathbb{Z})^{14}$.
- The kernels V_σ, V_τ and W_σ are 14-, 9-, and 7-dimensional respectively, and the intersections $V_\sigma \cap V_\tau$ and $W_\sigma \cap V_\tau$ are a 5- and a 7-dimensional subspace of $(\mathbb{Z}/2\mathbb{Z})^{21}$ respectively. The set of primes $\{\mathfrak{p}_{13,1}, \mathfrak{p}_{13,2}, \mathfrak{p}_{13,4}, \mathfrak{p}_{5,2}, \mathfrak{p}_{37,1}, \mathfrak{p}_{37,2}, \mathfrak{p}_{37,3}, \mathfrak{p}_{61,3}, \mathfrak{p}_{73,2}, \mathfrak{p}_{97,2}, \mathfrak{p}_{97,3}, \mathfrak{p}_{109,3}\}$ suffice to prove isomorphism of the full representations.

Class 4225b

- The level $\mathfrak{n} = \mathfrak{p}_{13,2}^2\mathfrak{p}_{5,1}$, and the residual representation attached to the corresponding elliptic curve has trivial image.
- The modulus $\mathfrak{m} = \mathfrak{p}_2^5\mathfrak{p}_{13,2}\mathfrak{p}_{5,1}$, and the corresponding ray class group $Cl(\mathcal{O}_F, \mathfrak{m})$ is isomorphic to $\mathbb{Z}/24\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z})^3$.
- The primes $\{\mathfrak{p}_3, \mathfrak{p}_{13,3}\}$ suffice to prove isomorphism of the residual representations.
- The primes $\{\mathfrak{p}_3, \mathfrak{p}_{13,1}, \mathfrak{p}_{13,3}, \mathfrak{p}_{13,4}, \mathfrak{p}_{5,2}, \mathfrak{p}_{37,1}, \mathfrak{p}_{37,2}, \mathfrak{p}_{37,3}, \mathfrak{p}_{37,4}, \mathfrak{p}_{7,1}, \mathfrak{p}_{7,2}, \mathfrak{p}_{61,1}, \mathfrak{p}_{61,3}, \mathfrak{p}_{61,4}, \mathfrak{p}_{73,1}, \mathfrak{p}_{73,2}, \mathfrak{p}_{73,3}, \mathfrak{p}_{97,2}, \mathfrak{p}_{97,3}, \mathfrak{p}_{109,3}, \mathfrak{p}_{11,1}, \mathfrak{p}_{157,2}, \mathfrak{p}_{157,4}, \mathfrak{p}_{181,4}, \mathfrak{p}_{193,4}, \mathfrak{p}_{229,1}, \mathfrak{p}_{229,2}, \mathfrak{p}_{17,1}, \mathfrak{p}_{313,3}, \mathfrak{p}_{409,1}, \mathfrak{p}_{409,2}\}$ satisfy the conditions for Livné's theorem, and therefore suffice to prove isomorphism of the full representations.

Class 4516

- The level $\mathfrak{n} = \mathfrak{p}_2\mathfrak{p}_{1129,1}$, where $\mathfrak{p}_{1129,1}$ is generated by $6t^3-2t^2-3t-1$, and the residual representation attached to the corresponding elliptic curve has image isomorphic to S_3.
- The modulus $\mathfrak{m} = \mathfrak{p}_2^5\mathfrak{p}_{1129,1}$, and the corresponding ray class group $Cl(\mathcal{O}_F, \mathfrak{m})$ is isomorphic to $\mathbb{Z}/24\mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z})^3$.
- The primes $\{\mathfrak{p}_3, \mathfrak{p}_{13,2}, \mathfrak{p}_{37,3}\}$ suffice to show that L_π can contain no quadratic extension of F other than F_E, while the prime $\mathfrak{p}_{13,3}$ suffices to show that L_π cannot be a cubic extension of F.
- The modulus $\mathfrak{m}_E = \mathfrak{q}_2\mathfrak{q}_{1129}$, where the primes $\mathfrak{q}_i$ divide $2\mathfrak{n}\mathcal{O}_{F_E}$, and the corresponding ray class group $Cl(\mathcal{O}_{F_E}, \mathfrak{m}_E)$ is isomorphic to $(\mathbb{Z}/3\mathbb{Z})^2$.
- The prime $\mathfrak{p}_{13,3}$ suffices to deduce that the residual representations are isomorphic.
- The modulus $\mathfrak{m}_{L_E} = \mathfrak{r}_{2,1}^9\mathfrak{r}_{2,2}^9\mathfrak{r}_{2,3}^9\mathfrak{r}_{1129,1}\mathfrak{r}_{1129,2}\mathfrak{r}_{1129,3}$, where the primes $\mathfrak{r}_{i,j}$ divide $2\mathfrak{n}\mathcal{O}_{L_E}$, and the corresponding ray class group $Cl(\mathcal{O}_{L_E}, \mathfrak{m}_{L_E})$ is isomorphic to $\mathbb{Z}/48\mathbb{Z} \times (\mathbb{Z}/4\mathbb{Z})^4 \times (\mathbb{Z}/2\mathbb{Z})^{13}$.
- The kernels V_σ, V_τ and W_σ are 12-, 8-, and 6-dimensional respectively, and the intersections $V_\sigma \cap V_\tau$ and $W_\sigma \cap V_\tau$ are a 4- and a 6-dimensional subspace of $(\mathbb{Z}/2\mathbb{Z})^{18}$ respectively. The set of primes $\{\mathfrak{p}_3, \mathfrak{p}_{13,1}, \mathfrak{p}_{13,2}, \mathfrak{p}_{13,3}, \mathfrak{p}_{5,1}, \mathfrak{p}_{5,2}, \mathfrak{p}_{37,1}, \mathfrak{p}_{37,3}, \mathfrak{p}_{7,1}, \mathfrak{p}_{73,1}\}$ suffice to prove isomorphism of the full representations.

Class 4672

- The level $\mathfrak{n} = \mathfrak{p}_2^3\mathfrak{p}_{73,1}$, and the residual representation attached to the corresponding elliptic curve has trivial image.
- The modulus $\mathfrak{m} = \mathfrak{p}_2^5\mathfrak{p}_{73,1}$, and the corresponding ray class group $Cl(\mathcal{O}_F, \mathfrak{m})$ is isomorphic to $\mathbb{Z}/8\mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z})^3$.
- For each possible extension F_π of F corresponding to a quadratic character of $Cl(\mathcal{O}_F, \mathfrak{m})$, the ray class group $Cl(\mathcal{O}_{F_\pi}, \mathfrak{m}_\pi)$ admits no cubic characters, and thus we immediately deduce that the residual representations are isomorphic.
- The primes $\{\mathfrak{p}_3, \mathfrak{p}_{13,1}, \mathfrak{p}_{13,2}, \mathfrak{p}_{13,3}, \mathfrak{p}_{13,4}, \mathfrak{p}_{5,1}, \mathfrak{p}_{5,2}, \mathfrak{p}_{37,3}, \mathfrak{p}_{61,3}, \mathfrak{p}_{61,4}, \mathfrak{p}_{73,2}, \mathfrak{p}_{73,3}, \mathfrak{p}_{97,2}, \mathfrak{p}_{109,1}, \mathfrak{p}_{17,2}\}$ satisfy the conditions for Livné's theorem, and therefore suffice to prove isomorphism of the full representations.

Class 4852

- The level $\mathfrak{n} = \mathfrak{p}_2\mathfrak{p}_{1213,1}$, where $\mathfrak{p}_{1213,1}$ is generated by $-t^3+2t^2+6t-2$, and the residual representation attached to the corresponding elliptic curve has image isomorphic to S_3.
- The modulus $\mathfrak{m} = \mathfrak{p}_2^5\mathfrak{p}_{1213,1}$, and the corresponding ray class group $Cl(\mathcal{O}_F, \mathfrak{m})$ is isomorphic to $\mathbb{Z}/12\mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z})^3$.
- The primes $\{\mathfrak{p}_3, \mathfrak{p}_{13,1}, \mathfrak{p}_{13,2}\}$ suffice to show that L_π can contain no quadratic extension of F other than F_E, while the prime $\mathfrak{p}_{13,3}$ suffices to show that L_π cannot be a cubic extension of F.
- The modulus $\mathfrak{m}_E = \mathfrak{q}_2\mathfrak{q}_{1213}$, where the primes $\mathfrak{q}_i$ divide $2\mathfrak{n}\mathcal{O}_{F_E}$, and the corresponding ray class group $Cl(\mathcal{O}_{F_E}, \mathfrak{m}_E)$ is isomorphic to $(\mathbb{Z}/3\mathbb{Z})^2$.
- The prime $\mathfrak{p}_{13,3}$ suffices to deduce that the residual representations are isomorphic.
- The modulus $\mathfrak{m}_{L_E} = \mathfrak{r}_{2,1}^9\mathfrak{r}_{2,2}^9\mathfrak{r}_{2,3}^9\mathfrak{r}_{1213,1}\mathfrak{r}_{1213,2}\mathfrak{r}_{1213,3}$, where the primes $\mathfrak{r}_{i,j}$ divide $2\mathfrak{n}\mathcal{O}_{L_E}$, and the corresponding ray class group $Cl(\mathcal{O}_{L_E}, \mathfrak{m}_{L_E})$ is isomorphic to $\mathbb{Z}/24\mathbb{Z} \times (\mathbb{Z}/4\mathbb{Z})^3 \times (\mathbb{Z}/2\mathbb{Z})^{14}$.
- The kernels V_σ, V_τ and W_σ are 12-, 8-, and 6-dimensional respectively, and the intersections $V_\sigma \cap V_\tau$ and $W_\sigma \cap V_\tau$ are a 4- and a 6-dimensional subspace of $(\mathbb{Z}/2\mathbb{Z})^{18}$ respectively. The set of primes $\{\mathfrak{p}_3, \mathfrak{p}_{13,1}, \mathfrak{p}_{13,2}, \mathfrak{p}_{5,1}, \mathfrak{p}_{5,2}, \mathfrak{p}_{37,3}, \mathfrak{p}_{61,2}, \mathfrak{p}_{61,3}, \mathfrak{p}_{73,2}, \mathfrak{p}_{97,3}\}$ suffice to prove isomorphism of the full representations.

