EXPLICIT METHODS FOR HILBERT MODULAR FORMS

LASSINA DEMBÉLÉ AND JOHN VOIGHT

ABSTRACT. We exhibit algorithms to compute systems of Hecke eigenvalues for spaces of Hilbert modular forms over a totally real field. We provide many explicit examples as well as applications to modularity and Galois representations.

CONTENTS

The study of modular forms remains a dominant theme in modern number theory, a consequence of their intrinsic appeal as well as their applications to a wide variety of mathematical problems. This subject has seen dramatic progress during the past half-century in an environment where both abstract theory and explicit computation have developed in parallel. Experiments will remain an essential tool in the years ahead, especially as we turn from classical contexts to less familiar terrain.

In this article, we discuss methods for explicitly computing spaces of Hilbert modular forms, refashioning algorithms over $\mathbb{Q}$ to the setting of totally real fields. Saving definitions for the sections that follow, we state our main result.

Theorem. *There exists an algorithm that, given a totally real field F, a nonzero ideal $\mathfrak{N}$ of the ring of integers of F, and a weight $k \in (\mathbb{Z}_{\geq 2})^{[F:\mathbb{Q}]}$, computes the space $S_k(\mathfrak{N})$ of Hilbert cusp forms of weight k and level $\mathfrak{N}$ over F as a Hecke module.*

This theorem is the work of the first author [15] together with Donnelly [18] combined with work of the second author [71] together with Greenberg [30].

The outline of this article is as follows. After briefly recalling methods for classical (elliptic) modular forms in §1, we introduce our results for computing Hilbert modular forms in the simplest case (of parallel weight 2 over a totally real field of strict class number 1) in

---

§2. In brief, our methods employ the Jacquet-Langlands correspondence to relate spaces of Hilbert modular forms to spaces of quaternionic modular forms that are more amenable to computation; we discuss this matter in §3, and consider two approaches (definite and indefinite) in §§4–5. In §6 we consider several examples in detail. Having thereby established the main ideas, we turn to an adelic description of Hilbert modular forms and their quaternionic incarnations in §7, then give a complete and general description of our algorithms in adelic language in §§8–9.

Although it is our intention to keep these notes as self-contained as possible, we will assume that the reader has a basic familiarity with classical modular forms and the methods employed to compute them. The algorithms exhibited below have been implemented in the computer algebra system Magma [3] and our examples are computed using this implementation. Donnelly and the second author [21] are using this implementation to compute Hecke data for thousands of forms over totally real fields up to degree 6.

1. Classical (elliptic) modular forms

To motivate our study of Hilbert modular forms, we begin by briefly considering algorithms for classical (elliptic) modular forms. For a more detailed introduction to modular forms, see the books by Darmon [11] and Diamond and Shurman [19], and for more information on computational aspects see Cremona [9], Kilford [40], Stein [66], and the many references contained therein.

Let $\mathcal{H} = \{x + yi \in \mathbb{C} : y > 0\}$ denote the upper-half plane and let $\mathcal{H}^* = \mathcal{H} \cup \mathbb{P}^1(\mathbb{Q})$ denote the completed upper half-plane with the *cusps* $\mathbb{P}^1(\mathbb{Q})$. The group

$$\mathrm{GL}_2^+(\mathbb{Q}) = \{\gamma \in \mathrm{GL}_2(\mathbb{Q}) : \det \gamma > 0\}$$

acts on $\mathcal{H}^*$ by linear fractional transformations. For $N \in \mathbb{Z}_{>0}$, we consider the subgroup of those integral matrices of determinant 1 that are upper-triangular modulo N,

$$\Gamma_0(N) = \left\{\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : N \mid c \right\} \subseteq \mathrm{GL}_2^+(\mathbb{Z}) = \mathrm{SL}_2(\mathbb{Z}) \subseteq \mathrm{GL}_2^+(\mathbb{Q}).$$

The group $\mathrm{P\Gamma}_0(N) = \Gamma_0(N)/\{\pm 1\}$ is a discrete subgroup of $\mathrm{PSL}_2(\mathbb{R})$. A *modular form* of weight $k \in \mathbb{Z}_{>0}$ and level N is a holomorphic function $f : \mathcal{H} \to \mathbb{C}$ such that

$$(1.1) \qquad f(\gamma z) = f\left(\frac{az+b}{cz+d}\right) = (cz+d)^k f(z)$$

for all $\gamma \in \Gamma_0(N)$ and such that $f(z)$ tends to a finite limit as z tends to any cusp (i.e., f is holomorphic at the cusps).

One can equivalently write this as follows. For $\gamma \in \mathrm{GL}_2(\mathbb{R})$ and $z \in \mathcal{H}$ we define $j(\gamma, z) = cz + d$. We then define a *weight k action* of $\mathrm{GL}_2^+(\mathbb{Q})$ on the space of complex-valued functions

on $\mathcal{H}$ by

$$(1.2) \qquad (f\mid_k \gamma)(z) = \frac{(\det \gamma)^{k-1}}{j(\gamma, z)^k} f(\gamma z).$$

Then (1.2) is equivalent to $f\mid_k \gamma = f$ for all $\gamma \in \Gamma_0(N)$.

Note that the determinant factor $(\det \gamma)^{k-1}$ in our definition is different from the usual $(\det \gamma)^{k/2}$, which is an analytic normalization. Consequently, the central subgroup $\mathbb{Q}^\times \subseteq \mathrm{GL}_2^+(\mathbb{Q})$ acts by $f\mid_k \gamma = \gamma^{k-2}f$.

Remark 1.3. For simplicity we treat only the case of $\Gamma_0(N)$-level structure in this article. If desired, one could without difficulty extend our methods to more general level structures with characters, and so on.

The $\mathbb{C}$-vector space of modular forms of weight k and level N is finite-dimensional and is denoted $M_k(N)$.

If $f \in M_k(N)$, then $f(z+1) = f(z)$ so f has a Fourier expansion

$$(1.4) \qquad f(z) = \sum_{n=0}^{\infty} a_n q^n = a_0 + a_1 q + a_2 q^2 + a_3 q^3 + \dots$$

where $a_n \in \mathbb{C}$ and $q = \exp(2\pi i z)$.

We say that f is a *cusp form* if $f(z) \to 0$ as z tends to any cusp (i.e., f vanishes at the cusps). The $\mathbb{C}$-vector space of cusp forms of weight k and level N is denoted $S_k(N)$. We have $M_k(N) = S_k(N) \oplus E_k(N)$ where $E_k(N)$ is spanned by the Eisenstein series of level N. Note that when $k \geq 2$ is even, then (1.1) is equivalent to

$$f(\gamma z)\,(d(\gamma z))^{k/2} = f(z)\,(dz)^{k/2}$$

so one may equivalently think of a cusp form $f \in S_k(N)$ as a holomorphic differential $k/2$-form on the *modular curve* $X_0(N) = \Gamma_0(N)\backslash\mathcal{H}^*$. (When k is odd, one must take be careful about taking the square root.) More generally, the action of $\Gamma_0(N)$ on $\mathcal{H} \times \mathbb{C}$ by

$$(z, v) \mapsto \left(\gamma z, \frac{j(\gamma, z)^k}{(\det \gamma)^{k-1}} v\right)$$

for $\gamma \in \Gamma_0(N)$ and $(z, v) \in \mathcal{H} \times \mathbb{C}$, gives rise to a line bundle on $X_0(N) = \Gamma_0(N)\backslash\mathcal{H}$ whose sections are precisely $S_k(N)$. These sections agree with differential forms up to a twist by a power of the determinant (largely invisible here as the determinant restricted to $\Gamma_0(N)$ is trivial); our normalization is more convenient in algebraic contexts, but in any case the Hecke module structure is the same.

The spaces $M_k(N)$ and $S_k(N)$ are equipped with an action of pairwise commuting diagonalizable *Hecke operators* T_n for each integer $n \in \mathbb{Z}_{>0}$. The Hecke operators can be thought of in several different ways: they arise from correspondences on the modular curve $X_0(N)$, as "averaging" operators over lattices of index n, or more formally from double coset decompositions for the group $\Gamma_0(N)$ inside $\mathrm{SL}_2(\mathbb{Z})$. The action of the Hecke operator T_n is determined by the action of T_p for $p \mid n$, and the latter for $p \nmid N$ in weight k are given simply by the formula

$$(T_p f)(z) = p^{k-1} f(pz) + \frac{1}{p}\sum_{a=0}^{p-1} f\left(\frac{z+a}{p}\right).$$

3

(For primes $p \mid N$ one omits the first term, and there are also operators called *Atkin-Lehner involutions*.) We say therefore that $S_k(N)$ is a *Hecke module*, namely, an abelian group equipped with an action of the *Hecke algebra* $\widetilde{\mathbb{T}} = \mathbb{Z}[T_p]_p = \mathbb{Z}[T_2, T_3, \dots]$, a polynomial ring in countably many variables over $\mathbb{Z}$ indexed by the primes. Our Hecke modules will always be finite-dimensional $\mathbb{C}$-vector spaces.

A form $f \in S_k(N)$ is an *oldform (at d)* if $f(z) = g(dz)$ for some $g \in S_k(M)$ with $M \mid N$ a proper divisor and $d \mid N/M$; we say f is a *newform* if f is a normalized eigenform which is orthogonal to the space of oldforms (with respect to the Petersson inner product).

The space $S_k(N)$ consequently has a basis of *eigenforms*, i.e., functions that are eigenfunctions for each Hecke operator T_n. If f is an eigenform, *normalized* so that $a_1 = 1$ in its q-expansion (1.4), then $T_n f = a_n f$. Moreover, the field $\mathbb{Q}(\{a_n\}) = E \subseteq \mathbb{C}$ is a number field and each *Hecke eigenvalue* a_n is an algebraic integer in E.

In this way, the system of Hecke eigenvalues $(a_p)_p$ for a normalized eigenform $f \in S_k(N)$ determine the form $f : \mathcal{H} \to \mathbb{C}$. These eigenvalues also determine the L-series

$$L(f, s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s} = \prod_{p \nmid N} \left(1 - \frac{a_p}{p^s} + \frac{1}{p^{2s+1-k}} \right)^{-1} \prod_{p \mid N} \left(1 - \frac{a_p}{p^s} \right)^{-1}$$

associated to f (defined for $\mathrm{Re}\, s > 1$), as well as the ℓ-adic Galois representations

$$\rho_{f,\ell} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\overline{\mathbb{Z}}_\ell)$$

associated to f with the property that for any prime $p \nmid \ell N$, we have

$$\mathrm{Tr}(\rho_{f,\ell}(\mathrm{Frob}_p)) = a_p(f) \quad \text{and} \quad \det(\rho_{f,\ell}(\mathrm{Frob}_p)) = p^{k-1}.$$

Several methods have been proposed for making the Hecke module $S_k(N)$ into an object amenable to explicit computation. With a view to their generalizations to Hilbert modular forms, we mention two approaches which have seen wide application. (We neglect the method of graphs [48] and a method which uses the Eichler-Selberg trace formula [35].) For simplicity, we restrict our discussion to the case of weight $k = 2$.