Class 5317

- The level $\mathfrak{n} = \mathfrak{p}_{13,4}\mathfrak{p}_{409,3}$, and the residual representation attached to the corresponding elliptic curve has trivial image.
- The modulus $\mathfrak{m} = \mathfrak{p}_2^5\mathfrak{p}_{13,4}\mathfrak{p}_{409,3}$, and the corresponding ray class group $Cl(\mathcal{O}_F, \mathfrak{m})$ is isomorphic to $\mathbb{Z}/24\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z})^3$.
- The primes $\{\mathfrak{p}_3, \mathfrak{p}_{13,2}\}$ suffice to prove isomorphism of the residual representations.
- The primes $\{\mathfrak{p}_3, \mathfrak{p}_{13,1}, \mathfrak{p}_{13,2}, \mathfrak{p}_{13,3}, \mathfrak{p}_{5,1}, \mathfrak{p}_{5,2}, \mathfrak{p}_{37,1}, \mathfrak{p}_{37,2}, \mathfrak{p}_{37,4}, \mathfrak{p}_{7,2}, \mathfrak{p}_{61,1}, \mathfrak{p}_{61,2}, \mathfrak{p}_{61,3}, \mathfrak{p}_{73,1}, \mathfrak{p}_{73,2}, \mathfrak{p}_{73,4}, \mathfrak{p}_{97,1}, \mathfrak{p}_{97,3}, \mathfrak{p}_{97,4}, \mathfrak{p}_{109,3}, \mathfrak{p}_{157,2}, \mathfrak{p}_{157,3}, \mathfrak{p}_{181,1}, \mathfrak{p}_{181,2}, \mathfrak{p}_{193,2}, \mathfrak{p}_{277,4}, \mathfrak{p}_{17,1}, \mathfrak{p}_{313,2}, \mathfrak{p}_{373,3}, \mathfrak{p}_{409,1}, \mathfrak{p}_{457,1}\}$ satisfy the conditions for Livné's theorem, and therefore suffice to prove isomorphism of the full representations.

Class 5473

- The level $\mathfrak{n} = \mathfrak{p}_{13,4}\mathfrak{p}_{421,2}$, and the residual representation attached to the corresponding elliptic curve has trivial image.
- The modulus $\mathfrak{m} = \mathfrak{p}_2^5\mathfrak{p}_{13,4}\mathfrak{p}_{421,2}$, and the corresponding ray class group $Cl(\mathcal{O}_F, \mathfrak{m})$ is isomorphic to $\mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z})^3$.
- The primes $\{\mathfrak{p}_3, \mathfrak{p}_{13,1}\}$ suffice to prove isomorphism of the residual representations.
- The primes $\{\mathfrak{p}_3,\ \mathfrak{p}_{13,1},\ \mathfrak{p}_{13,2},\ \mathfrak{p}_{13,3},\ \mathfrak{p}_{5,1},\ \mathfrak{p}_{5,2},\ \mathfrak{p}_{37,1},\ \mathfrak{p}_{37,2},\ \mathfrak{p}_{37,3},\ \mathfrak{p}_{37,4},\ \mathfrak{p}_{61,1},\ \mathfrak{p}_{61,2},\ \mathfrak{p}_{73,1},\ \mathfrak{p}_{73,2},\ \mathfrak{p}_{73,4},\ \mathfrak{p}_{97,1},\ \mathfrak{p}_{97,3},\ \mathfrak{p}_{97,4},\ \mathfrak{p}_{109,1},\ \mathfrak{p}_{109,3},\ \mathfrak{p}_{109,4},\ \mathfrak{p}_{157,1},\ \mathfrak{p}_{157,2},\ \mathfrak{p}_{181,4},\ \mathfrak{p}_{193,2},\ \mathfrak{p}_{17,1},\ \mathfrak{p}_{313,1},\ \mathfrak{p}_{313,3},\ \mathfrak{p}_{349,1},\ \mathfrak{p}_{409,2},\ \mathfrak{p}_{457,4}\}$ satisfy the conditions for Livné's theorem, and therefore suffice to prove isomorphism of the full representations.

$\mathfrak{p}$	$\mathfrak{p}_{13,1}$	$\mathfrak{p}_{13,2}$	$\mathfrak{p}_{13,3}$	$\mathfrak{p}_{13,4}$	$\mathfrak{p}_{5,1}$	$\mathfrak{p}_{5,2}$	$\mathfrak{p}_{37,1}$	$\mathfrak{p}_{37,2}$
$a_{\mathfrak{p}}$	-6	4	4	-6	-4	-4	-2	-2
$\mathfrak{p}$	$\mathfrak{p}_{37,3}$	$\mathfrak{p}_{37,4}$	$\mathfrak{p}_{7,1}$	$\mathfrak{p}_{61,2}$	$\mathfrak{p}_{61,3}$	$\mathfrak{p}_{73,1}$	$\mathfrak{p}_{73,2}$	$\mathfrak{p}_{97,1}$
$a_{\mathfrak{p}}$	-2	-2	10	2	2	14	4	-2
$\mathfrak{p}$	$\mathfrak{p}_{97,2}$	$\mathfrak{p}_{109,2}$	$\mathfrak{p}_{109,3}$	$\mathfrak{p}_{11,1}$	$\mathfrak{p}_{181,2}$	$\mathfrak{p}_{181,3}$	$\mathfrak{p}_{193,1}$	$\mathfrak{p}_{17,1}$
$a_{\mathfrak{p}}$	8	10	10	2	-8	-8	-26	-20
$\mathfrak{p}$	$\mathfrak{p}_{313,1}$	$\mathfrak{p}_{337,1}$	$\mathfrak{p}_{349,1}$	$\mathfrak{p}_{349,4}$	$\mathfrak{p}_{19,1}$	$\mathfrak{p}_{409,2}$	$\mathfrak{p}_{23,1}$	$\mathfrak{p}_{601,2}$
$a_{\mathfrak{p}}$	34	-22	-30	-30	2	30	10	22

Eigenvalues $a_{\mathfrak{p}}$ of the Hecke operators $T_{\mathfrak{p}}$ on class 441

$\mathfrak{p}$	$\mathfrak{p}_3$	$\mathfrak{p}_{13,1}$	$\mathfrak{p}_{13,2}$	$\mathfrak{p}_{13,3}$	$\mathfrak{p}_{13,4}$	$\mathfrak{p}_{5,1}$	$\mathfrak{p}_{37,1}$	$\mathfrak{p}_{37,3}$
$a_{\mathfrak{p}}$	0	4	4	-6	-6	6	-2	-2
$\mathfrak{p}$	$\mathfrak{p}_{7,1}$	$\mathfrak{p}_{73,1}$	$\mathfrak{p}_{73,3}$	$\mathfrak{p}_{97,3}$	$\mathfrak{p}_{109,2}$	$\mathfrak{p}_{109,4}$	$\mathfrak{p}_{457,1}$	
$a_{\mathfrak{p}}$	-10	4	-6	-2	10	10	18	

Eigenvalues $a_{\mathfrak{p}}$ of the Hecke operators $T_{\mathfrak{p}}$ on class 1156

$\mathfrak{p}$	$\mathfrak{p}_3$	$\mathfrak{p}_{13,1}$	$\mathfrak{p}_{13,2}$	$\mathfrak{p}_{13,4}$	$\mathfrak{p}_{5,1}$	$\mathfrak{p}_{5,2}$	$\mathfrak{p}_{37,1}$	$\mathfrak{p}_{37,2}$
$a_{\mathfrak{p}}$	-2	2	2	-4	-4	-10	2	2
$\mathfrak{p}$	$\mathfrak{p}_{37,3}$	$\mathfrak{p}_{37,4}$	$\mathfrak{p}_{61,1}$	$\mathfrak{p}_{61,2}$	$\mathfrak{p}_{61,3}$	$\mathfrak{p}_{73,1}$	$\mathfrak{p}_{73,3}$	$\mathfrak{p}_{73,4}$
$a_{\mathfrak{p}}$	2	8	2	-10	8	-16	14	-10
$\mathfrak{p}$	$\mathfrak{p}_{97,1}$	$\mathfrak{p}_{97,2}$	$\mathfrak{p}_{97,4}$	$\mathfrak{p}_{109,1}$	$\mathfrak{p}_{109,2}$	$\mathfrak{p}_{109,4}$	$\mathfrak{p}_{181,1}$	$\mathfrak{p}_{193,1}$
$a_{\mathfrak{p}}$	2	2	-4	2	2	-10	2	-22
$\mathfrak{p}$	$\mathfrak{p}_{229,3}$	$\mathfrak{p}_{17,1}$	$\mathfrak{p}_{313,1}$	$\mathfrak{p}_{313,4}$	$\mathfrak{p}_{373,1}$	$\mathfrak{p}_{409,1}$	$\mathfrak{p}_{1321,1}$	
$a_{\mathfrak{p}}$	-4	2	-10	14	-10	32	-10	

Eigenvalues $a_{\mathfrak{p}}$ of the Hecke operators $T_{\mathfrak{p}}$ on class 2041

$\mathfrak{p}$	$\mathfrak{p}_3$	$\mathfrak{p}_{13,1}$	$\mathfrak{p}_{13,2}$	$\mathfrak{p}_{13,3}$	$\mathfrak{p}_{13,4}$	$\mathfrak{p}_{5,1}$
$a_{\mathfrak{p}}$	-4	-1	1	-6	-3	1
$\mathfrak{p}$	$\mathfrak{p}_{37,3}$	$\mathfrak{p}_{61,1}$	$\mathfrak{p}_{97,1}$	$\mathfrak{p}_{97,3}$	$\mathfrak{p}_{109,3}$	$\mathfrak{p}_{193,1}$
$a_{\mathfrak{p}}$	-3	-12	0	-10	8	-10

Eigenvalues $a_{\mathfrak{p}}$ of the Hecke operators $T_{\mathfrak{p}}$ on class 2257

$\mathfrak{p}$	$\mathfrak{p}_3$	$\mathfrak{p}_{13,1}$	$\mathfrak{p}_{13,3}$	$\mathfrak{p}_{5,2}$	$\mathfrak{p}_{37,2}$
$a_{\mathfrak{p}}$	1	-4	-4	8	2
$\mathfrak{p}$	$\mathfrak{p}_{37,3}$	$\mathfrak{p}_{7,1}$	$\mathfrak{p}_{7,2}$	$\mathfrak{p}_{61,3}$	
$a_{\mathfrak{p}}$	11	-4	-4	-10	

Eigenvalues $a_{\mathfrak{p}}$ of the Hecke operators $T_{\mathfrak{p}}$ on class 2452

$\mathfrak{p}$	$\mathfrak{p}_{13,1}$	$\mathfrak{p}_{13,3}$	$\mathfrak{p}_{13,4}$	$\mathfrak{p}_{5,2}$
$a_{\mathfrak{p}}$	4	-1	-1	1
$\mathfrak{p}$	$\mathfrak{p}_{37,1}$	$\mathfrak{p}_{37,2}$	$\mathfrak{p}_{37,3}$	$\mathfrak{p}_{61,3}$
$a_{\mathfrak{p}}$	-7	-2	-7	-8

Eigenvalues $a_{\mathfrak{p}}$ of the Hecke operators $T_{\mathfrak{p}}$ on class 2500a

$\mathfrak{p}$	$\mathfrak{p}_3$	$\mathfrak{p}_{13,1}$	$\mathfrak{p}_{13,2}$	$\mathfrak{p}_{13,4}$	$\mathfrak{p}_{5,1}$	$\mathfrak{p}_{5,2}$	$\mathfrak{p}_{37,1}$	$\mathfrak{p}_{37,2}$
$a_{\mathfrak{p}}$	4	2	-4	-4	2	-10	2	-10
$\mathfrak{p}$	$\mathfrak{p}_{37,3}$	$\mathfrak{p}_{37,4}$	$\mathfrak{p}_{7,2}$	$\mathfrak{p}_{61,1}$	$\mathfrak{p}_{61,2}$	$\mathfrak{p}_{73,1}$	$\mathfrak{p}_{73,2}$	$\mathfrak{p}_{73,3}$
$a_{\mathfrak{p}}$	-10	2	8	-10	2	-4	14	2
$\mathfrak{p}$	$\mathfrak{p}_{97,1}$	$\mathfrak{p}_{97,2}$	$\mathfrak{p}_{109,2}$	$\mathfrak{p}_{109,3}$	$\mathfrak{p}_{157,2}$	$\mathfrak{p}_{157,4}$	$\mathfrak{p}_{229,1}$	$\mathfrak{p}_{229,2}$
$a_{\mathfrak{p}}$	2	14	14	-10	2	-16	8	2
$\mathfrak{p}$	$\mathfrak{p}_{241,3}$	$\mathfrak{p}_{17,1}$	$\mathfrak{p}_{313,1}$	$\mathfrak{p}_{19,1}$	$\mathfrak{p}_{397,3}$	$\mathfrak{p}_{409,2}$	$\mathfrak{p}_{409,3}$	
$a_{\mathfrak{p}}$	14	8	-10	2	2	14	2	

Eigenvalues $a_{\mathfrak{p}}$ of the Hecke operators $T_{\mathfrak{p}}$ on class 2977

$\mathfrak{p}$	$\mathfrak{p}_3$	$\mathfrak{p}_{13,1}$	$\mathfrak{p}_{13,2}$	$\mathfrak{p}_{13,3}$	$\mathfrak{p}_{5,1}$	$\mathfrak{p}_{5,2}$	$\mathfrak{p}_{37,1}$	$\mathfrak{p}_{37,2}$
$a_\mathfrak{p}$	2	−2	−2	6	2	−6	−10	−2
$\mathfrak{p}$	$\mathfrak{p}_{37,4}$	$\mathfrak{p}_{61,1}$	$\mathfrak{p}_{61,2}$	$\mathfrak{p}_{73,1}$	$\mathfrak{p}_{73,4}$	$\mathfrak{p}_{97,1}$	$\mathfrak{p}_{17,1}$	
$a_\mathfrak{p}$	6	−2	−2	10	10	18	2	

Eigenvalues $a_\mathfrak{p}$ of the Hecke operators $T_\mathfrak{p}$ on class 3328

$\mathfrak{p}$	$\mathfrak{p}_3$	$\mathfrak{p}_{13,1}$	$\mathfrak{p}_{13,2}$	$\mathfrak{p}_{13,3}$	$\mathfrak{p}_{13,4}$	$\mathfrak{p}_{5,1}$	$\mathfrak{p}_{37,1}$	$\mathfrak{p}_{37,3}$
$a_\mathfrak{p}$	−2	−4	−4	2	2	8	−10	−2
$\mathfrak{p}$	$\mathfrak{p}_{7,1}$	$\mathfrak{p}_{7,2}$	$\mathfrak{p}_{61,3}$	$\mathfrak{p}_{61,4}$	$\mathfrak{p}_{73,1}$	$\mathfrak{p}_{73,2}$	$\mathfrak{p}_{97,1}$	$\mathfrak{p}_{97,2}$
$a_\mathfrak{p}$	2	2	2	2	2	2	14	14
$\mathfrak{p}$	$\mathfrak{p}_{109,1}$	$\mathfrak{p}_{109,3}$	$\mathfrak{p}_{157,1}$	$\mathfrak{p}_{157,3}$	$\mathfrak{p}_{181,1}$	$\mathfrak{p}_{181,2}$	$\mathfrak{p}_{181,3}$	$\mathfrak{p}_{181,4}$
$a_\mathfrak{p}$	−4	−4	−10	−10	2	2	2	2
$\mathfrak{p}$	$\mathfrak{p}_{193,1}$	$\mathfrak{p}_{17,1}$	$\mathfrak{p}_{337,1}$	$\mathfrak{p}_{19,1}$	$\mathfrak{p}_{409,1}$	$\mathfrak{p}_{409,3}$	$\mathfrak{p}_{601,3}$	
$a_\mathfrak{p}$	14	32	2	20	−22	−22	20	

Eigenvalues $a_\mathfrak{p}$ of the Hecke operators $T_\mathfrak{p}$ on class 3721b

$\mathfrak{p}$	$\mathfrak{p}_3$	$\mathfrak{p}_{13,1}$	$\mathfrak{p}_{13,2}$	$\mathfrak{p}_{13,3}$
$a_\mathfrak{p}$	−5	−1	−6	−6
$\mathfrak{p}$	$\mathfrak{p}_{5,1}$	$\mathfrak{p}_{37,2}$	$\mathfrak{p}_{61,1}$	$\mathfrak{p}_{73,2}$
$a_\mathfrak{p}$	1	3	−13	4

Eigenvalues $a_\mathfrak{p}$ of the Hecke operators $T_\mathfrak{p}$ on class 3844

$\mathfrak{p}$	$\mathfrak{p}_3$	$\mathfrak{p}_{13,1}$	$\mathfrak{p}_{13,2}$	$\mathfrak{p}_{13,3}$	$\mathfrak{p}_{13,4}$	$\mathfrak{p}_{5,1}$	$\mathfrak{p}_{5,2}$	$\mathfrak{p}_{37,1}$
$a_\mathfrak{p}$	4	2	−4	2	2	2	−4	2
$\mathfrak{p}$	$\mathfrak{p}_{37,2}$	$\mathfrak{p}_{37,3}$	$\mathfrak{p}_{7,1}$	$\mathfrak{p}_{61,1}$	$\mathfrak{p}_{61,3}$	$\mathfrak{p}_{61,4}$	$\mathfrak{p}_{73,1}$	$\mathfrak{p}_{73,2}$
$a_\mathfrak{p}$	2	2	−4	2	14	−10	2	2
$\mathfrak{p}$	$\mathfrak{p}_{73,3}$	$\mathfrak{p}_{73,4}$	$\mathfrak{p}_{97,1}$	$\mathfrak{p}_{97,2}$	$\mathfrak{p}_{97,3}$	$\mathfrak{p}_{109,1}$	$\mathfrak{p}_{109,2}$	$\mathfrak{p}_{157,4}$
$a_\mathfrak{p}$	2	2	−16	2	14	2	−16	−4
$\mathfrak{p}$	$\mathfrak{p}_{277,1}$	$\mathfrak{p}_{17,1}$	$\mathfrak{p}_{17,2}$	$\mathfrak{p}_{337,4}$	$\mathfrak{p}_{349,2}$	$\mathfrak{p}_{373,1}$	$\mathfrak{p}_{409,3}$	
$a_\mathfrak{p}$	−10	2	2	2	32	14	−10	

Eigenvalues $a_\mathfrak{p}$ of the Hecke operators $T_\mathfrak{p}$ on class 4033a

$\mathfrak{p}$	$\mathfrak{p}_3$	$\mathfrak{p}_{13,1}$	$\mathfrak{p}_{13,2}$	$\mathfrak{p}_{13,3}$	$\mathfrak{p}_{13,4}$	$\mathfrak{p}_{5,1}$	$\mathfrak{p}_{5,2}$	$\mathfrak{p}_{37,1}$
$a_\mathfrak{p}$	−2	−4	2	2	2	−4	2	2
$\mathfrak{p}$	$\mathfrak{p}_{37,2}$	$\mathfrak{p}_{37,3}$	$\mathfrak{p}_{7,1}$	$\mathfrak{p}_{61,1}$	$\mathfrak{p}_{61,2}$	$\mathfrak{p}_{61,3}$	$\mathfrak{p}_{61,4}$	$\mathfrak{p}_{73,1}$
$a_\mathfrak{p}$	2	2	−10	8	−4	8	2	2
$\mathfrak{p}$	$\mathfrak{p}_{73,2}$	$\mathfrak{p}_{73,3}$	$\mathfrak{p}_{73,4}$	$\mathfrak{p}_{97,1}$	$\mathfrak{p}_{97,2}$	$\mathfrak{p}_{97,3}$	$\mathfrak{p}_{109,1}$	$\mathfrak{p}_{109,2}$
$a_\mathfrak{p}$	2	2	−16	−10	8	−10	2	2
$\mathfrak{p}$	$\mathfrak{p}_{109,4}$	$\mathfrak{p}_{157,4}$	$\mathfrak{p}_{17,2}$	$\mathfrak{p}_{313,4}$	$\mathfrak{p}_{373,1}$	$\mathfrak{p}_{409,2}$	$\mathfrak{p}_{409,3}$	
$a_\mathfrak{p}$	2	−10	20	26	−34	2	14	