The first method goes by the name *modular symbols* and has been developed by Birch, Swinnerton-Dyer, Manin, Mazur, Merel, Cremona [9], Stein [66], and many others. The Hecke operators T_p act naturally on the integral homology $H_1(X_0(N), \mathbb{Z}; \mathrm{cusps})$—linear combinations of paths in the completed upper half plane $\mathcal{H}^*$ whose endpoints are cusps and whose images in $X_0(N)$ are linear combinations of loops—and integration defines a nondegenerate Hecke-equivariant pairing which gives rise to an isomorphism (the Eichler-Shimura theorem)

$$H_1(X_0(N), \mathbb{C}; \mathrm{cusps}) \cong S_2(N) \oplus \overline{S_2(N)}$$

where $^-$ denotes complex conjugation. The formalism of modular symbols then presents the space $H_1(X_0(N), \mathbb{Z}; \mathrm{cusps})$ explicitly in terms of paths in $\mathcal{H}^*$ whose endpoints are cusps (elements of $\mathbb{P}^1(\mathbb{Q})$) and whose images in $X_0(N)$ are a linear combination of loops. We have an explicit description of the action of the Hecke operators on the space of modular symbols, and the *Manin trick* (the Euclidean algorithm) yields an algorithm for writing an arbitrary modular symbol as a $\mathbb{Z}$-linear combination of a finite set of generating symbols, thereby recovering $S_2(N)$ as a Hecke module.

The second method goes by the name *Brandt matrices* and goes back to Brandt, Eichler [23, 24], Pizer [50], Kohel [45], and others. In this approach, a basis for $S_2(N)$ is obtained by linear combinations of theta series associated to (right) ideals in a quaternion order of

4

discriminant N. These theta series are generating series which encode the number of elements in the ideal with a given reduced norm, and the Brandt matrices which represent the action of the Hecke operators are obtained via this combinatorial (counting) data.

2. Classical Hilbert modular forms

We now consider the situation where the classical modular forms from the previous section are replaced by forms over a totally real field. References for Hilbert modular forms include Freitag [25], van der Geer [26] and Goren [29].

Let F be a totally real field with $[F : \mathbb{Q}] = n$ and let $\mathbb{Z}_F$ be its ring of integers. The case $n = 1$ gives $F = \mathbb{Q}$ and this was treated in the previous section, so we assume throughout this section that $n > 1$. Let $v_1, \ldots, v_n : F \to \mathbb{R}$ be the real places of F, and write $v_i(x) = x_i$. For $\gamma \in \mathrm{M}_2(F)$ we write $\gamma_i = v_i(\gamma) \in \mathrm{M}_2(\mathbb{R})$.

For simplicity, in these first few sections (§§2–6) we assume that F has strict class number 1; the general case, which is more technical, is treated in §7 and thereafter.

The group
$$\mathrm{GL}_2^+(F) = \{\gamma \in \mathrm{GL}_2(F) : \det \gamma_i > 0 \text{ for } i = 1, \ldots, n\}$$
acts naturally on $\mathcal{H}^n$ by coordinatewise linear fractional transformations
$$z \mapsto \gamma z = (\gamma_i z_i)_i = \left(\frac{a_i z_i + b_i}{c_i z_i + d_i}\right)_{i=1,\ldots,n}.$$

For a nonzero ideal $\mathfrak{N} \subseteq \mathbb{Z}_F$, let
$$\Gamma_0(\mathfrak{N}) = \left\{\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2^+(\mathbb{Z}_F) : c \in \mathfrak{N}\right\} \subseteq \mathrm{GL}_2^+(\mathbb{Z}_F) \subseteq \mathrm{GL}_2(F).$$

Let $\mathrm{P}\Gamma_0(\mathfrak{N}) = \Gamma_0(\mathfrak{N})/\mathbb{Z}_F^\times \subseteq \mathrm{PGL}_2^+(\mathbb{Z}_F)$. Then the image of $\mathrm{P}\Gamma_0(\mathfrak{N})$ under the embeddings $\gamma \mapsto (\gamma_i)_i$ is a discrete subgroup of $\mathrm{PGL}_2^+(\mathbb{R})^n$.

Under the assumption that F has strict class number 1, we have
$$\mathbb{Z}_{F,+}^\times = \{x \in \mathbb{Z}_F^\times : x_i > 0 \text{ for all } i\} = \mathbb{Z}_F^{\times 2}$$
and hence $\mathrm{GL}_2^+(\mathbb{Z}_F) = \mathbb{Z}_F^\times \mathrm{SL}_2(\mathbb{Z}_F)$, and so alternatively we may identify
$$\mathrm{P}\Gamma_0(\mathfrak{N}) \cong \left\{\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}_F) : c \in \mathfrak{N}\right\}/\{\pm 1\}$$
in analogy with the case $F = \mathbb{Q}$.

Definition 2.1. *A* Hilbert modular form *of parallel weight 2 and level $\mathfrak{N}$ is a holomorphic function $f : \mathcal{H}^n \to \mathbb{C}$ such that*

$$(2.2) \qquad f(\gamma z) = f\left(\frac{a_1 z_1 + b_1}{c_1 z_1 + d_1}, \ldots, \frac{a_n z_n + b_n}{c_n z_n + d_n}\right) = \left(\prod_{i=1}^n \frac{(c_i z_i + d_i)^2}{\det \gamma_i}\right) f(z)$$

for all $\gamma \in \Gamma_0(\mathfrak{N})$.

We denote by $M_2(\mathfrak{N})$ the space of Hilbert modular forms of parallel weight 2 and level $\mathfrak{N}$; it is a finite-dimensional $\mathbb{C}$-vector space. The reader is warned not to confuse $M_2(\mathfrak{N})$ with the ring $\mathrm{M}_2(R)$ of 2×2-matrices over a ring R.

Remark 2.3. There is no holomorphy condition at the cusps in Definition 2.1 as there was for classical modular forms. Indeed, under our assumption that $[F : \mathbb{Q}] = n > 1$, this follows automatically from Koecher's principle [26, §1].

Note also that if $u \in \mathbb{Z}_F^\times$, then $\gamma(u) = \begin{pmatrix} u & 0 \\ 0 & u \end{pmatrix} \in \mathrm{GL}_2^+(\mathbb{Z}_F)$ acts trivially on $\mathcal{H}$ and at the same time gives a vacuous condition in (2.2), explaining the appearance of the determinant term which was missing in the classical case.

Analogous to (1.2), we define

$$(2.4) \qquad (f \mid \gamma)(z) = \left(\prod_{i=1}^n \frac{\det \gamma_i}{j(\gamma_i, z)^2} \right) f(\gamma z)$$

for $f : \mathcal{H}^n \to \mathbb{C}$ and $\gamma \in \mathrm{GL}_2^+(F)$; then (2.2) is equivalent to $(f \mid \gamma)(z) = f(z)$ for all $\gamma \in \Gamma_0(\mathfrak{N})$.

The group $\mathrm{GL}_2^+(F)$ also acts naturally on the *cusps* $\mathbb{P}^1(F) \hookrightarrow \mathbb{P}^1(\mathbb{R})^n$. We say that $f \in M_2(\mathfrak{N})$ is a *cusp form* if $f(z) \to 0$ whenever z tends to a cusp, and we denote the space of cusp forms (of parallel weight 2 and level $\mathfrak{N}$) by $S_2(\mathfrak{N})$. We have an orthogonal decomposition $M_2(\mathfrak{N}) = S_2(\mathfrak{N}) \oplus E_2(\mathfrak{N})$ where $E_2(\mathfrak{N})$ is spanned by Eisenstein series of level $\mathfrak{N}$; for level $\mathfrak{N} = (1)$, we have $\dim E_2(1) = \# \mathrm{Cl}^+ \mathbb{Z}_F$, where $\mathrm{Cl}^+ \mathbb{Z}_F$ denotes the strict class group of $\mathbb{Z}_F$.

Hilbert modular forms admit Fourier expansions as follows. For a fractional ideal $\mathfrak{b}$ of F, let

$$\mathfrak{b}_+ = \{x \in \mathfrak{b} : x_i > 0 \text{ for } i = 1, \ldots, n\}.$$

Let $\mathfrak{d}$ be the different of F, and let $\mathfrak{d}^{-1}$ denote the inverse different. A Hilbert modular form $f \in M_2(\mathfrak{N})$ admits a Fourier expansion

$$(2.5) \qquad f(z) = a_0 + \sum_{\mu \in (\mathfrak{d}^{-1})_+} a_\mu e^{2\pi i \, \mathrm{Tr}(\mu z)}.$$

with $a_0 = 0$ if f is a cusp form.

Let $f \in M_2(\mathfrak{N})$ and let $\mathfrak{n} \subseteq \mathbb{Z}_F$ be a nonzero ideal. Then under our hypothesis that F has strict class number 1, we may write $\mathfrak{n} = \nu \mathfrak{d}$ for some $\nu \in \mathfrak{d}_+$; we then define $a_\mathfrak{n} = a_\nu$. The transformation rule (2.2) implies that $a_\mathfrak{n}$ does not depend on the choice of ν, and we call $a_\mathfrak{n}$ the *Fourier coefficient* of f at $\mathfrak{n}$.

The spaces $M_2(\mathfrak{N})$ and $S_2(\mathfrak{N})$ are also equipped with an action of pairwise commuting diagonalizable *Hecke operators* $T_\mathfrak{n}$ indexed by the nonzero ideals $\mathfrak{n}$ of $\mathbb{Z}_F$. For example, given a prime $\mathfrak{p} \nmid \mathfrak{N}$ and a totally positive generator p of $\mathfrak{p}$ we have

$$(2.6) \qquad (T_\mathfrak{p} f)(z) = N(\mathfrak{p}) f(pz) + \frac{1}{N(\mathfrak{p})} \sum_{a \in \mathbb{F}_\mathfrak{p}} f\left(\frac{z+a}{p} \right),$$

where $\mathbb{F}_\mathfrak{p} = \mathbb{Z}_F/\mathfrak{p}$ is the residue field of $\mathfrak{p}$; this definition is indeed independent of the choice of generator p. Using the notation (2.4), we can equivalently write

$$(2.7) \qquad (T_\mathfrak{p} f)(z) = \sum_{a \in \mathbb{P}^1(\mathbb{F}_\mathfrak{p})} (f \mid \pi_a)(z)$$

where $\pi_\infty = \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}$ and $\pi_a = \begin{pmatrix} 1 & a \\ 0 & p \end{pmatrix}$ for $a \in \mathbb{F}_{\mathfrak{p}}$.

If $f \in S_2(\mathfrak{N})$ is an eigenform, *normalized* so that $a_{(1)} = 1$, then $T_{\mathfrak{n}}f = a_{\mathfrak{n}}f$, and each eigenvalue $a_{\mathfrak{n}}$ is an algebraic integer which lies in the number field $E = \mathbb{Q}(\{a_{\mathfrak{n}}\}) \subseteq \mathbb{C}$ (see Shimura [60, Section 2]) generated by the Fourier coefficients of f. We again have notions of *oldforms* and *newforms*, analogously defined (so that a newform is in particular a normalized eigenform).

Associated to an eigenform $f \in S_2(\mathfrak{N})$ we have an *L-function*

$$L(f, s) = \sum_{\mathfrak{n}} \frac{a_{\mathfrak{n}}}{N\mathfrak{n}^s}$$

and $\mathfrak{l}$-adic Galois representations

$$\rho_{f,\mathfrak{l}} : \mathrm{Gal}(\overline{F}/F) \to \mathrm{GL}_2(\overline{\mathbb{Z}}_{F,\mathfrak{l}})$$

for primes $\mathfrak{l}$ of $\mathbb{Z}_F$ such that, for any prime $\mathfrak{p} \nmid \mathfrak{N}$, we have

$$\mathrm{Tr}(\rho_{f,\mathfrak{l}}(\mathrm{Frob}_{\mathfrak{p}})) = a_{\mathfrak{p}}(f) \quad \text{and} \quad \det(\rho_{f,\mathfrak{l}}(\mathrm{Frob}_{\mathfrak{p}})) = N\mathfrak{p}.$$

Each of these is determined by the Hecke eigenvalues $a_{\mathfrak{n}}$ of f, so we are again content to compute $S_2(\mathfrak{N})$ as a Hecke module.