Eigenvalues $a_\mathfrak{p}$ of the Hecke operators $T_\mathfrak{p}$ on class 4033b

$\mathfrak{p}$	$\mathfrak{p}_3$	$\mathfrak{p}_{13,1}$	$\mathfrak{p}_{13,2}$	$\mathfrak{p}_{13,3}$	$\mathfrak{p}_{5,1}$
$a_\mathfrak{p}$	−2	−4	−1	−4	−5
$\mathfrak{p}$	$\mathfrak{p}_{5,2}$	$\mathfrak{p}_{37,2}$	$\mathfrak{p}_{61,2}$	$\mathfrak{p}_{61,4}$	
$a_\mathfrak{p}$	−2	4	−13	10	

Eigenvalues $a_\mathfrak{p}$ of the Hecke operators $T_\mathfrak{p}$ on class 4057

$\mathfrak{p}$	$\mathfrak{p}_{13,1}$	$\mathfrak{p}_{13,2}$	$\mathfrak{p}_{13,4}$	$\mathfrak{p}_{5,2}$	$\mathfrak{p}_{37,1}$	$\mathfrak{p}_{37,2}$
$a_\mathfrak{p}$	−3	1	−5	1	−7	−10
$\mathfrak{p}$	$\mathfrak{p}_{37,3}$	$\mathfrak{p}_{61,3}$	$\mathfrak{p}_{73,2}$	$\mathfrak{p}_{97,2}$	$\mathfrak{p}_{97,3}$	$\mathfrak{p}_{109,3}$
$\mathfrak{p}$	−2	−12	14	10	8	−10

Eigenvalues $a_\mathfrak{p}$ of the Hecke operators $T_\mathfrak{p}$ on class 4069

$\mathfrak{p}$	$\mathfrak{p}_{3}$	$\mathfrak{p}_{13,1}$	$\mathfrak{p}_{13,3}$	$\mathfrak{p}_{13,4}$	$\mathfrak{p}_{5,2}$	$\mathfrak{p}_{37,1}$	$\mathfrak{p}_{37,2}$	$\mathfrak{p}_{37,3}$
$a_{\mathfrak{p}}$	-2	-4	-2	-6	4	0	-2	-6
$\mathfrak{p}$	$\mathfrak{p}_{37,4}$	$\mathfrak{p}_{7,1}$	$\mathfrak{p}_{7,2}$	$\mathfrak{p}_{61,1}$	$\mathfrak{p}_{61,3}$	$\mathfrak{p}_{61,4}$	$\mathfrak{p}_{73,1}$	$\mathfrak{p}_{73,2}$
$a_{\mathfrak{p}}$	-2	-6	2	-6	-10	-2	8	2
$\mathfrak{p}$	$\mathfrak{p}_{73,3}$	$\mathfrak{p}_{97,2}$	$\mathfrak{p}_{97,3}$	$\mathfrak{p}_{109,3}$	$\mathfrak{p}_{11,1}$	$\mathfrak{p}_{157,2}$	$\mathfrak{p}_{157,4}$	$\mathfrak{p}_{181,4}$
$a_{\mathfrak{p}}$	-14	-2	6	14	-12	-6	4	-10
$\mathfrak{p}$	$\mathfrak{p}_{193,4}$	$\mathfrak{p}_{229,1}$	$\mathfrak{p}_{229,2}$	$\mathfrak{p}_{17,1}$	$\mathfrak{p}_{313,3}$	$\mathfrak{p}_{409,1}$	$\mathfrak{p}_{409,2}$	
$a_{\mathfrak{p}}$	-2	-14	20	-24	-10	10	-38	

Eigenvalues $a_{\mathfrak{p}}$ of the Hecke operators $T_{\mathfrak{p}}$ on class 4225b

$\mathfrak{p}$	$\mathfrak{p}_{3}$	$\mathfrak{p}_{13,1}$	$\mathfrak{p}_{13,2}$	$\mathfrak{p}_{13,3}$	$\mathfrak{p}_{5,1}$
$a_{\mathfrak{p}}$	5	4	-1	-6	-4
$\mathfrak{p}$	$\mathfrak{p}_{5,2}$	$\mathfrak{p}_{37,1}$	$\mathfrak{p}_{37,3}$	$\mathfrak{p}_{7,1}$	$\mathfrak{p}_{73,1}$
$a_{\mathfrak{p}}$	6	-12	3	-10	-11

Eigenvalues $a_{\mathfrak{p}}$ of the Hecke operators $T_{\mathfrak{p}}$ on class 4516

$\mathfrak{p}$	$\mathfrak{p}_{3}$	$\mathfrak{p}_{13,1}$	$\mathfrak{p}_{13,2}$	$\mathfrak{p}_{13,3}$	$\mathfrak{p}_{13,4}$	$\mathfrak{p}_{5,1}$	$\mathfrak{p}_{5,2}$	$\mathfrak{p}_{37,3}$
$a_{\mathfrak{p}}$	2	-2	-2	-2	6	-6	2	6
$\mathfrak{p}$	$\mathfrak{p}_{61,3}$	$\mathfrak{p}_{61,4}$	$\mathfrak{p}_{73,2}$	$\mathfrak{p}_{73,3}$	$\mathfrak{p}_{97,2}$	$\mathfrak{p}_{109,1}$	$\mathfrak{p}_{17,2}$	
$a_{\mathfrak{p}}$	-2	-10	-6	10	2	14	-30	

Eigenvalues $a_{\mathfrak{p}}$ of the Hecke operators $T_{\mathfrak{p}}$ on class 4672

$\mathfrak{p}$	$\mathfrak{p}_{3}$	$\mathfrak{p}_{13,1}$	$\mathfrak{p}_{13,2}$	$\mathfrak{p}_{13,3}$	$\mathfrak{p}_{5,1}$	$\mathfrak{p}_{5,2}$
$a_{\mathfrak{p}}$	-3	-1	-7	-2	3	-8
$\mathfrak{p}$	$\mathfrak{p}_{37,3}$	$\mathfrak{p}_{61,2}$	$\mathfrak{p}_{61,3}$	$\mathfrak{p}_{73,2}$	$\mathfrak{p}_{97,3}$	
$a_{\mathfrak{p}}$	2	-12	4	14	6	

Eigenvalues $a_{\mathfrak{p}}$ of the Hecke operators $T_{\mathfrak{p}}$ on class 4852

$\mathfrak{p}$	$\mathfrak{p}_{3}$	$\mathfrak{p}_{13,1}$	$\mathfrak{p}_{13,2}$	$\mathfrak{p}_{13,3}$	$\mathfrak{p}_{5,1}$	$\mathfrak{p}_{5,2}$	$\mathfrak{p}_{37,1}$	$\mathfrak{p}_{37,2}$
$a_{\mathfrak{p}}$	2	-2	6	-2	2	2	6	-10
$\mathfrak{p}$	$\mathfrak{p}_{37,4}$	$\mathfrak{p}_{7,2}$	$\mathfrak{p}_{61,1}$	$\mathfrak{p}_{61,2}$	$\mathfrak{p}_{61,3}$	$\mathfrak{p}_{73,1}$	$\mathfrak{p}_{73,2}$	$\mathfrak{p}_{73,4}$
$a_{\mathfrak{p}}$	6	2	-2	-10	-10	10	10	10
$\mathfrak{p}$	$\mathfrak{p}_{97,1}$	$\mathfrak{p}_{97,3}$	$\mathfrak{p}_{97,4}$	$\mathfrak{p}_{109,3}$	$\mathfrak{p}_{157,2}$	$\mathfrak{p}_{157,3}$	$\mathfrak{p}_{181,1}$	$\mathfrak{p}_{181,2}$
$a_{\mathfrak{p}}$	-14	2	-6	-2	-2	-2	-2	22
$\mathfrak{p}$	$\mathfrak{p}_{193,2}$	$\mathfrak{p}_{277,4}$	$\mathfrak{p}_{17,1}$	$\mathfrak{p}_{313,2}$	$\mathfrak{p}_{373,3}$	$\mathfrak{p}_{409,1}$	$\mathfrak{p}_{457,1}$	
$a_{\mathfrak{p}}$	2	6	34	-22	22	10	-22	

Eigenvalues $a_{\mathfrak{p}}$ of the Hecke operators $T_{\mathfrak{p}}$ on class 5317

$\mathfrak{p}$	$\mathfrak{p}_{3}$	$\mathfrak{p}_{13,1}$	$\mathfrak{p}_{13,2}$	$\mathfrak{p}_{13,3}$	$\mathfrak{p}_{5,1}$	$\mathfrak{p}_{5,2}$	$\mathfrak{p}_{37,1}$	$\mathfrak{p}_{37,2}$
$a_{\mathfrak{p}}$	-2	2	2	4	2	8	2	-4
$\mathfrak{p}$	$\mathfrak{p}_{37,3}$	$\mathfrak{p}_{37,4}$	$\mathfrak{p}_{61,1}$	$\mathfrak{p}_{61,2}$	$\mathfrak{p}_{73,1}$	$\mathfrak{p}_{73,2}$	$\mathfrak{p}_{73,4}$	$\mathfrak{p}_{97,1}$
$a_{\mathfrak{p}}$	2	2	14	8	14	14	14	8
$\mathfrak{p}$	$\mathfrak{p}_{97,3}$	$\mathfrak{p}_{97,4}$	$\mathfrak{p}_{109,1}$	$\mathfrak{p}_{109,3}$	$\mathfrak{p}_{109,4}$	$\mathfrak{p}_{157,1}$	$\mathfrak{p}_{157,2}$	$\mathfrak{p}_{181,4}$
$a_{\mathfrak{p}}$	8	2	2	14	-10	-4	-22	2
$\mathfrak{p}$	$\mathfrak{p}_{193,2}$	$\mathfrak{p}_{17,1}$	$\mathfrak{p}_{313,1}$	$\mathfrak{p}_{313,3}$	$\mathfrak{p}_{349,1}$	$\mathfrak{p}_{409,2}$	$\mathfrak{p}_{457,4}$	
$a_{\mathfrak{p}}$	-22	-10	8	-10	2	-22	-12	