We are now ready to state the first version of our main result.

Theorem 2.8 (Dembélé [15], Greenberg-Voight [30]). *There exists an algorithm which, given a totally real field F of strict class number 1 and a nonzero ideal $\mathfrak{N} \subseteq \mathbb{Z}_F$, computes the space $S_2(\mathfrak{N})$ of Hilbert cusp forms of parallel weight 2 and level $\mathfrak{N}$ over F as a Hecke module.*

In other words, there exists an explicit finite procedure which takes as input the field F and the ideal $\mathfrak{N} \subseteq \mathbb{Z}_F$ encoded in bits (in the usual way, see e.g. Cohen [7]), and outputs a finite set of sequences $(a_{\mathfrak{p}}(f))_{\mathfrak{p}}$ encoding the Hecke eigenvalues for each cusp form constituent f in $S_2(\mathfrak{N})$, where $a_{\mathfrak{p}}(f) \in E_f \subseteq \overline{\mathbb{Q}}$. (This algorithm will produce any finite subsequence in a finite amount of time, but in theory will produce the entire sequence if it is left to run forever.) Alternatively, this algorithm can simply output matrices for the Hecke operators $T_{\mathfrak{p}}$; one recovers the constituent forms using linear algebra.

Example 2.9. Let $F = \mathbb{Q}(\sqrt{5})$. Then $\mathbb{Z}_F = \mathbb{Z}[w]$ where $w = (1+\sqrt{5})/2$ satisfying $w^2 - w - 1 = 0$. Let $\mathfrak{N} = (3w - 14) \subseteq \mathbb{Z}_F$; we have $N(\mathfrak{N}) = 229$ is prime. We compute that $\dim S_2(\mathfrak{N}) = 4$. There are 2 Hecke irreducible subspaces of dimensions 1 and 3, corresponding to newforms f and g (and its Galois conjugates). We have the following table of eigenvalues; we write $\mathfrak{p} = (p)$ for $p \in \mathbb{Z}_F$.

$\mathfrak{p}$	(2)	$(w+2)$	(3)	$(w+3)$	$(w-4)$
$N\mathfrak{p}$	4	5	9	11	11
$a_{\mathfrak{p}}(f)$	-3	-4	-1	0	-2
$a_{\mathfrak{p}}(g)$	t	$t^2 - 4t + 1$	$-t^2 + 2t + 2$	$t^2 - 2t - 3$	$-3t^2 + 8t + 1$

Here, the element $t \in \overline{\mathbb{Q}}$ satisfies $t^3 - 3t^2 - t + 1 = 0$ and $E = \mathbb{Q}(t)$ is an S_3-field of discriminant 148.

Recall that in the method of modular symbols, a cusp form $f \in S_2(N)$ corresponds to a holomorphic differential (1-)form $(2\pi i)f(z)\,dz$ on $X_0(N)$ and so, by the theorem of Eichler-Shimura, arises naturally in the space $H^1(X_0(N), \mathbb{C})$. In a similar way, a Hilbert cusp form $f \in S_2(\mathfrak{N})$ gives rise to a holomorphic differential n-form $(2\pi i)^n f(z_1, \ldots, z_n)\,dz_1 \cdots dz_n$ on the *Hilbert modular variety* $X_0(\mathfrak{N})$, the desingularization of the compact space $\Gamma_0(\mathfrak{N})\backslash(\mathcal{H}^n)^*$ where $(\mathcal{H}^n)^* = \mathcal{H}^n \cup \mathbb{P}^1(F)$. But now $X_0(\mathfrak{N})$ is an algebraic variety of complex dimension n and f arises in the cohomology group $H^n(X_0(\mathfrak{N}), \mathbb{C})$. Computing with higher dimensional varieties (and higher degree cohomology groups) is not an easy task! So we seek an alternative approach.

Langlands functoriality predicts that $S_2(\mathfrak{N})$ as a Hecke module occurs in the cohomology of other "modular" varieties as well. This functoriality was already evident by the fact that both modular symbols and their quaternionic variant, Brandt matrices, can be used to compute the classical space $S_2(N)$. In our situation, this functoriality is known as the Jacquet-Langlands correspondence, which ultimately will allow us to work with varieties of complex dimension 1 or 0 by considering twisted forms of GL_2 over F arising from quaternion algebras. In dimension 1, we will arrive at an algorithm which works in the cohomology of a Shimura curve, analogous to a modular curve, and thereby give a kind of analogue of modular symbols; in dimension 0, we generalize Brandt matrices by working with theta series on (totally definite) quaternion orders.

3. Quaternionic modular forms

In this section, we define modular forms on quaternion algebras; our main reference is Hida [34]. We retain the notation of the previous section; in particular, F is a totally real field of degree $[F : \mathbb{Q}] = n$ with ring of integers $\mathbb{Z}_F$.

A *quaternion algebra* B over F is a central simple algebra of dimension 4. Equivalently, a quaternion algebra B over F is an F-algebra generated by elements i, j satisfying

$$(3.1) \qquad i^2 = a, \quad j^2 = b, \quad \text{and} \quad ji = -ij$$

for some $a, b \in F^\times$; we denote such an algebra $B = \left(\dfrac{a, b}{F}\right)$. For more information about quaternion algebras, see Vignéras [68].

Let B be a quaternion algebra over F. Then B has a unique involution $\overline{} : B \to B$ called *conjugation* such that $x\overline{x} \in F$ for all $x \in B$; we define the *reduced norm* of x to be $\mathrm{nrd}(x) = x\overline{x}$. For $B = \left(\dfrac{a, b}{F}\right)$ as in (3.1) and $x = u + vi + zj + wij \in B$, we have

$$\overline{x} = u - (vi + zj + wij) \quad \text{and} \quad \mathrm{nrd}(x) = u^2 - av^2 - bz^2 + abw^2.$$

A $\mathbb{Z}_F$-*lattice* of B is a finitely generated $\mathbb{Z}_F$-submodule I of B such that $FI = B$. An *order* $\mathcal{O}$ of B is a $\mathbb{Z}_F$-lattice which is also a subring of B. A *maximal order* of B is an order which is not properly contained in any other order. Let $\mathcal{O}_0(1) \subseteq B$ be a maximal order in B.

A *right fractional* $\mathcal{O}$-*ideal* is a $\mathbb{Z}_F$-lattice I such that its *right order* $\mathcal{O}_R(I) = \{x \in B : xI \subseteq I\}$ is equal to $\mathcal{O}$; left ideals are defined analogously.

Let $K \supset F$ be a field containing F. Then $B_K = B \otimes_F K$ is a quaternion algebra over K, and we say K *splits* B if $B_K \cong \mathrm{M}_2(K)$.

Let v be a noncomplex place of F, and let F_v denote the completion of F at v. Then there is a unique quaternion algebra over F_v which is a division ring, up to isomorphism. We say B is *unramified* (or *split*) at v if F_v splits B, otherwise we say B is *ramified* at v. The set S of ramified places of B is a finite set of even cardinality which characterizes B up to isomorphism, and conversely given any such set S there is a quaternion algebra over B ramified exactly at the places in S. We define the *discriminant* $\mathfrak{D}$ of B to be the ideal of $\mathbb{Z}_F$ given by the product of all finite ramified places of B.

Let $\mathfrak{N} \subseteq \mathbb{Z}_F$ be an ideal which is coprime to the discriminant $\mathfrak{D}$. Then there is an isomorphism

$$\iota_{\mathfrak{N}} : \mathcal{O}_0(1) \hookrightarrow \mathcal{O}_0(1) \otimes_{\mathbb{Z}_F} \mathbb{Z}_{F,\mathfrak{N}} \cong \mathrm{M}_2(\mathbb{Z}_{F,\mathfrak{N}})$$

where $\mathbb{Z}_{F,\mathfrak{N}}$ denotes the completion of $\mathbb{Z}_F$ at $\mathfrak{N}$. Let

$$\mathcal{O}_0(\mathfrak{N}) = \{x \in \mathcal{O}_0(1) : \iota_{\mathfrak{N}}(x) \text{ is upper triangular modulo } \mathfrak{N}\};$$

the order $\mathcal{O}_0(\mathfrak{N})$ is called an *Eichler order* of level $\mathfrak{N}$. We will abbreviate $\mathcal{O} = \mathcal{O}_0(\mathfrak{N})$.

We number the real places $v_1, \ldots, v_n$ of F so that B is split at $v_1, \ldots, v_r$ and ramified at $v_{r+1}, \ldots, v_n$, so that

$$B \otimes_{\mathbb{Q}} \mathbb{R} \cong \mathrm{M}_2(\mathbb{R})^r \times \mathbb{H}^{n-r}$$

where $\mathbb{H} = \left(\dfrac{-1, -1}{\mathbb{R}}\right)$ is the division ring of Hamiltonians. If B is ramified at all real places (i.e. $r = 0$) then we say that B is *(totally) definite*, and otherwise we say B is *indefinite*. The arithmetic properties of the algebra B and its forms are quite different according as B is definite or indefinite, and so we consider these two cases separately. Using an adelic language, one can treat them more uniformly (though to some extent this merely repackages the difference)—we refer to §8 for this approach.

First, suppose that B is indefinite, so that $r > 0$. The case $B \cong \mathrm{M}_2(\mathbb{Q})$ corresponds to the classical case of elliptic modular forms; this was treated in §1, so we assume $B \ncong \mathrm{M}_2(\mathbb{Q})$. Let

$$\iota_{\infty} : B \hookrightarrow \mathrm{M}_2(\mathbb{R})^r$$

denote the map corresponding to the split embeddings $v_1, \ldots, v_r$. Then the group

$$B_+^{\times} = \{\gamma \in B^{\times} : \det \gamma_i = (\mathrm{nrd}\,\gamma)_i > 0 \text{ for } i = 1, \ldots, r\}$$

acts on $\mathcal{H}^r$ by coordinatewise linear fractional transformations. Let

$$\mathcal{O}_+^{\times} = \mathcal{O}^{\times} \cap B_+^{\times}.$$

Under the assumption that F has strict class number 1, which we maintain, we have

$$\mathcal{O}_+^{\times} = \mathbb{Z}_F^{\times} \mathcal{O}_1^{\times}$$

where $\mathcal{O}_1^{\times} = \{\gamma \in \mathcal{O} : \mathrm{nrd}(\gamma) = 1\}$. Let

$$\Gamma = \Gamma_0^B(\mathfrak{N}) = \iota_{\infty}(\mathcal{O}_+^{\times}) \subseteq \mathrm{GL}_2^+(\mathbb{R})^r.$$

and let $\mathrm{P}\Gamma = \Gamma/\mathbb{Z}_F^{\times}$. Then $\mathrm{P}\Gamma$ is a discrete subgroup of $\mathrm{PGL}_2^+(\mathbb{R})^r$ which can be identified with

$$\mathrm{P}\Gamma \cong \iota_{\infty}(\mathcal{O}_1^{\times})/\{\pm 1\} \subseteq \mathrm{PSL}_2(\mathbb{R}).$$

9

Definition 3.2. *Let B be indefinite. A* quaternionic modular form *for B of parallel weight 2 and level $\mathfrak{N}$ is a holomorphic function $f : \mathcal{H}^r \to \mathbb{C}$ such that*

$$(3.3) \qquad f(\gamma z) = f\left(\frac{a_1 z_1 + b_1}{c_1 z_1 + d_1}, \ldots, \frac{a_r z_r + b_r}{c_r z_r + d_r}\right) = \left(\prod_{i=1}^{r} \frac{(c_i z_i + d_i)^2}{\det \gamma_i}\right) f(z)$$

for all $\gamma \in \Gamma_0^B(\mathfrak{N})$.

Analogous to (2.4), we define

$$(3.4) \qquad (f \mid \gamma)(z) = f(\gamma z) \prod_{i=1}^{r} \frac{\det \gamma_i}{j(\gamma_i, z)^2}$$

for $f : \mathcal{H}^r \to \mathbb{C}$ and $\gamma \in B_+^\times$; then (3.3) is equivalent to $(f \mid \gamma)(z) = f(z)$ for all $\gamma \in \Gamma_0^B(\mathfrak{N})$.

We denote by $M_2^B(\mathfrak{N})$ the space of quaternionic modular forms for B of parallel weight 2 and level $\mathfrak{N}$, a finite-dimensional $\mathbb{C}$-vector space.

A quaternionic modular form for $B = \mathrm{M}_2(F)$ is exactly a Hilbert modular form over F; our presentation in these three sections has been consciously redundant so as to emphasize this similarity. (We could recover the definition of cusp forms given in Section 1 if we also impose the condition that the form vanish at the cusps.) As we will see later, this similarity is less apparent when the general and more technical theory is exposited.

The Hecke operators are defined on $M_2^B(\mathfrak{N})$ following their definition in (2.7). Let $\mathfrak{p}$ be a prime of $\mathbb{Z}_F$ with $\mathfrak{p} \nmid \mathfrak{D}\mathfrak{N}$, and let p be a totally positive generator of $\mathfrak{p}$. Define

$$\Theta(\mathfrak{p}) = \mathcal{O}_+^\times \backslash \{\pi \in \mathcal{O}_+ : \mathrm{nrd}(\pi)\mathbb{Z}_F = \mathfrak{p}\} = \mathcal{O}_+^\times \backslash \{\pi \in \mathcal{O}_+ : \mathrm{nrd}(\pi) = p\}.$$

The set $\Theta(\mathfrak{p})$ has cardinality $N\mathfrak{p} + 1$. The Hecke operator $T_\mathfrak{p}$ is then given by

$$(3.5) \qquad (T_\mathfrak{p} f)(z) = \sum_{\pi \in \Theta(\mathfrak{p})} (f \mid \pi)(z).$$

The set $\Theta(\mathfrak{p})$ admits an explicit description as follows. As above, let $\mathbb{F}_\mathfrak{p} = \mathbb{Z}_F / \mathfrak{p}$ be the residue field of $\mathfrak{p}$, and let $\iota_\mathfrak{p} : \mathcal{O} \hookrightarrow \mathrm{M}_2(\mathbb{Z}_{F,\mathfrak{p}})$ be a splitting. Then the set $\Theta(\mathfrak{p})$ is in bijection with the set of left ideals of $\mathcal{O}$ by $\pi \mapsto \mathcal{O}\pi$. This set of left ideals is in bijection [41, Lemma 6.2] with the set $\mathbb{P}^1(\mathbb{F}_\mathfrak{p})$: explicitly, given the splitting $\iota_\mathfrak{p}$, the left ideal corresponding to $a = (x : y) \in \mathbb{P}^1(\mathbb{F}_\mathfrak{p})$ is

$$(3.6) \qquad J_a = \mathcal{O}\iota_\mathfrak{p}^{-1}\begin{pmatrix} x & y \\ 0 & 0 \end{pmatrix} + \mathcal{O}\mathfrak{p}.$$

By strong approximation [68, Théorème III.4.3], each of the ideals J_a is principal, so $J_a = \mathcal{O}\pi_a$ with $\mathrm{nrd}(\pi_a) = p$ for all $a \in \mathbb{P}^1(\mathbb{F}_\mathfrak{p})$. Therefore, we have $\Theta(\mathfrak{p}) = \{\pi_a : a \in \mathbb{P}^1(\mathbb{F}_\mathfrak{p})\}$.

This definition reduces to the one given in (2.7) for Hilbert modular forms with the choices $\pi_\infty = \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}$ and $\pi_a = \begin{pmatrix} 1 & a \\ 0 & p \end{pmatrix}$ for $a \in \mathbb{F}_\mathfrak{p}$.

Having treated Hilbert modular forms in the previous section, now suppose that $B \not\cong \mathrm{M}_2(F)$, or equivalently that B is a division ring. Then a modular form is vacuously a cusp form as there are no cusps! We then refer to quaternionic modular forms equally well as *quaternionic cusp forms* and let $S_2^B(\mathfrak{N}) = M_2^B(\mathfrak{N})$. Here, a cusp form f gives a holomorphic differential r-form $(2\pi i)^r f(z_1, \ldots, z_r) \, dz_1 \cdots dz_r$ on the associated *quaternionic Shimura variety* $X_0^B(\mathfrak{N}) = \Gamma_0^B(\mathfrak{N}) \backslash \mathcal{H}^r$, a complex variety of dimension r.

The important case for us will be when $r = 1$. Then $\Gamma_0^B(\mathfrak{N}) \subseteq \mathrm{PGL}_2^+(\mathbb{R})$ acts on the upper half-plane and the quotient $\Gamma_0^B(\mathfrak{N}) \backslash \mathcal{H}$ can be given the structure of a Riemann surface, known as a *Shimura curve*. In this simple case, a cusp form for B is simply a holomorphic map $f : \mathcal{H} \to \mathbb{C}$ such that $f(\gamma z) = (c_1 z + d_1)^2 f(z)$ for all $\gamma \in \Gamma_0^B(\mathfrak{N})$, where $\gamma_1 = v_1(\gamma) = \begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix}$ and v_1 is the unique split real place of F.

Next, suppose that B is definite, so that $r = 0$. Recall that $\mathcal{O} = \mathcal{O}_0(\mathfrak{N}) \subseteq \mathcal{O}_0(1)$ is an Eichler order of level $\mathfrak{N}$. A right fractional $\mathcal{O}$-ideal is *invertible* if there exists a left fractional $\mathcal{O}$-ideal I^{-1} such that $I^{-1}I = \mathcal{O}$, or equivalently if I is *locally principal*, i.e., for each (finite) prime ideal $\mathfrak{p}$ of $\mathbb{Z}_F$, the ideal $I_\mathfrak{p}$ is a principal right $\mathcal{O}_\mathfrak{p}$-ideal. If I is invertible, then necessarily $I^{-1} = \{x \in B : xI \subseteq \mathcal{O}\}$.

Let I, J be invertible right fractional $\mathcal{O}$-ideals. We say that I and J are in the same *right ideal class* (or are *isomorphic*) if there exists an $x \in B^\times$ such that $I = xJ$, or equivalently if I and J are isomorphic as right $\mathcal{O}$-modules. We write $[I]$ for the equivalence class of I under this relation and denote the set of invertible right $\mathcal{O}$-ideal classes by $\mathrm{Cl}\,\mathcal{O}$. The set $\mathrm{Cl}\,\mathcal{O}$ is finite and $H = \#\,\mathrm{Cl}\,\mathcal{O}$ is independent of the choice of Eichler order $\mathcal{O} = \mathcal{O}_0(\mathfrak{N})$ of level $\mathfrak{N}$.

Definition 3.7. *Let B be definite. A* quaternionic modular form *for B of parallel weight 2 and level $\mathfrak{N}$ is a map*
$$f : \mathrm{Cl}\,\mathcal{O}_0(\mathfrak{N}) \to \mathbb{C}.$$

The space of quaternionic modular forms $M_2^B(\mathfrak{N})$ is obviously a $\mathbb{C}$-vector space of dimension equal to H.

A modular form for B which is orthogonal to the (1-dimensional) subspace of constant functions is called a *cusp form* for B; the space of such forms is denoted $S_2^B(\mathfrak{N})$.

The Hecke operators are defined on $M_2^B(\mathfrak{N})$ as follows. Let $\mathfrak{p}$ be a prime ideal of $\mathbb{Z}_F$ with $\mathfrak{p} \nmid \mathfrak{N}$. For a right $\mathcal{O}$-ideal I with $\mathrm{nrd}(I)$ coprime to $\mathfrak{p}$, the Hecke operator $T_\mathfrak{p}$ is given by

(3.8)
$$(T_\mathfrak{p} f)([I]) = \sum_{\substack{J \subseteq I \\ \mathrm{nrd}(JI^{-1}) = \mathfrak{p}}} f([J]),$$

the sum over all invertible right $\mathcal{O}$-ideals $J \subseteq I$ such that $\mathrm{nrd}(J) = \mathfrak{p}\,\mathrm{nrd}(I)$. As in (3.5), this sum is also naturally over $\mathbb{P}^1(\mathbb{F}_\mathfrak{p})$, indexing the ideals of norm index $\mathfrak{p}$. This definition does not depend on the choice of representative I in its ideal class.

Consequent to the definitions in the previous paragraphs, we may now consider the Hecke modules of quaternionic cusp forms over F for the different quaternion algebras B over F. These spaces are related to each other, and thus to spaces of Hilbert modular forms, according to their arithmetic invariants by the *Jacquet-Langlands correspondence* as follows.

Theorem 3.9 (Eichler-Shimizu-Jacquet-Langlands)**.** *Let B be a quaternion algebra over F of discriminant $\mathfrak{D}$ and let $\mathfrak{N}$ be an ideal coprime to $\mathfrak{D}$. Then there is an injective map of Hecke modules*
$$S_2^B(\mathfrak{N}) \hookrightarrow S_2(\mathfrak{D}\mathfrak{N})$$
whose image consists of those Hilbert cusp forms which are new at all primes $\mathfrak{p} \mid \mathfrak{D}$.

Proof. See Jacquet and Langlands [36, Chap. XVI], Gelbart and Jacquet [27, §8] and work of Hida [32]; another useful reference is Hida [33, Proposition 2.12] who deduces Theorem 3.9 from the representation theoretic results of Jacquet and Langlands. $\square$

Theorem 3.9 yields an isomorphism

$$S_2^B(\mathfrak{N}) \cong S_2(\mathfrak{N})$$

when the quaternion algebra B has discriminant $\mathfrak{D} = (1)$. Since a quaternion algebra must be ramified at an even number of places, when $n = [F : \mathbb{Q}]$ is even we can achieve this for the definite quaternion algebra B which is ramified at exactly the real places of F (and no finite place). When n is odd, the simplest choice is to instead take B to be ramified at all but one real place of F (and still no finite place), and hence B is indefinite (and $g = 1$).

Remark 3.10. Note that in general a space of newforms can be realized as a Hecke module inside many different spaces of quaternionic cusp forms. Indeed, for any factorization $\mathfrak{M} = \mathfrak{D}\mathfrak{N}$ with $\mathfrak{D}$ squarefree and $\mathfrak{N}$ coprime to $\mathfrak{D}$, we consider a quaternion algebra B of discriminant $\mathfrak{D}$ (ramified at either all or all but one real place of F) and thereby realize $S_2^B(\mathfrak{N}) \cong S_2(\mathfrak{M})^{\mathfrak{D}\text{-new}}$. For example, if p, q are (rational) primes, then the space $S_2(pq)^{\text{new}}$ of classical newforms can, after splitting off old subspaces, be computed using an indefinite quaternion algebra of discriminant 1 or pq (corresponding to a modular curve or a Shimura curve, respectively) or a definite quaternion algebra of discriminant p or q.

Our main conclusion from this section is that to compute spaces of Hilbert cusp forms it suffices to compute instead spaces of quaternionic cusp forms. The explicit description of $S_2^B(\mathfrak{N})$ as a Hecke module varies according as if B is definite or indefinite.

4. DEFINITE METHOD

In this section, we discuss a method for computing Hilbert modular forms using a definite quaternion algebra B.