Eigenvalues $a_{\mathfrak{p}}$ of the Hecke operators $T_{\mathfrak{p}}$ on class 5473

6.6.2 The Field F_2

Let $F = F_2$, which we recall is defined to be $\mathbb{Q}(t)$, where t is a root of the polynomial $x^4 - x^3 + 2x^2 + x + 1$. The table below gives a list of the prime ideals of F of norm at most 500, together with a generator for each ideal:

$\mathfrak{p}$	Generator	$\mathfrak{p}$	Generator	$\mathfrak{p}$	Generator
$\mathfrak{p}_{2,1}$	$\frac{1}{2}(-t^3+2t^2-4t-1)$	$\mathfrak{p}_{139,4}$	$-t^3-3t+1$	$\mathfrak{p}_{17,1}$	$\frac{1}{2}(-t^3-8t-5)$
$\mathfrak{p}_{2,2}$	t^3-t^2+2t	$\mathfrak{p}_{151,1}$	$\frac{1}{2}(3t^3-2t^2+6t-3)$	$\mathfrak{p}_{17,2}$	$-3t^3+2t^2-3t-1$
$\mathfrak{p}_3$	$\frac{1}{2}(t^3-2t^2+2t-3)$	$\mathfrak{p}_{151,2}$	$3t^3-4t^2+6t$	$\mathfrak{p}_{331,1}$	$\frac{1}{2}(3t^3-6t^2+10t-9)$
$\mathfrak{p}_{19,1}$	$\frac{1}{2}(3t^3-4t^2+4t+1)$	$\mathfrak{p}_{151,3}$	$\frac{1}{2}(-t^3+2t^2-6t-5)$	$\mathfrak{p}_{331,2}$	$\frac{1}{2}(-5t^3+6t^2-10t-11)$
$\mathfrak{p}_{19,2}$	$\frac{1}{2}(-t^3+2t^2-4t-3)$	$\mathfrak{p}_{151,4}$	$\frac{1}{2}(-3t^3+2t^2-6t-9)$	$\mathfrak{p}_{331,3}$	$\frac{1}{2}(7t^3-12t^2+18t-5)$
$\mathfrak{p}_{19,3}$	$\frac{1}{2}(-t^3-2t-5)$	$\mathfrak{p}_{13,1}$	$\frac{1}{2}(t^3-2t^2+2t-7)$	$\mathfrak{p}_{331,4}$	$-4t^3+6t^2-9t-4$
$\mathfrak{p}_{19,4}$	$t-2$	$\mathfrak{p}_{13,2}$	$\frac{1}{2}(3t^3-6t^2+6t-5)$	$\mathfrak{p}_{349,1}$	$\frac{1}{2}(5t^3-2t^2+2t+11)$
$\mathfrak{p}_5$	$\frac{1}{2}(-3t^3+2t^2-6t-3)$	$\mathfrak{p}_{181,1}$	$\frac{1}{2}(3t^3-8t^2+8t-3)$	$\mathfrak{p}_{349,2}$	$\frac{1}{2}(5t^3-2t^2+10t+3)$
$\mathfrak{p}_{31,1}$	$-2t^3+2t^2-4t-1$	$\mathfrak{p}_{181,2}$	$\frac{1}{2}(3t^3-4t^2+6t-5)$	$\mathfrak{p}_{349,3}$	$3t^3-5t^2+6t-1$
$\mathfrak{p}_{31,2}$	$\frac{1}{2}(t^3+2t^2-2t+3)$	$\mathfrak{p}_{181,3}$	$-t^3+2t^2-3t-3$	$\mathfrak{p}_{349,4}$	$\frac{1}{2}(-7t^3+6t^2-14t-9)$
$\mathfrak{p}_{31,3}$	$\frac{1}{2}(t^3+2t^2-2t+5)$	$\mathfrak{p}_{181,4}$	$2t^3-3t^2+4t-2$	$\mathfrak{p}_{379,1}$	$3t^3-2t^2+4t$
$\mathfrak{p}_{31,4}$	$\frac{1}{2}(-3t^3+2t^2-2t-3)$	$\mathfrak{p}_{199,1}$	$\frac{1}{2}(7t^3-10t^2+14t+1)$	$\mathfrak{p}_{379,2}$	$\frac{1}{2}(5t^3-2t^2+8t-1)$
$\mathfrak{p}_{7,1}$	t^3-2t^2+2t+2	$\mathfrak{p}_{199,2}$	$-3t^3+3t^2-6t-1$	$\mathfrak{p}_{379,3}$	$\frac{1}{2}(3t^3-10t^2+14t-7)$
$\mathfrak{p}_{7,2}$	$-t^3+2t^2-2t+2$	$\mathfrak{p}_{199,3}$	$-2t^3+2t^2-4t-5$	$\mathfrak{p}_{379,4}$	$\frac{1}{2}(-t^3-2t^2-6t-7)$
$\mathfrak{p}_{61,1}$	$\frac{1}{2}(3t^3-2t^2+6t-1)$	$\mathfrak{p}_{199,4}$	$\frac{1}{2}(3t^3-6t^2+2t+3)$	$\mathfrak{p}_{409,1}$	$\frac{1}{2}(5t^3-2t^2+10t+1)$
$\mathfrak{p}_{61,2}$	$\frac{1}{2}(-3t^3+2t^2-6t-7)$	$\mathfrak{p}_{211,1}$	$\frac{1}{2}(3t^3-6t^2+8t-7)$	$\mathfrak{p}_{409,2}$	$-t^3-2t^2+2t-2$
$\mathfrak{p}_{61,3}$	$-2t^3+2t^2-2t-3$	$\mathfrak{p}_{211,2}$	$\frac{1}{2}(3t^3-4t^2+4t-5)$	$\mathfrak{p}_{409,3}$	$\frac{1}{2}(-7t^3+6t^2-14t-11)$
$\mathfrak{p}_{61,4}$	$-2t^2+2t-1$	$\mathfrak{p}_{211,3}$	$-2t^3+3t^2-4t-4$	$\mathfrak{p}_{409,4}$	$\frac{1}{2}(9t^3-10t^2+18t+5)$
$\mathfrak{p}_{79,1}$	t^3-2t^2+3t-3	$\mathfrak{p}_{211,4}$	t^3-2t^2+t-3	$\mathfrak{p}_{421,1}$	$\frac{1}{2}(3t^3-8t^2+4t-5)$
$\mathfrak{p}_{79,2}$	$\frac{1}{2}(-t^3+4t^2-4t-3)$	$\mathfrak{p}_{229,1}$	t^3-3t^2+2t-3	$\mathfrak{p}_{421,2}$	$\frac{1}{2}(5t^3-8t^2+6t-3)$
$\mathfrak{p}_{79,3}$	$\frac{1}{2}(-3t^3+4t^2-6t-7)$	$\mathfrak{p}_{229,2}$	$\frac{1}{2}(3t^3-8t^2+8t-5)$	$\mathfrak{p}_{421,3}$	$\frac{1}{2}(-7t^3+12t^2-16t-5)$
$\mathfrak{p}_{79,4}$	$\frac{1}{2}(3t^3-4t^2+4t-3)$	$\mathfrak{p}_{229,3}$	t^3-t^2+2t-3	$\mathfrak{p}_{421,4}$	$\frac{1}{2}(-7t^3+10t^2-12t-9)$
$\mathfrak{p}_{109,1}$	$\frac{1}{2}(-5t^3+8t^2-12t-5)$	$\mathfrak{p}_{229,4}$	$\frac{1}{2}(5t^3-8t^2+10t-3)$	$\mathfrak{p}_{439,1}$	$\frac{1}{2}(-t^3+4t^2-8t-5)$
$\mathfrak{p}_{109,2}$	$\frac{1}{2}(3t^3-6t^2+10t-7)$	$\mathfrak{p}_{241,1}$	$\frac{1}{2}(3t^3-8t^2+12t-1)$	$\mathfrak{p}_{439,2}$	$\frac{1}{2}(5t^3-4t^2+8t-3)$
$\mathfrak{p}_{109,3}$	$\frac{1}{2}(-5t^3+6t^2-10t-9)$	$\mathfrak{p}_{241,2}$	$-t^3+t^2-4t-3$	$\mathfrak{p}_{439,3}$	$-3t^3+5t^2-8t-3$
$\mathfrak{p}_{109,4}$	$2t^3-2t^2+2t-1$	$\mathfrak{p}_{241,3}$	$\frac{1}{2}(3t^3-4t^2+10t-5)$	$\mathfrak{p}_{439,4}$	$\frac{1}{2}(7t^3-10t^2+16t-3)$
$\mathfrak{p}_{11,1}$	$\frac{1}{2}(-5t^3+8t^2-10t-5)$	$\mathfrak{p}_{241,4}$	$\frac{1}{2}(3t^3-2t^2+8t-3)$	$\mathfrak{p}_{499,1}$	$\frac{1}{2}(t^3+4t^2-8t+9)$
$\mathfrak{p}_{11,2}$	$\frac{1}{2}(3t^3-6t^2+4t-3)$	$\mathfrak{p}_{271,1}$	$\frac{1}{2}(-7t^3+10t^2-14t-9)$	$\mathfrak{p}_{499,2}$	$\frac{1}{2}(-5t^3+8t^2-10t-9)$
$\mathfrak{p}_{139,1}$	$-2t^3+3t^2-6t+2$	$\mathfrak{p}_{271,2}$	$\frac{1}{2}(-7t^3+12t^2-16t-3)$	$\mathfrak{p}_{499,3}$	$2t^2-5t+4$
$\mathfrak{p}_{139,2}$	$\frac{1}{2}(-5t^3+6t^2-12t-7)$	$\mathfrak{p}_{271,3}$	$\frac{1}{2}(t^3-4t^2+6t-11)$	$\mathfrak{p}_{499,4}$	$2t^3-4t^2+5t-4$
$\mathfrak{p}_{139,3}$	$\frac{1}{2}(-t^3-6t-5)$	$\mathfrak{p}_{271,4}$	$\frac{1}{2}(-3t^3+8t^2-4t-1)$		

We now provide, for the two cuspidal classes with rational eigenvalues found in **Section 5.3.2**, a list of primes which suffice to prove modularity of the corresponding elliptic curve, using the techniques of the previous sections. For the curve with conductor of norm 244, we list the Hecke eigenvalues $a_{\mathfrak{p}}(\pi)$ for each of these primes, and are therefore able to prove that it is modular. For the second curve, with conductor of norm 2071, we were unable to compute all of the required Hecke eigenvalues, but list those that we were able to calculate.