We continue with our notation and our assumption that F has strict class number 1; in particular, B is a definite quaternion algebra over F with discriminant $\mathfrak{D}$ and $\mathcal{O}$ is an Eichler order of level $\mathfrak{N}$. We accordingly call the method in this section the *definite method*: it is a generalization of the method of Brandt matrices mentioned briefly in §2 and was first exhibited by Eichler [22] and Pizer [50] for $F = \mathbb{Q}$, but the first explicit algorithm was given by Socrates and Whitehouse [62].

Let $I_1, \ldots, I_H$ be a set of representative right ideals for $\text{Cl}\,\mathcal{O}$, with $H = \#\,\text{Cl}\,\mathcal{O}$. As vector spaces, we have simply that

$$M_2^B(\mathfrak{N}) = \text{Map}(\text{Cl}\,\mathcal{O}, \mathbb{C}) \cong \bigoplus_{i=1}^H \mathbb{C}\,I_i,$$

associating to each ideal (class) its characteristic function. Let $\mathcal{O}_i = \mathcal{O}_L(I_i)$ be the left order of I_i and let $e_i = \#(\mathcal{O}_i^\times / \mathbb{Z}_F^\times)$.

The action of the Hecke operators is defined by (3.8): we define the $\mathfrak{p}$th-*Brandt matrix* $T(\mathfrak{p})$ for $\mathcal{O}$ to be the matrix whose (i, j)th entry is equal to

$$(4.1) \qquad b(\mathfrak{p})_{i,j} = \#\{J \subseteq I_j : \text{nrd}(JI_j^{-1}) = \mathfrak{p} \text{ and } [J] = [I_i]\} \in \mathbb{Z}.$$

The Brandt matrix $T(\mathfrak{p})$ is an $H \times H$-matrix with integral entries such that the sum of the entries in each column is equal to $N\mathfrak{p} + 1$. The Hecke operator $T_\mathfrak{p}$ then acts by $T(\mathfrak{p})$ on $\bigoplus_i \mathbb{C}I_i$ (on the right), identifying an ideal class with its characteristic function.

The Brandt matrix is just a compact way of writing down the adjacency matrix of the graph with vertices $X = \text{Cl}\,\mathcal{O}$ where there is a directed edge from I_i to each ideal class which represents an ideal of index $N\mathfrak{p}$ in I_i. Indeed, consider the graph whose vertices are right

$\mathcal{O}$-ideals of norm a power of $\mathfrak{p}$ and draw a directed edge from I to J if $\mathrm{nrd}(JI^{-1}) = \mathfrak{p}$. Then this graph is a k-regular tree with $N\mathfrak{p} + 1$ edges leaving each vertex. The above adjacency matrix is obtained by taking the quotient of this graph by identifying two ideals if they are in the same ideal class.

Alternatively, we may give an expression for the Brandt matrices in terms of elements instead of ideals. A containment $J \subseteq I_j$ of right $\mathcal{O}$-ideals with $[I_i] = [J]$ corresponds to an element $x \in JI_i^{-1} \subset I_j I_i^{-1}$ via $J = xI_i$, and we have $\mathrm{nrd}(JI_j^{-1}) = \mathfrak{p}$ if and only if $\mathrm{nrd}(x)\,\mathrm{nrd}(I_i)/\mathrm{nrd}(I_j) = \mathfrak{p}$.

Writing $JI_i^{-1} = x\mathcal{O}_i$, we see that x is unique up to multiplication on the right by $\mathcal{O}_i^\times$. We have $\mathcal{O}_i^\times = (\mathcal{O}_i)_1^\times \mathbb{Z}_F^\times$ and $(\mathcal{O}_i)_1^\times \cap \mathbb{Z}_F^\times = \{\pm 1\}$, so $2e_i = \#(\mathcal{O}_i)_1^\times$. To eliminate the contribution of the factor $\mathbb{Z}_F^\times$, we normalize as follows: let p be a totally positive generator for $\mathfrak{p}$ and similarly q_i for $\mathrm{nrd}(I_i)$ for $i = 1, \ldots, H$. Then $x \in I_j I_i^{-1}$ can be chosen so that $\mathrm{nrd}(x)(q_i/q_j) = p$ and is unique up to multiplication by $(\mathcal{O}_i)_1^\times$.

$$(4.2) \qquad b(\mathfrak{p})_{i,j} = \frac{1}{2e_i} \#\left\{ x \in I_j I_i^{-1} : \mathrm{nrd}(x)\frac{q_i}{q_j} = p \right\}.$$

The advantage of the expression (4.2) is that it can be expressed simply in terms of a quadratic form. Since B is definite, the space $B \hookrightarrow B \otimes_{\mathbb{Q}} \mathbb{R} \cong \mathbb{H}^n \cong \mathbb{R}^{4n}$ comes equipped with the positive definite quadratic form $\mathrm{Tr\,nrd} : B \to \mathbb{R}$. If J is a $\mathbb{Z}_F$-lattice, then $J \cong \mathbb{Z}^{4n}$ embeds as a Euclidean lattice $J \hookrightarrow \mathbb{R}^{4n}$ with respect to this quadratic form. It follows that one can compute $b(\mathfrak{p})_{i,j}$ by computing all elements $x \in I_i I_j^{-1}$ such that $\mathrm{Tr}(q_j/q_i)\,\mathrm{nrd}(x) \le \mathrm{Tr}\,p$, a finite set.

Before giving references for the technical details about how the Brandt matrices above are computed explicitly, we pause to give three examples.

Example 4.3. Consider the quaternion algebra $B = \left(\dfrac{-1, -23}{\mathbb{Q}}\right)$, so that B is generated by i, j subject to $i^2 = -1$, $j^2 = -23$ and $ji = -ij$. We have the maximal order $\mathcal{O} = \mathcal{O}_0(1) = \mathbb{Z} \oplus \mathbb{Z}i \oplus \mathbb{Z}k \oplus \mathbb{Z}ik$ where $k = (j+1)/2$. We consider the prime $p = 2$; we have an embedding $\mathcal{O} \hookrightarrow \mathrm{M}_2(\mathbb{Z}_2)$ where $i, k \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ (mod 2).

We begin by computing the ideal classes in $\mathcal{O}$. We start with $C_1 = [\mathcal{O}]$. We have 3 ideals of norm 2, namely $I_{(0:1)} = 2\mathcal{O} + ik\mathcal{O}$, $I_{(1:1)} = 2\mathcal{O} + (i+1)k\mathcal{O}$, and $I_{(1:0)} = 2\mathcal{O} + k\mathcal{O}$. If one of these ideals is principal, then it is generated by an element of reduced norm 2. The reduced norm gives a quadratic form

$$\mathrm{nrd} : \mathcal{O} \to \mathbb{Z}$$
$$x + yi + zk + wik \mapsto x^2 + xz + y^2 + yw + 6z^2 + 6w^2$$

We see immediately that $\mathrm{nrd}(x + yi + zk + wik) = 2$ if and only if $z = w = 0$ and $x = y = \pm 1$. This shows that $I_{(1:1)} = (i+1)\mathcal{O}$ is principal but $I_{(1:0)}$ and $I_{(0:1)}$ are not. Note also that we find $2e_1 = 4$ solutions matching (4.2). We notice, however, that $iI_{(1:0)} = I_{(0:1)}$, so we have just a second ideal class $C_2 = [I_{(0:1)}]$.

Now of the two ideals contained in $I_{(0:1)}$ of norm 4, we have $I_{(0:1)}^{(4)} = 4\mathcal{O} + i(k+2)\mathcal{O}$ belongs to C_1 whereas $I_{(2:1)}^{(4)} = 4\mathcal{O} + (2i + 2k + ik)\mathcal{O}$ gives rise to a new ideal class $C_2 = [I_{(2:1)}]$. If

we continue, each of the two ideals contained in $I_{(0:1)}^{(4)}$ of norm 8 belong to C_1, and it follows that $H = \# \operatorname{Cl} \mathcal{O} = 3$.

From this computation, we have also computed the Brandt matrix $T(2) = \begin{pmatrix} 1 & 1 & 0 \\ 2 & 1 & 3 \\ 0 & 1 & 0 \end{pmatrix}$. Indeed, the first column encodes the fact that of the three right $\mathcal{O}$-ideals of reduced norm 2, there is one which is principal and hence belongs to C_1 and two that belong to C_2. We think of this matrix as acting on the right on row vectors.

The characteristic polynomial of $T(2)$ factors as $(x-3)(x^2+x-1)$. The vector $(1,1,1)$ is an eigenvector with eigenvalue 3 which generates the space of constant functions and gives rise to the Eisenstein series having eigenvalues $a_p = p+1$ for all primes $p \neq 23$. The space of cusp forms $S_2^B(1)$ is correspondingly of dimension 2 and is irreducible as a Hecke module. The Hecke module $S_2^B(1)$ can be explicitly identified with $S_2(23)$ using theta correspondence. For example, the series

$$\theta_1(q) = \sum_{\gamma \in \mathcal{O}} q^{\operatorname{nrd}(\gamma)} = \sum_{x,y,z,w \in \mathbb{Z}} q^{x^2+xz+y^2+yw+6z^2+6w^2} = 1 + 4q^2 + 4q^4 + 4q^8 + 8q^{10} + \dots$$

is the q-expansion of a modular form of level 23 and weight 2 and corresponds to (the characteristic of) C_1. For more details, we refer to Pizer [50, Theorem 2.29], where the first computer algorithm for computing Brandt matrices over $\mathbb{Q}$ is also described.

Now we give an example over a quadratic field.

Example 4.4. Let $F = \mathbb{Q}(\sqrt{5})$. Then $\mathbb{Z}_F = \mathbb{Z}[w]$ where $w = (1+\sqrt{5})/2$ satisfying $w^2 - w - 1 = 0$. The prime 61 splits in F; let $\mathfrak{N} = (3w+7)\mathbb{Z}_F$ be one of the primes above it. We consider the (Hamilton) quaternion algebra $B = \left(\dfrac{-1,-1}{F} \right)$ over F of discriminant $\mathfrak{D} = (1)$. We have the maximal order

$$\mathcal{O}_0(1) = \mathbb{Z}_F \oplus i\mathbb{Z}_F \oplus k\mathbb{Z}_F \oplus ik\mathbb{Z}_F, \quad \text{where} \quad k = \frac{(1+w) + wi + j}{2},$$

and the Eichler order $\mathcal{O} \subseteq \mathcal{O}_0(1)$ of level $\mathfrak{N}$ given by

$$\mathcal{O} = \mathbb{Z}_F \oplus (3w+7)i\mathbb{Z}_F \oplus (-30i + k)\mathbb{Z}_F \oplus (w + 20i + ik)\mathbb{Z}_F.$$

The class number of $\mathcal{O}$ is $H = 3$. The following ideals give a set of representatives for $\operatorname{Cl} \mathcal{O}$: we take $I_1 = \mathcal{O}$,

$$I_2 = 2\mathcal{O} + ((w+2) - (2w+2)i + (-1+3w)ik)\mathcal{O}$$
$$= 2\mathbb{Z}_F \oplus (6w+14)i\mathbb{Z}_F \oplus ((w+1) + (-2w+5)i - k)\mathbb{Z}_F \oplus (1 - 6i + wik)\mathbb{Z}_F$$

and $I_3 = 2\mathcal{O} + ((w+1) + (1-w)i + (2-2w)k)\mathcal{O}$.

We compute the orders $e_i = \#(\mathcal{O}_i/\mathbb{Z}_F^\times)$ as $e_1 = 2$, $e_2 = 5$ and $e_3 = 3$. For example, the element $u = (2w)i - k - wik \in \mathcal{O}$ satisfies the equation $u^2 + 1 = 0$, and so yields an element of order 2 in $\mathcal{O}^\times/\mathbb{Z}_F^\times$. It follows that none of these orders are isomorphic (i.e., conjugate) in B.

The first few Brandt matrices are:

$$T(2) = \begin{pmatrix} 1 & 5 & 3 \\ 2 & 0 & 0 \\ 2 & 0 & 2 \end{pmatrix}, \quad T(\sqrt{5}) = \begin{pmatrix} 4 & 0 & 3 \\ 0 & 1 & 3 \\ 2 & 5 & 0 \end{pmatrix}, \quad T(3) = \begin{pmatrix} 4 & 5 & 6 \\ 2 & 0 & 3 \\ 4 & 5 & 1 \end{pmatrix},$$

$$T(w+3) = \begin{pmatrix} 4 & 10 & 6 \\ 4 & 2 & 0 \\ 4 & 0 & 6 \end{pmatrix}, \quad T(w-4) = \begin{pmatrix} 6 & 5 & 6 \\ 2 & 2 & 3 \\ 4 & 5 & 3 \end{pmatrix}.$$

We note that $N(w+3) = N(w-4) = 11$.

For example, the first column of the matrix $T(2)$ records the fact that of the $5 = N(2) + 1$ right $\mathcal{O}$-ideals of norm (2), there is exactly one which is principal, two are isomorphic to I_2 and the other two are isomorphic to I_3.
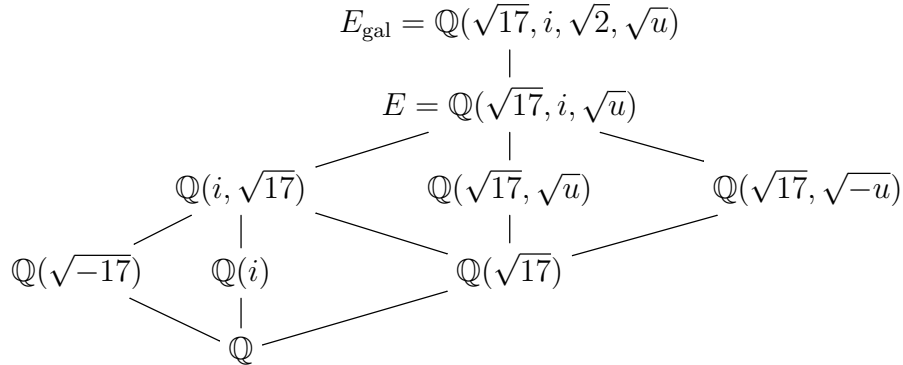
The space $S_2^B(\mathfrak{N})$ of cusp forms is an irreducible 2-dimensional Hecke module, represented by a constituent form f with corresponding eigenvector $(2, 5w, -3w - 3)$. In particular, the ring of Hecke operators $\mathbb{T}_f = \mathbb{Z}[a_\mathfrak{p}]$ restricted to f is equal to $\mathbb{T}_f = \mathbb{Z}[w]$, by coincidence. We have the following table of eigenvalues for f.

$\mathfrak{p}$	(2)	$(w+2)$	(3)	$(w+3)$	$(w-4)$
$N\mathfrak{p}$	4	5	9	11	11
$a_\mathfrak{p}(f)$	$2w - 2$	$-3w + 1$	$-w - 2$	$4w - 2$	$-w$

For further discussion of the geometric objects which arise from this computation, see the discussion in Section 6.

Finally, one interesting example.

Example 4.5. Let $F = \mathbb{Q}(\sqrt{15})$ and let $\mathfrak{N} = (5, \sqrt{15})$. Then there exists a cusp form constituent of an irreducible space of dimension 8 in $S_2(\mathfrak{N})$ such that no single Hecke eigenvalue generates the entire field E of Hecke eigenvalues.

$$E_{\text{gal}} = \mathbb{Q}(\sqrt{17}, i, \sqrt{2}, \sqrt{u})$$
$$|$$
$$E = \mathbb{Q}(\sqrt{17}, i, \sqrt{u})$$

$$\mathbb{Q}(i, \sqrt{17}) \qquad \mathbb{Q}(\sqrt{17}, \sqrt{u}) \qquad \mathbb{Q}(\sqrt{17}, \sqrt{-u})$$

$$\mathbb{Q}(\sqrt{-17}) \qquad \mathbb{Q}(i) \qquad \mathbb{Q}(\sqrt{17})$$

$$\mathbb{Q}$$

Here, $u = (5 + \sqrt{17})/2$ and E_{gal} is the Galois closure of E. Each Hecke eigenvalue $a_\mathfrak{p}$ for this form f generates a proper subfields of E. (There are also examples of this phenomenon over $\mathbb{Q}$, and they are related to the phenomenon of inner twists; this was analyzed over $\mathbb{Q}$ by Koo, Stein, and Wiese [44].)

With these examples in hand, we now give an overview of how these computations are performed; for more detail, see work of the first author [15]. It is clear we need several algorithms to compute Brandt matrices. First, we need a basic suite of algorithms for

working with quaternion orders and ideals; these are discussed in work of Kirschmer and the second author [41, Section 1], and build on basic tools for number rings by Cohen [7]. As part of this suite, we need a method to compute a maximal order, which is covered by work of the second author [72]. Next, we need to compute a set of representatives for $\operatorname{Cl}\mathcal{O}$ and to test if two right $\mathcal{O}$-ideals are isomorphic: this is covered by Kirschmer and the second author [41, Sections 6–7], including a runtime analysis. To compute a set of representatives, we use direct enumeration in the tree as in Example 4.3 and a mass formula due to Eichler as an additional termination criterion. To test for isomorphism, we use lattice methods to find short vectors with respect to the quadratic form $\operatorname{Tr}\operatorname{nrd}$.

In this method, to compute with level $\mathfrak{N}$ one must compute a set of representatives $\operatorname{Cl}\mathcal{O} = \operatorname{Cl}\mathcal{O}_0(\mathfrak{N})$ anew. The first author has given an improvement on this basic algorithm, allowing us to work always with ideal classes $\operatorname{Cl}\mathcal{O}_0(1)$ belonging to the maximal order at the small price of a more complicated description of the Hecke module. The proof of correctness for this method is best explained in the adelic language, so we refer to Section 8 for more detail.

Let $I_1, \ldots, I_h$ be representatives for $\operatorname{Cl}\mathcal{O}_0(1)$ and suppose that $\mathfrak{N}$ is relatively prime to $\operatorname{nrd}(I_i)$ for each i—this is made possible by strong approximation. As before, let $\mathfrak{p}$ be a prime of $\mathbb{Z}_F$ with $\mathfrak{p} \nmid \mathfrak{D}$. Let p be a totally positive generator for $\mathfrak{p}$, and let q_i be a totally positive generator for $\operatorname{nrd}(I_i)$. By our notation, we have $\mathcal{O}_L(I_i) = \mathcal{O}_0(1)_i$. Let $\Gamma_i = \mathcal{O}_0(1)_i^\times / \mathbb{Z}_F^\times$. For each i, j, consider the set

$$\Theta(\mathfrak{p})_{i,j} = \Gamma_j \backslash \left\{ x \in I_j I_i^{-1} : \operatorname{nrd}(x) \frac{q_i}{q_j} = p \right\}$$

where Γ_j acts by the identification $\mathcal{O}_0(1)_i^\times / \mathbb{Z}_F^\times = \mathcal{O}_0(1)_1^\times / \{\pm 1\}$. Via a splitting isomorphism

$$\iota_\mathfrak{N} : \mathcal{O}_0(1) \hookrightarrow \mathcal{O}_0(1) \otimes \mathbb{Z}_{F,\mathfrak{N}} \cong \operatorname{M}_2(\mathbb{Z}_{F,\mathfrak{N}}),$$

the group $\mathcal{O}_0(1)^\times$ acts on $\mathbb{P}^1(\mathbb{Z}_F/\mathfrak{N})$ and since $\mathcal{O}_0(1) \otimes \mathbb{Z}_{F,\mathfrak{N}} \cong \mathcal{O}_0(1)_i \otimes \mathbb{Z}_{F,\mathfrak{N}}$ for each i (since $\operatorname{nrd}(I_i)$ is prime to $\mathfrak{N}$), the group $\Gamma_i = \mathcal{O}_0(1)_i^\times / \mathbb{Z}_F^\times$ similarly acts on $\mathbb{P}^1(\mathbb{Z}_F/\mathfrak{N})$.

We then define a Hecke module structure on $\bigoplus_{i=1}^h \mathbb{C}[\Gamma_i \backslash \mathbb{P}^1(\mathbb{Z}_F/\mathfrak{N})]$ via the map

$$\mathbb{C}[\Gamma_j \backslash \mathbb{P}^1(\mathbb{Z}_F/\mathfrak{N})] \to \mathbb{C}[\Gamma_i \backslash \mathbb{P}^1(\mathbb{Z}_F/\mathfrak{N})]$$

$$\Gamma_j x \mapsto \sum_{\gamma \in \Theta(\mathfrak{p})_{i,j}} \Gamma_i(\gamma x)$$

on each component. It is a nontrivial but nevertheless routine calculation that this Hecke module is isomorphic to the Hecke module $M_2^B(\mathfrak{N})$ defined by the Brandt matrices at the beginning of this section.

Example 4.6. We keep the notations of Example 4.4. The quaternion algebra B has class number 1, thus the maximal order $\mathcal{O}_0(1)$ is unique up to conjugation. We have $\Gamma = \mathcal{O}_0(1)^\times / \mathbb{Z}_F^\times$ has cardinality 60. We consider the splitting map

$$\bar{\iota}_\mathfrak{N} : \mathcal{O}_0(1) \to \mathcal{O}_0(1) \otimes_{\mathbb{Z}_F} (\mathbb{Z}_F/\mathfrak{N}) \cong \operatorname{M}_2(\mathbb{Z}_F/\mathfrak{N})$$

given by

$$\bar{\iota}_\mathfrak{N}(i) = \begin{pmatrix} 11 & 0 \\ 37 & 50 \end{pmatrix}, \ \bar{\iota}_\mathfrak{N}(k) = \begin{pmatrix} 47 & 58 \\ 18 & 33 \end{pmatrix}, \ \bar{\iota}_\mathfrak{N}(ik) = \begin{pmatrix} 29 & 28 \\ 16 & 14 \end{pmatrix}.$$

(One directly verifies that $\bar{\iota}_{\mathfrak{N}}(ik) = \bar{\iota}_{\mathfrak{N}}(i)\bar{\iota}_{\mathfrak{N}}(k)$.) We let Γ act on $\mathbb{P}^1(\mathbb{Z}_F/\mathfrak{N})$ on the left via $\bar{\iota}_{\mathfrak{N}}$. By the above discussion, we have

$$M_2^B(\mathfrak{N}) \cong \mathbb{C}[\Gamma \backslash \mathbb{P}^1(\mathbb{Z}_F/\mathfrak{N})].$$

The action of Γ on $\mathbb{P}^1(\mathbb{Z}_F/\mathfrak{N})$ has three orbits which are represented by $x_1 = (1 : 0)$, $x_2 = (1 : 1)$ and $x_3 = (23 : 1)$ whose stabilizers have cardinality $e_1 = 2$, $e_2 = 5$ and $e_3 = 3$. Thus $M_2^B(\mathfrak{N})$ is a free module generated by the orbits Γx_1, Γx_2 and Γx_3. Writing down the Hecke action in that basis, we obtain the same Hecke operators as in Example 4.4.

Remark 4.7. The approach presented above has some advantages over the usual definition of Brandt matrices above. First of all, it is better suited for working with more general level structures, such as those that do not come from Eichler orders. For example, adding a character in this context is quite transparent. Secondly, when working over the same number field, a substantial amount of the required data can be precomputed and reused as the level varies, and consequently one gains significantly in the efficiency of the computation.