Class 244

- The level $\mathfrak{n} = \mathfrak{p}_{2,2}\mathfrak{p}_{61,3}$, and the residual representation attached to the corresponding elliptic curve has trivial image.
- The modulus $\mathfrak{m} = \mathfrak{p}_{2,1}^3\mathfrak{p}_{2,2}^3\mathfrak{p}_{61,3}$, and the corresponding ray class group $Cl(\mathcal{O}_F, \mathfrak{m})$ is isomorphic to $\mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z})^3$.
- The prime $\mathfrak{p}_{19,1}$ suffices to prove isomorphism of the residual representations.
- The primes $\{\mathfrak{p}_{3,1}, \mathfrak{p}_{19,1}, \mathfrak{p}_{19,2}, \mathfrak{p}_{19,3}, \mathfrak{p}_{19,4}, \mathfrak{p}_5, \mathfrak{p}_{31,1}, \mathfrak{p}_{31,2}, \mathfrak{p}_{31,4}, \mathfrak{p}_{7,1}, \mathfrak{p}_{7,2}, \mathfrak{p}_{61,1}, \mathfrak{p}_{61,2}, \mathfrak{p}_{61,4}, \mathfrak{p}_{79,1}, \mathfrak{p}_{79,2}, \mathfrak{p}_{79,3}, \mathfrak{p}_{109,4}, \mathfrak{p}_{11,1}, \mathfrak{p}_{139,3}, \mathfrak{p}_{151,2}, \mathfrak{p}_{181,1}, \mathfrak{p}_{181,2}, \mathfrak{p}_{181,3}, \mathfrak{p}_{199,1}, \mathfrak{p}_{211,1}, \mathfrak{p}_{211,4}, \mathfrak{p}_{229,1}, \mathfrak{p}_{241,3}, \mathfrak{p}_{379,4}, \mathfrak{p}_{1009,1}\}$, where $\mathfrak{p}_{1009,1}$ is generated by $\frac{1}{2}(11t^3 - 14t^2 + 20t + 5)$, satisfy the conditions for Livné's theorem, and therefore suffice to prove isomorphism of the full representations.

Class 2071

- The level $\mathfrak{n} = \mathfrak{p}_{19,2}\mathfrak{p}_{109,3}$, and the residual representation attached to the corresponding elliptic curve has trivial image.
- The modulus $\mathfrak{m} = \mathfrak{p}_{2,1}^3\mathfrak{p}_{2,2}^3\mathfrak{p}_{19,2}\mathfrak{p}_{109,3}$, and the corresponding ray class group $Cl(\mathcal{O}_F, \mathfrak{m})$ is isomorphic to $\mathbb{Z}/36/\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z})^4$.
- The primes $\{\mathfrak{p}_{3,1}, \mathfrak{p}_{19,1}, \mathfrak{p}_{19,4}, \mathfrak{p}_{31,1}\}$ suffice to prove isomorphism of the residual representations.
- The primes $\{\mathfrak{p}_{3,1}, \mathfrak{p}_{19,1}, \mathfrak{p}_{19,3}, \mathfrak{p}_{19,4}, \mathfrak{p}_5, \mathfrak{p}_{31,1}, \mathfrak{p}_{31,2}, \mathfrak{p}_{31,3}, \mathfrak{p}_{31,4}, \mathfrak{p}_{7,1}, \mathfrak{p}_{7,2}, \mathfrak{p}_{61,1}, \mathfrak{p}_{61,2}, \mathfrak{p}_{61,3}, \mathfrak{p}_{61,4}, \mathfrak{p}_{79,1}, \mathfrak{p}_{79,2}, \mathfrak{p}_{79,3}, \mathfrak{p}_{79,4}, \mathfrak{p}_{109,1}, \mathfrak{p}_{109,4}, \mathfrak{p}_{11,2}, \mathfrak{p}_{139,2}, \mathfrak{p}_{139,3}, \mathfrak{p}_{139,4}, \mathfrak{p}_{151,1}, \mathfrak{p}_{151,2}, \mathfrak{p}_{13,1}, \mathfrak{p}_{13,2}, \mathfrak{p}_{181,1}, \mathfrak{p}_{181,2}, \mathfrak{p}_{181,4}, \mathfrak{p}_{199,1}, \mathfrak{p}_{199,2}, \mathfrak{p}_{211,1}, \mathfrak{p}_{211,2}, \mathfrak{p}_{211,4}, \mathfrak{p}_{229,1}, \mathfrak{p}_{229,2}, \mathfrak{p}_{229,3}, \mathfrak{p}_{229,4}, \mathfrak{p}_{241,1}, \mathfrak{p}_{241,3}, \mathfrak{p}_{241,4}, \mathfrak{p}_{271,2}, \mathfrak{p}_{331,1}, \mathfrak{p}_{331,3}, \mathfrak{p}_{331,4}, \mathfrak{p}_{379,4}, \mathfrak{p}_{409,1}, \mathfrak{p}_{439,2}, \mathfrak{p}_{439,4}, \mathfrak{p}_{499,1}, \mathfrak{p}_{541,1}, \mathfrak{p}_{601,1}, \mathfrak{p}_{691,1}, \mathfrak{p}_{739,1}, \mathfrak{p}_{919,1}, \mathfrak{p}_{1009,1}, \mathfrak{p}_{1009,2}, \mathfrak{p}_{1069,1}, \mathfrak{p}_{1381,1}, \mathfrak{p}_{41,1}\}$, where the primes $\mathfrak{p}_{541,1}$, $\mathfrak{p}_{601,1}$, $\mathfrak{p}_{691,1}$, $\mathfrak{p}_{739,1}$, $\mathfrak{p}_{919,1}$, $\mathfrak{p}_{1009,1}$, $\mathfrak{p}_{1009,2}$, $\mathfrak{p}_{1069,1}$, $\mathfrak{p}_{1381,1}$ and $\mathfrak{p}_{41,1}$ are generated by $\frac{1}{2}(-7t^3 + 8t^2 - 16t - 11)$, $\frac{1}{2}(9t^3 - 8t^2 + 14t + 9)$, $\frac{1}{2}(-3t^3 + 10t^2 - 4t - 1)$, $t^3 - 5t^2 + 6t - 5$, $\frac{1}{2}(-5t^3 - 12t - 3)$, $\frac{1}{2}(-7t^3 + 8t^2 - 16t - 13)$, $\frac{1}{2}(11t^3 - 14t^2 + 20t + 5)$, $4t^3 - 2t^2 + 5t + 2$, $\frac{1}{2}(7t^3 - 14t^2 + 22t - 13)$, and $\frac{1}{2}(-5t^3 + 10t^2 - 22t + 5)$ respectively, satisfy the conditions for Livné's theorem, and therefore suffice to prove isomorphism of the full representations.

$\mathfrak{p}$	$\mathfrak{p}_{3,1}$	$\mathfrak{p}_{19,1}$	$\mathfrak{p}_{19,2}$	$\mathfrak{p}_{19,3}$	$\mathfrak{p}_{19,4}$	$\mathfrak{p}_{5}$	$\mathfrak{p}_{31,1}$	$\mathfrak{p}_{31,2}$
$a_{\mathfrak{p}}$	-2	-4	-4	-4	8	2	-4	8
$\mathfrak{p}$	$\mathfrak{p}_{31,4}$	$\mathfrak{p}_{7,1}$	$\mathfrak{p}_{7,2}$	$\mathfrak{p}_{61,1}$	$\mathfrak{p}_{61,2}$	$\mathfrak{p}_{61,4}$	$\mathfrak{p}_{79,1}$	$\mathfrak{p}_{79,2}$
$a_{\mathfrak{p}}$	-4	2	2	-10	2	-10	-16	8
$\mathfrak{p}$	$\mathfrak{p}_{79,3}$	$\mathfrak{p}_{109,4}$	$\mathfrak{p}_{11,1}$	$\mathfrak{p}_{139,3}$	$\mathfrak{p}_{151,2}$	$\mathfrak{p}_{181,1}$	$\mathfrak{p}_{181,2}$	$\mathfrak{p}_{181,3}$
$a_{\mathfrak{p}}$	8	14	-10	8	-16	-10	26	-10
$\mathfrak{p}$	$\mathfrak{p}_{199,1}$	$\mathfrak{p}_{211,1}$	$\mathfrak{p}_{211,4}$	$\mathfrak{p}_{229,1}$	$\mathfrak{p}_{241,3}$	$\mathfrak{p}_{379,4}$	$\mathfrak{p}_{1009,1}$	
$a_{\mathfrak{p}}$	-16	-4	8	14	2	20	-22	

Eigenvalues $a_{\mathfrak{p}}$ of the Hecke operators $T_{\mathfrak{p}}$ on class 244