5. Indefinite method

In this section, we discuss a method for computing Hilbert modular forms using a indefinite quaternion algebra B with $r = 1$. We accordingly call our method the *indefinite method*. The method is due to Greenberg and the second author [30]. We seek to generalize the method of modular symbols by working with (co)homology. We continue to suppose that F has strict class number 1, and we assume that $B \not\cong \mathrm{M}_2(\mathbb{Q})$ for uniformity of presentation.

Recall that in this case we have defined a group $\Gamma = \Gamma_0^B(\mathfrak{N}) \subseteq \mathrm{GL}_2^+(\mathbb{R})$ such that $P\Gamma = \Gamma/\mathbb{Z}_F^\times \subseteq \mathrm{PGL}_2^+(\mathbb{R})$ is discrete; the quotient $X = X_0^B(\mathfrak{N}) = \Gamma \backslash \mathcal{H}$ is a Shimura curve and quaternionic cusp forms on B correspond to holomorphic differential 1-forms on X. Integration gives a Hecke-equivariant isomorphism which is the analogue of the Eichler-Shimura theorem, namely

$$S_2^B(\mathfrak{N}) \oplus \overline{S_2^B(\mathfrak{N})} \xrightarrow{\sim} H^1(X_0^B(\mathfrak{N}), \mathbb{C}).$$

We recover $S_2^B(\mathfrak{N})$ by taking the +-eigenspace for complex conjugation on both sides. Putting this together with the Jacquet-Langlands correspondence, we have

$$S_2(\mathfrak{D}\mathfrak{N})^{\mathfrak{D}-\mathrm{new}} \cong S_2^B(\mathfrak{N}) \cong H^1(X_0^B(\mathfrak{N}), \mathbb{C})^+.$$

We have the identifications

$$H^1(X, \mathbb{C}) = H^1(X_0^B(\mathfrak{N}), \mathbb{C}) \cong H^1(\Gamma_0^B(\mathfrak{N}), \mathbb{C}) = \mathrm{Hom}(\Gamma_0^B(\mathfrak{N}), \mathbb{C}) = \mathrm{Hom}(\Gamma, \mathbb{C}).$$

To complete this description, we must relate the action of the Hecke operators. Let $\mathfrak{p} \nmid \mathfrak{D}\mathfrak{N}$ be prime and let p be a totally positive generator of $\mathfrak{p}$. As in (3.5), let

(5.1) $$\Theta(\mathfrak{p}) = \mathcal{O}_+^\times \backslash \{\pi \in \mathcal{O}_+ : \mathrm{nrd}(\pi) = p\}$$

and choose representatives π_a for these orbits labeled by $a \in \mathbb{P}^1(\mathbb{F}_\mathfrak{p})$. Then any $\gamma \in \Gamma$ by right multiplication permutes the elements of $\Theta(\mathfrak{p})$, and hence there is a unique permutation γ^* of $\mathbb{P}^1(\mathbb{F}_\mathfrak{p})$ such that for all $a \in \mathbb{P}^1(\mathbb{F}_\mathfrak{p})$ we have

$$\pi_a \gamma = \delta_a \pi_{\gamma^* a}$$

with $\delta_a \in \Gamma$. For $f \in H^1(\Gamma, \mathbb{C}) = \mathrm{Hom}(\Gamma, \mathbb{C})$, we then define

(5.2) $$(T_\mathfrak{p} f)(\gamma) = \sum_{\pi_a \in \Theta(\mathfrak{p})} f(\delta_a).$$

In a similar way, we compute the action of complex conjugation T_∞ via the relation

$$(T_\infty f)(\gamma) = f(\delta)$$

where $\mu\gamma = \delta\mu$ and $\mu \in \mathcal{O}^\times \setminus \mathcal{O}_1^\times$.

We begin with two examples, to illustrate the objects and methods involved.

Example 5.3. Let $F = \mathbb{Q}(\sqrt{29})$. Then $\mathbb{Z}_F = \mathbb{Z}[w]$ is the ring of integers of F where $w = (1 + \sqrt{29})/2$ satisfies $w^2 - w - 7 = 0$. Indeed F has strict class number 1 and $u = w + 2$ is a fundamental unit of F.

Let $B = \left(\dfrac{-1, u}{F}\right)$, so B is generated over F by i, j subject to $i^2 = -1$, $j^2 = u$, and $ji = -ij$. The algebra B is ramified at the prime ideal $2\mathbb{Z}_F$ and the nonidentity real place of B (taking $\sqrt{29} \mapsto -\sqrt{29}$) and no other place. The identity real place gives an embedding

$$\iota_\infty : B \hookrightarrow B \otimes_F \mathbb{R} \cong \mathrm{M}_2(\mathbb{R})$$

$$i, j \mapsto \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} \sqrt{u} & 0 \\ 0 & -\sqrt{u} \end{pmatrix} = \begin{pmatrix} 2.27... & 0 \\ 0 & -2.27... \end{pmatrix}$$

Let

$$\mathcal{O} = \mathcal{O}_0(1) = \mathbb{Z}_F \oplus \mathbb{Z}_F i \oplus \mathbb{Z}_F j \oplus \mathbb{Z}_F k$$

where $k = (1+i)(w+1+j)/2$. Then $\mathcal{O}$ is a maximal order of B with discriminant $\mathfrak{D} = 2\mathbb{Z}_F$. Let $\Gamma = \iota_\infty(\mathcal{O}_1^\times) \subseteq \mathrm{SL}_2(\mathbb{R})$ be as above and let $X = X(1)_\mathbb{C} = \Gamma \backslash \mathcal{H}$ be the associated Shimura curve.

Although they are not an intrinsic part of our algorithm, we mention that the area of X (normalized so that an ideal triangle has area $1/2$) is given by

$$A = \frac{4}{(2\pi)^{2n}} d_F^{3/2} \zeta_F(2) \Phi(\mathfrak{D}) = \frac{4}{(2\pi)^4} \sqrt{29}^3 \zeta_F(2)(4 - 1) = \frac{3}{2}$$

where $\Phi(\mathfrak{D}) = \prod_{\mathfrak{p} | \mathfrak{D}}(\mathbb{N}\mathfrak{p} + 1)$, and the genus of X is given by the Riemann-Hurwitz formula as

$$A = 2g - 2 + \sum_q e_q \left(1 - \frac{1}{q}\right)$$

where e_q is the number of elliptic cycles of order $q \in \mathbb{Z}_{\geq 2}$ in Γ. An explicit formula for e_q given in terms of class numbers and Legendre symbols yields $e_2 = 3$ and $e_q = 0$ for $q > 2$. Thus $2g - 2 = 0$, so $g = 1$. For more details on these formulas and further introduction, see work of the second author [70] and the references given there.

Next, we compute a fundamental domain for Γ, yielding a presentation for Γ; we consider this as a black box for now. The domain, displayed in the unit disc, is as follows.
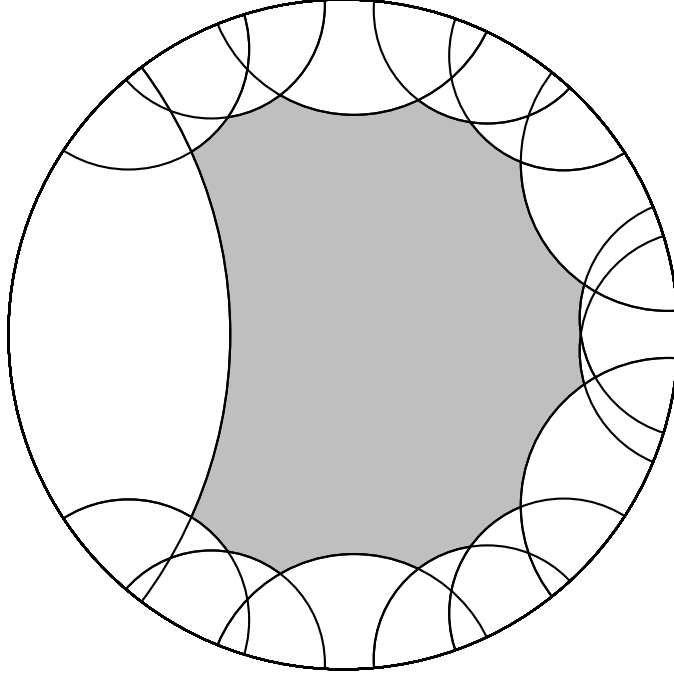
We obtain the presentation

$$\Gamma \cong \langle \gamma, \gamma', \delta_1, \delta_2, \delta_3 : \delta_1^2 = \delta_2^2 = \delta_3^2 = [\gamma, \gamma']\delta_1\delta_2\delta_3 = 1 \rangle$$

where

$$\gamma = -w - 1 + i - 2j + k$$
$$\gamma' = 2 + 2i + (w - 1)j - (w - 1)k$$
$$\delta_1 = (2w + 2) + wi + j + 4k$$
$$\delta_2 = i$$
$$\delta_3 = (w + 1) + (2w + 3)i - j - k.$$

The above method gives the isomorphisms of Hecke modules

$$S_2(2\mathbb{Z}_F)^{\text{new}} \cong S_2^B(1) = \{f : \mathcal{H} \to \mathbb{C} : f(gz)\, d(gz) = f(z)\, dz \text{ for all } g \in \Gamma\} \cong H^1(\Gamma, \mathbb{C})^+.$$

We compute that $H^1(\Gamma, \mathbb{C})^+ \cong \text{Hom}(\Gamma, \mathbb{C})^+ = \mathbb{C}f$ where f is the characteristic function of γ, i.e., $f(\gamma) = 1$, $f(\gamma') = 0$ and $f(\delta_i) = 0$ for $i = 1, 2, 3$.

We compute the Hecke operator $T_{\mathfrak{p}}$ for $\mathfrak{p}$ odd according the definition (5.2). Let $\mathfrak{p} = (w + 1)\mathbb{Z}_F$. Then $N\mathfrak{p} = p = 5$. We compute the action of $T_{\mathfrak{p}}$ on $H^1(\Gamma, \mathbb{C})^+$ given by $T_{\mathfrak{p}}f = a_{\mathfrak{p}}(f)f$. The Hecke operators act as a sum over $p + 1$ left ideals of reduced norm p, indexed by $\mathbb{P}^1(\mathbb{F}_5)$. Let

$$\iota_{\mathfrak{p}} : \mathcal{O} \hookrightarrow \text{M}_2(\mathbb{Z}_{F,\mathfrak{p}}) \cong \text{M}_2(\mathbb{Z}_5)$$

$$i, j, ij \mapsto \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix} \quad (\text{mod } 5).$$

Specifying the images modulo $\mathfrak{p}$ gives them uniquely, as they lift to $\text{M}_2(\mathbb{Z}_5)$ using Hensel's lemma. (Note that $j^2 = u \equiv 1 \pmod{w + 1}$.)

Let $J_\infty, J_0, \ldots, J_4$ be defined by

$$J_a = J_{(x:y)} = \mathcal{O}\iota_\mathfrak{p}^{-1}\begin{pmatrix} x & y \\ 0 & 0 \end{pmatrix} + \mathfrak{p}\mathcal{O}$$

as in (3.6). Then $J_a = \mathcal{O}\pi_a$ are principal left $\mathcal{O}$-ideals by strong approximation. For example, $J_0 = \mathcal{O}(i - ij) + (w + 2)\mathcal{O} = \mathcal{O}\pi_0$ where $\pi_0 = (-w + 3) + wi + j + ij$.