$\mathfrak{p}$	$\mathfrak{p}_{3,1}$	$\mathfrak{p}_{19,1}$	$\mathfrak{p}_{19,3}$	$\mathfrak{p}_{19,4}$	$\mathfrak{p}_{5}$	$\mathfrak{p}_{31,1}$	$\mathfrak{p}_{31,2}$	$\mathfrak{p}_{31,3}$
$a_{\mathfrak{p}}$	-2	2	2	2	8	8	8	2
$\mathfrak{p}$	$\mathfrak{p}_{31,4}$	$\mathfrak{p}_{7,1}$	$\mathfrak{p}_{7,2}$	$\mathfrak{p}_{61,1}$	$\mathfrak{p}_{61,2}$	$\mathfrak{p}_{61,3}$	$\mathfrak{p}_{61,4}$	$\mathfrak{p}_{79,1}$
$a_{\mathfrak{p}}$	2	-10	-10	-4	-4	14	2	14
$\mathfrak{p}$	$\mathfrak{p}_{79,2}$	$\mathfrak{p}_{79,3}$	$\mathfrak{p}_{79,4}$	$\mathfrak{p}_{109,1}$	$\mathfrak{p}_{109,4}$	$\mathfrak{p}_{11,2}$	$\mathfrak{p}_{139,2}$	$\mathfrak{p}_{139,3}$
$a_{\mathfrak{p}}$	-4	8	8	8	-16	2	-10	-4
$\mathfrak{p}$	$\mathfrak{p}_{139,4}$	$\mathfrak{p}_{151,1}$	$\mathfrak{p}_{151,2}$	$\mathfrak{p}_{13,1}$	$\mathfrak{p}_{13,2}$	$\mathfrak{p}_{181,1}$	$\mathfrak{p}_{181,2}$	$\mathfrak{p}_{181,4}$
$a_{\mathfrak{p}}$	20	20	2	8	2	-10	2	-16
$\mathfrak{p}$	$\mathfrak{p}_{199,1}$	$\mathfrak{p}_{199,2}$	$\mathfrak{p}_{211,1}$	$\mathfrak{p}_{211,2}$	$\mathfrak{p}_{211,4}$	$\mathfrak{p}_{229,1}$	$\mathfrak{p}_{229,2}$	$\mathfrak{p}_{229,3}$
$a_{\mathfrak{p}}$	2	-16	-16	2	-16	20	-22	2
$\mathfrak{p}$	$\mathfrak{p}_{229,4}$	$\mathfrak{p}_{241,1}$	$\mathfrak{p}_{241,3}$	$\mathfrak{p}_{241,4}$	$\mathfrak{p}_{271,2}$	$\mathfrak{p}_{331,1}$	$\mathfrak{p}_{331,3}$	$\mathfrak{p}_{331,4}$
$a_{\mathfrak{p}}$	-10	20	2	8	-22	2	-16	8
$\mathfrak{p}$	$\mathfrak{p}_{379,4}$	$\mathfrak{p}_{409,1}$	$\mathfrak{p}_{439,2}$	$\mathfrak{p}_{439,4}$	$\mathfrak{p}_{499,1}$	$\mathfrak{p}_{541,1}$	$\mathfrak{p}_{601,1}$	$\mathfrak{p}_{691,1}$
$a_{\mathfrak{p}}$	20	20	-34	-4	8	-28	$-$	$-$
$\mathfrak{p}$	$\mathfrak{p}_{739,1}$	$\mathfrak{p}_{919,1}$	$\mathfrak{p}_{1009,1}$	$\mathfrak{p}_{1009,2}$	$\mathfrak{p}_{1069,1}$	$\mathfrak{p}_{1381,1}$	$\mathfrak{p}_{41,1}$	
$a_{\mathfrak{p}}$	$-$	$-$	$-$	$-$	$-$	$-$	$-$	

Eigenvalues $a_{\mathfrak{p}}$ of the Hecke operators $T_{\mathfrak{p}}$ on class 2071

6.6.3 The Field F_3

Let $F = F_3$, which we recall is defined to be $\mathbb{Q}(t)$, where t is a primitive eighth root of unity. The table below gives a list of the prime ideals of F of norm at most 350, together with a generator for each ideal:

$\mathfrak{p}$	Generator	$\mathfrak{p}$	Generator	$\mathfrak{p}$	Generator
$\mathfrak{p}_2$	$t+1$	$\mathfrak{p}_{97,1}$	$-3t^2-2t$	$\mathfrak{p}_{233,4}$	$-2t^3+t^2+4t+2$
$\mathfrak{p}_{3,1}$	t^3+t^2-t	$\mathfrak{p}_{97,2}$	$2t^3-t^2-t-3$	$\mathfrak{p}_{241,1}$	$-t^3+4t+2$
$\mathfrak{p}_{3,2}$	t^3-t^2-t	$\mathfrak{p}_{97,3}$	t^3-t^2+3t-2	$\mathfrak{p}_{241,2}$	$-3t^3-t^2+3t+2$
$\mathfrak{p}_{17,1}$	$t+2$	$\mathfrak{p}_{97,4}$	t^3+t^2-2t-3	$\mathfrak{p}_{241,3}$	$-2t^3-4t^2+1$
$\mathfrak{p}_{17,2}$	t^3+2	$\mathfrak{p}_{113,1}$	t^3-t^2-3t	$\mathfrak{p}_{241,4}$	$-t^3-3t^2-2t-3$
$\mathfrak{p}_{17,3}$	$2t+1$	$\mathfrak{p}_{113,2}$	$3t^3+t^2-t$	$\mathfrak{p}_{257,1}$	$t+4$
$\mathfrak{p}_{17,4}$	$2t^3+1$	$\mathfrak{p}_{113,3}$	$-2t^3-t^2+2t+4$	$\mathfrak{p}_{257,2}$	$-4t^3-3t^2-3t+1$
$\mathfrak{p}_{5,1}$	$2t^3-t$	$\mathfrak{p}_{113,4}$	$-2t^3+t^2+2t+4$	$\mathfrak{p}_{257,3}$	$4t+1$
$\mathfrak{p}_{5,2}$	t^3-2t	$\mathfrak{p}_{11,1}$	t^3+3t^2-t	$\mathfrak{p}_{257,4}$	$-t^3+3t^2+3t+4$
$\mathfrak{p}_{41,1}$	$-t^3+2t^2+t-1$	$\mathfrak{p}_{11,2}$	t^3-3t^2-t	$\mathfrak{p}_{281,1}$	$3t^3+2t^2-2t$
$\mathfrak{p}_{41,2}$	$-t^3+t^2+2t-1$	$\mathfrak{p}_{137,1}$	$2t^3+2t^2-2t-1$	$\mathfrak{p}_{281,2}$	$2t^3-2t^2-3t$
$\mathfrak{p}_{41,3}$	$-2t^3-t^2-t-1$	$\mathfrak{p}_{137,2}$	$-2t^3-2t^2+2t-1$	$\mathfrak{p}_{281,3}$	$-4t^3-t^2+t+5$
$\mathfrak{p}_{41,4}$	t^3+t^2+2t-1	$\mathfrak{p}_{137,3}$	$2t^3-2t^2-2t-1$	$\mathfrak{p}_{281,4}$	$-5t^3-t^2+t+4$
$\mathfrak{p}_{7,1}$	$-t^3-2t^2+2$	$\mathfrak{p}_{137,4}$	$-2t^3+2t^2+2t-1$	$\mathfrak{p}_{313,1}$	$-3t^3-2t^2+3t+3$
$\mathfrak{p}_{7,2}$	t^2+3t+1	$\mathfrak{p}_{13,1}$	$-3t^3-2t$	$\mathfrak{p}_{313,2}$	$-2t^3-2t^2+3t+2$
$\mathfrak{p}_{73,1}$	$-3t^3+t+3$	$\mathfrak{p}_{13,2}$	$3t^3-2t$	$\mathfrak{p}_{313,3}$	$-3t^3-3t^2+2t+3$
$\mathfrak{p}_{73,2}$	$-3t^3-t^2+3$	$\mathfrak{p}_{193,1}$	$-3t^3-t^2-2t-1$	$\mathfrak{p}_{313,4}$	$-2t^3-3t^2+2t+2$
$\mathfrak{p}_{73,3}$	t^3-2t^2-2t	$\mathfrak{p}_{193,2}$	$2t^3+t^2+3t-1$	$\mathfrak{p}_{337,1}$	$-4t^2-3t$
$\mathfrak{p}_{73,4}$	$2t^3+2t^2-t$	$\mathfrak{p}_{193,3}$	$-3t^3-t^2+2t-1$	$\mathfrak{p}_{337,2}$	$3t^3-t^2-t-4$
$\mathfrak{p}_{89,1}$	$-2t^3-2t^2-3t$	$\mathfrak{p}_{193,4}$	$-2t^3+t^2+3t-1$	$\mathfrak{p}_{337,3}$	$-t^3+4t^2-3t-1$
$\mathfrak{p}_{89,2}$	$-3t^3+t+1$	$\mathfrak{p}_{233,1}$	$-t^3+t^2+t+4$	$\mathfrak{p}_{337,4}$	t^3+t^2-3t-4
$\mathfrak{p}_{89,3}$	$-2t^3+3t+2$	$\mathfrak{p}_{233,2}$	$-2t^3-2t^2-4t-1$		
$\mathfrak{p}_{89,4}$	$-3t^2-t-1$	$\mathfrak{p}_{233,3}$	$-2t^3+2t^2-4t+1$		

We now provide, for the single cuspidal class with rational eigenvalues found in **Section 5.3.3**, a list of primes which suffice to prove modularity of the corresponding elliptic curve, using the techniques of the previous sections. We list the corresponding Hecke eigenvalues for each prime, and are therefore able to conclude that the curve is indeed modular.

Class 881

- The level $\mathfrak{n} = \mathfrak{p}_{881,1}$, which is generated by the element $-4t^2 + 5t$, and the residual representation attached to the corresponding elliptic curve has trivial image.
- The modulus $\mathfrak{m} = \mathfrak{p}_2^9\mathfrak{p}_{881,1}$, and the corresponding ray class group $Cl(\mathcal{O}_F, \mathfrak{m})$ is isomorphic to $\mathbb{Z}/8\mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z})^3$.
- For each possible extension F_π of F corresponding to a quadratic character of $Cl(\mathcal{O}_F, \mathfrak{m})$, the ray class group $Cl(\mathcal{O}_{F_\pi}, \mathfrak{m}_\pi)$ admits no cubic characters, and thus we immediately deduce that the residual representations are isomorphic.
- The primes $\{\mathfrak{p}_{3,1}, \mathfrak{p}_{3,2}, \mathfrak{p}_{17,1}, \mathfrak{p}_{17,2}, \mathfrak{p}_{17,3}, \mathfrak{p}_{5,1}, \mathfrak{p}_{5,2}, \mathfrak{p}_{41,2}, \mathfrak{p}_{7,1}, \mathfrak{p}_{7,2}, \mathfrak{p}_{73,1}, \mathfrak{p}_{73,4}, \mathfrak{p}_{97,2}, \mathfrak{p}_{13,2}, \mathfrak{p}_{337,3}\}$ satisfy the conditions for Livné's theorem, and therefore suffice to prove isomorphism of the full representations.

$\mathfrak{p}$	$\mathfrak{p}_{3,1}$	$\mathfrak{p}_{3,2}$	$\mathfrak{p}_{17,1}$	$\mathfrak{p}_{17,2}$	$\mathfrak{p}_{17,3}$	$\mathfrak{p}_{5,1}$	$\mathfrak{p}_{5,2}$	$\mathfrak{p}_{41,2}$
$a_\mathfrak{p}$	4	-2	-6	0	0	2	2	6
$\mathfrak{p}$	$\mathfrak{p}_{7,1}$	$\mathfrak{p}_{7,2}$	$\mathfrak{p}_{73,1}$	$\mathfrak{p}_{73,4}$	$\mathfrak{p}_{97,2}$	$\mathfrak{p}_{13,2}$	$\mathfrak{p}_{337,3}$	
$a_\mathfrak{p}$	2	2	-16	-10	2	-10	14	

Eigenvalues $a_\mathfrak{p}$ of the Hecke operators $T_\mathfrak{p}$ on class 881

Chapter 7

Bibliography

[**AGM02**] A. Ash, P.E. Gunnells, M. McConnell: *Cohomology of congruence subgroups of* $\mathrm{SL}(4,\mathbb{Z})$, J. of Number Theory, **94**, 2002, pp. 181-212.

[**AGM11**] A. Ash, P.E. Gunnells, M. McConnell: *Resolutions of the Steinberg module for* $\mathrm{GL}(n)$, J. Algebra **349**, 2012, pp. 380-390.

[**AGM13**] A. Ash, P.E. Gunnells, M. McConnell: *Mod 2 homology of* $\mathrm{GL}(4)$ *and Galois representations*, to appear in J. Number Theory, eprint arXiv:1304.5684v2, 2013.

[**Ash77**] A. Ash: *Deformation retracts with lowest possible dimension of arithmetic quotients of self-adjoint homogeneous cones*, Math. Ann. **225**, 1977, pp. 69-76.

[**Bro94**] K. Brown: *Cohomology of groups*, Graduate Texts in Mathematics, **87**, Springer-Verlag, New York, 1994.

[**Bum98**] D. Bump: *Automorphic forms and representations*, Cambridge Studies in Advanced Mathematics, **55**, 1998.

[**BS73**] A. Borel, J.P. Serre: *Corners and arithmetic groups*, Comment. Math. Helv. **48**, 1973, pp. 436-491, Avec un appendice: Arrondissement des variétés à coins, par A. Douady et L. Hérault.

[**Car94**] H. Carayol: *Modular forms and Galois representations with values in a complete local ring*, in *p-adic monodromy and the Birch and Swinnerton-Dyer conjecture*, B. Mazur, G. Stevens (eds.), proceedings of a conference at Boston University, August 12-16, 1991, Cont. Math. **165**, 1994, pp. 213-237.

[**Chê08**] G. Chênevert: *Exponential sums, hypersurfaces with many symmetries and Galois representations*, Department of Mathematics and Statistics, McGill University, Montreal, 2008.
Available at http://chenevert.ath.cx/PDF/thesis.pdf.

[**Cog04**] J. Cogdell: *Langlands conjectures for* GL_n, pp. 229-250 in *An introduction to the Langlands program*, eds. J. Bernstein, S. Gelbart, Birkhäuser, 2004.

[**Coh00**] H. Cohen: *Advanced topics in computational number theory*, Graduate Texts in Mathematics, Springer-Verlag, **193**, 2000.

[**DGKY14**] S. Donnelly, P.E. Gunnells, A. Klages-Mundt, D. Yasaki: *A table of elliptic curves over the cubic field of discriminant -23*, eprint arXiv:1409.7911, 2014.

[**DGP10**] L.V. Dieulefait, L. Guerberoff, A. Pacetti: *Proving modularity for a given elliptic curve over an imaginary quadratic field*, Math. Comp. **79**, 2010, pp. 1145-1170.

[**DS05**] F. Diamond and J. Shurman, *A First Course in Modular Forms*, Springer Graduate Texts in Mathematics **228**, 2005.

[**EGS10**] P. Elbaz-Vincent, H. Gangl, C. Soulé: *Perfect forms and the cohomology of modular groups*, eprint arXiv:1001.0789, 2010.

[**FHS13**] N. Freitas, B. Le Hung, S. Siksek: *Elliptic curves over real quadratic fields are modular*, to appear in Invent. Math., eprint arXiv:1310.7088v4, 2013.

[**Gel97**] S. Gelbart, *Three lectures on the modularity of* $\bar{\rho}_{E,3}$ *and the Langlands reciprocity conjecture*, pp. 156-208 in *Modular forms and Fermat's last theorem*, eds. G. Cornell, J.H. Silverman, G. Stevens, Springer-Verlag, New York, 1997. Papers from the Instructional Conference on Number Theory and Arithmetic Geometry held at Boston University, Boston, MA, August 9-18, 1995.

[**Get13**] J.R. Getz: *Lecture notes on automorphic representations*, 2013.
Available at http://www.math.duke.edu/∼jgetz/aut_reps.pdf.

[**GHY13**] P.E. Gunnells, F. Hajir, D. Yasaki: *Modular forms and elliptic curves over the field of fifth roots of unity*, Experimental Math. **22**, 2013, no. 2, pp. 203-216.

[**Gun99**] P.E. Gunnells: *Modular symbols for* $\mathbb{Q}$*-rank one groups and Voronoï reduction*, J. Number Theory **75**, 1999, no. 2, pp. 198-219.

[**Gun11**] P.E. Gunnells: *Lectures on computing cohomology of arithmetic groups*, Proceedings of the Conference on Modular Forms, Heidelberg, Germany, 2011. Contributions in Mathematical and Computational Sciences (Springer-Verlag) **6**, 2014, pp. 3-45.

[**GY08**] P.E. Gunnells, D. Yasaki: *Hecke operators and Hilbert modular forms*, Algorithmic number theory, Lecture Notes in Comput. Sci., **5011**, Springer, Berlin, 2008, pp. 387-401.

[**GY13**] P.E. Gunnells, D. Yasaki: *Modular forms and elliptic curves over the cubic field of discriminant* 23, Int. J. Number Theory **9**, 2013, no. 1, pp. 53-76.

[**Har06**] G. Harder: *Cohomology of arithmetic groups*, 2006, manuscript in preparation. Available online at http://www.math.uni-bonn.de/people/harder/Manuscripts/

[**Hid93**] H. Hida: *Elementary theory of L-functions and Eisenstein series*, London Mathematical Society Student Texts, **26**, 1993.

[**JL70**] H. Jacquet and R.P. Langlands: *Automorphic forms on* GL(2), Lecture Notes in Mathematics, **114**, Springer-Verlage, Berlin, 1970.

[**Koe60**] M. Koecher: *Beiträge zu einer Reduktionstheorie in Positivitätsbereichen*, I, Math. Ann. **141**, 1960, pp. 384-432.

[**Kub76**] D.S. Kubert: *Universal bounds on the torsion of elliptic curves*, Proc. London Math. Soc. (3) **33**, no. 2, 1976, pp. 193-237.

[**Kud04**] S. Kudla: *From modular forms to automorphic representations*, pp. 133-152 in *An introduction to the Langlands program*, eds. J. Bernstein, S. Gelbart, Birkhäuser, 2004.

[**Liv87**] R. Livné: *Cubic exponential sums and Galois representations*, in *Current Trends in Arithmetical Algebraic Geometry* (Arcata, Calif., 1985), Contemp. Math., **67**, Amer. Math. Soc., Providence, RI, 1987, pp. 247-261.

[**LP10**] K. Lux, H. Pahlings: *Representations of groups, a computational approach*, Cambridge Studies in Advanced Mathematics **124**, Cambridge University Press, 2010.

[**MAG14**] The Computational Algebra Group, University of Sydney, *MAGMA*, Version 2.20-9, 2014.
Available at http://magma.maths.usyd.edu.au/magma.

[**Mok14**] C.P. Mok: *Galois representations attached to automorphic forms on* GL_2 *over CM fields*, Compos. Math. **150**, no. 4, 2014, pp. 523-567.

[**PAR14**] The PARI Group, Bordeaux. PARI/GP, version 2.7.2, 2014.
Available from http://pari.math.u-bordeaux.fr/.

[**Par75**] C. J. Parry, *Units of algebraic number fields*, J. Number Theory **7**, 1975, pp. 385-388; corr. **9**, 1977, p. 278.

[**Rob00**] A.M. Robert: *A course in p-adic analysis*, Graduate Texts in Mathematics, **198**, Springer-Verlag, New York, 2000.

[**Sch06**] J. Schwermer, *The cohomological approach to cuspidal automorphic representations*, Cont. Math., **488**, 2006, pp. 257-285.

[**Sch09**] A. Schrmann, *Enumerating perfect forms*, pp. 359-378 in Quadratic Forms: Algebra, Arithmetic, and Geometry, AMS Contemporary Mathematics **437**, 2009.

[**Ser71**] J.P. Serre: *Cohomologie des groupes discrets*, Propsects in Mathematics (Proc. Sympos., Princeton Univ., Princton, N.J., 1970), Princeton Univ. Press, Princeton, N.J., Ann. of Math. Studies, **70**, 1971, pp. 77-169.

[**Ser95**] J.P. Serre: *Représentations linéaires sur des anneaux locaux, d'apres Carayol*, Publ. Inst. Math. Jussieu, **49**, 1995.

[**Sil09**] J. Silverman, *The arithmetic of elliptic curves*, Second Edition, Graduate Texts in Mathematics, **106**, Springer, Dordrecht, 2009.

[**Ski09**] C. Skinner: *A note on the p-adic Galois representations attached to Hilbert modular forms*, Documenta Mathematica, **14**, 2009, pp. 241-258.

[**Sol69**] L. Solomon: *The Steinberg character of a finite group with BN-pair*, Theory of Finite Groups (Brauer and Sah, eds.), Benjamin, 1969.

[**Ste07**] W. Stein: *Modular forms, a computational approach*, Graduate Studies in Mathematics, **79**, American Mathematical Society, Providence, RI, 2007. With an appendix by Paul E. Gunnells.

[**Wie08**] G. Wiese: *Galois representations*, Lecture course at Universität Duisburg-Essen, 2008.
Available at http://math.uni.lu/∼wiese/notes/GalRep.pdf.

[**Yas09**] D. Yasaki: *Binary hermitian forms over a cyclotomic field*, J. Algebra, **322**, 2009, pp. 4132-4142.