We compute the Hecke operators as in (5.2). For $f : \Gamma \to \mathbb{C}$ and $\gamma \in \Gamma$, we compute elements $\delta_a \in \Gamma$ indexed by $a \in \mathbb{P}^1(\mathbb{F}_\mathfrak{p})$ and γ^* a permutation of $\mathbb{P}^1(\mathbb{F}_\mathfrak{p})$ such that $\pi_a\gamma = \delta_a\pi_{\gamma^*a}$ for all $a \in \mathbb{P}^1(\mathbb{F}_\mathfrak{p})$; then

$$(T_\mathfrak{p}f)(\gamma) = \sum_{a \in \mathbb{P}^1(\mathbb{F}_\mathfrak{p})} f(\delta_a).$$

The contribution to the sum for f simply counts the number of occurrences of γ in the product $\pi_a\gamma\pi_{\gamma^*a} = \delta_a \in \Gamma$. Carrying out this computation for various primes, we obtain the following table.

$N\mathfrak{p}$	5	7	9	13	23	29	53	59	67	71	83
$a_\mathfrak{p}(f)$	1	-2	5	-1	-6	10	-1	10	8	-8	13
$N\mathfrak{p} + 1 - a(\mathfrak{p})$	5	10	5	15	30	20	55	50	60	80	70

Here we list only the norm of the prime as the eigenvalue does not depend on the choice of prime $\mathfrak{p}$ of the given norm. This suggests that f corresponds to a base change of a form from $\mathbb{Q}$.

So we look through tables of elliptic curves over $\mathbb{Q}$ whose conductor is divisible only by 2 and 29. We find the curve E labelled $\mathsf{1682c1}$, where $1682 = 2 \cdot 29^2$, given by

$$E : y^2 + xy = x^3 + x^2 - 51318x - 4555676.$$

Let E_F denote the base change of E to F. We compute that the twist E'_F of E_F by $-u\sqrt{29}$, given by

$$E'_F : y^2 + (w + 1)xy = x^3 + (-w + 1)x^2 + (-11w - 20)x + (23w + 52)$$

has conductor $2\mathbb{Z}_F$. Since the extension $F/\mathbb{Q}$ is abelian, by base change theorems we know that there exists a Hilbert cusp form associated to E'_F over F which is new of level $2\mathbb{Z}_F$, which therefore must be equal to f. This verifies that the Jacobian $J(1)$ of $X(1)$ is isogenous to E'_F. We verify that $\#E'_F(\mathbb{F}_\mathfrak{p}) = N\mathfrak{p} + 1 - a(\mathfrak{p})$ and (as suggested by the table) that E has a 5-torsion point, $(-1, -2w - 5)$ (and consequently so too does $J(1)$).

Example 5.4. To illustrate the Jacquet-Langlands correspondence (Theorem 3.9) in action, we return to Example 4.4. Recall $F = \mathbb{Q}(\sqrt{5})$ and $w = (1 + \sqrt{5})/2$. We find the quaternion algebra $B = \left(\dfrac{w, -(3w + 7)}{F}\right)$ which is ramified at $\mathfrak{N} = (3w + 7)\mathbb{Z}_F$, a prime of norm 61, and one infinite place. The order $\mathcal{O} = \mathcal{O}_0(1)$ with $\mathbb{Z}_F$-basis $1, i, k, ik$, where $k = ((w + 1) + wi + j)/2$, is maximal. As above, we compute that $A(X) = 10$ and $g(X) = 2 = \dim S_2^B(1) = \dim S_2(\mathfrak{N})^{\text{new}}$. Now we have the following fundamental domain:
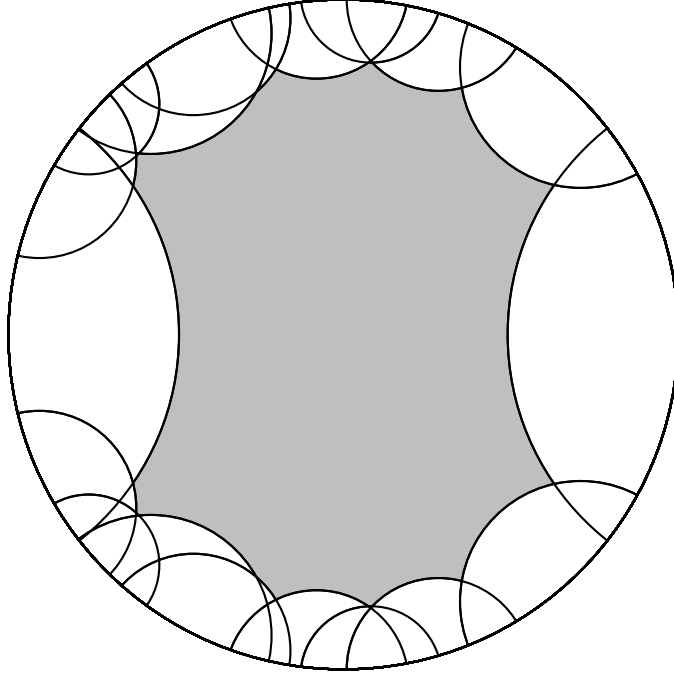
We obtain the presentation

$$\Gamma(1) \cong \langle \gamma_1, \gamma_1', \gamma_2, \gamma_2' : [\gamma_1, \gamma_1'][\gamma_2, \gamma_2'] = 1 \rangle.$$

(In particular, $\Gamma(1)$ is a torsion-free group.) We have $\dim H^1(X, \mathbb{C}) = 4$, and on the basis of characteristic functions given by $\gamma_1, \gamma_1', \gamma_2, \gamma_2'$, the action of complex conjugation is given by the matrix $\begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 1 & 0 & -1 \\ 0 & -1 & -1 & 0 \end{pmatrix}$: this is computed in a way We thus obtain a basis for $H = H^1(X, \mathbb{C})^+ \cong S_2^B(1)$. Computing Hecke operators as in the previous example, we find as in Example 4.4 that $S_2^B(1)$ is irreducible as a Hecke module, and find that

$$H \mid T_2 = \begin{pmatrix} 2 & 2 \\ -2 & -4 \end{pmatrix}, \quad H \mid T_{\sqrt{5}} = \begin{pmatrix} -5 & -3 \\ 3 & 4 \end{pmatrix}, \quad H \mid T_3 = \begin{pmatrix} -4 & -1 \\ 1 & -1 \end{pmatrix},$$

$$H \mid T_{w+3} = \begin{pmatrix} 6 & 4 \\ -4 & -6 \end{pmatrix}, \quad H \mid T_{w-4} = \begin{pmatrix} -2 & -1 \\ 1 & 1 \end{pmatrix}.$$

Happily, the characteristic polynomials of these operators agree with those computed using the definite method.

We now give an overview of how these computations are performed: for more details, see the reference by Greenberg and the second author [30]. To compute effectively the systems of Hecke eigenvalues in the cohomology of a Shimura curve, we need several algorithms. First, we need to compute an explicit finite presentation of Γ with a solution to the word problem in Γ, i.e., given $\delta \in \Gamma$, write δ as an explicit word in the generators for Γ. Secondly, we need to compute a generator (with totally positive reduced norm) of a left ideal $I \subseteq \mathcal{O}$. The first of these problems is solved by computing a Dirichlet domain; the second is solved using lattice methods. We discuss each of these in turn.

Let $p \in \mathcal{H}$ have trivial stabilizer $\Gamma_p = \{g \in \Gamma : gp = p\} = \{1\}$. The *Dirichlet domain* centered at p is the set

$$D(p) = \{z \in \mathcal{H} : d(z, p) \leq d(gz, p) \text{ for all } g \in \Gamma\}$$

where d denotes the hyperbolic distance. In other words, we pick in every Γ-orbit the closest points z to p. The set $D(p)$ is a closed, connected, hyperbolically convex fundamental domain for Γ whose boundary consists of finitely many geodesic segments, called *sides*, and comes equipped with a *side pairing*, a partition of the set of sides into pairs s, s^* with $s^* = g(s)$ for some $g \in \Gamma$. (We must respect a convention when a side s is fixed by an element of order 2, considering s to be the union of two sides meeting at the fixed point of g.)

The second author has proven [69] that there exists an algorithm which computes a Dirichlet domain D for Γ, a side pairing for D, and a finite presentation for Γ with a minimal set of generators together with a solution to the word problem for Γ. This algorithm computes D inside the unit disc $\mathcal{D}$, and we consider now Γ acting on $\mathcal{D}$ by a conformal transformation which maps $p \to 0$. We find then that $\mathcal{D}$ can be computed as an *exterior domain*, namely, the intersection of the exteriors of *isometric circles* $I(g)$ for elements $g \in \Gamma$, where $I(g) = \{z \in \mathbb{C} : |cz + d| = 1\}$ where $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SU(1,1)$. We find generators for the group by enumerating short vectors with respect to a certain positive definite quadratic form depending on p.

The solution to the word problem comes from a reduction algorithm that finds elements which contribute to the fundamental domain and removes redundant elements. Given a finite subset $G \subset \Gamma \setminus \{1\}$ we say that γ is *G-reduced* if for all $g \in G$, we have $d(\gamma 0, 0) \leq d(g\gamma 0, 0)$. We have a straightforward algorithm to obtain a G-reduced element, which we denote $\gamma \mapsto \mathrm{red}_G(\gamma)$: if $d(\gamma 0, 0) > d(g\gamma 0, 0)$ for some $g \in G$, set $\gamma := g\gamma$ and repeat. When the exterior domain of G is a fundamental domain, we have $\mathrm{red}_G(\gamma) = 1$ if and only if $\gamma \in \Gamma$. This reduction is analogous to the generalized division algorithm in a polynomial ring over a field.

Example 5.5. Let F be the (totally real) cubic subfield of $\mathbb{Q}(\zeta_{13})$ with discriminant $d_F = 169$. We have $F = \mathbb{Q}(b)$ where $b^3 + 4b^2 + b - 1 = 0$. (F has strict class number 1.)

The quaternion algebra $B = \left(\dfrac{-1, b}{F}\right)$ has discriminant $\mathfrak{D} = (1)$ and is ramified at 2 of the 3 real places of F. We take $\mathcal{O}$ to be an Eichler order of level $\mathfrak{p} = (b + 2)$, a prime ideal of norm 5; explicitly, we have

$$\mathcal{O} = \mathbb{Z}_F \oplus (b+2)i\mathbb{Z}_F \oplus \frac{b^2 + (b+4)i + j}{2}\mathbb{Z}_F \oplus \frac{b + (b^2+4)\alpha + \alpha\beta}{2}\mathbb{Z}_F.$$

We compute a fundamental domain for the group $\Gamma = \Gamma_0^{(1)}(\mathfrak{p}) = \iota_\infty(\mathcal{O}_1^*)/\{\pm 1\}$. We take $p = 9/10i \in \mathcal{H}$.

We first enumerate elements of $\mathcal{O}$ by their absolute reduced norm. Of the first 260 elements, we find 29 elements of reduced norm 1.
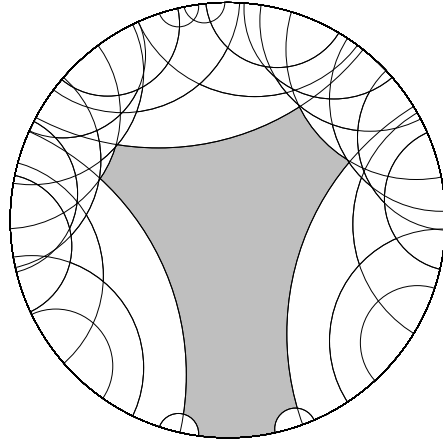
Let G be the set of elements which contribute to the boundary. For each $g \notin G$, we compute $\text{red}_G(g)$. Each in fact reduces to 1, so we are left with 8 elements.
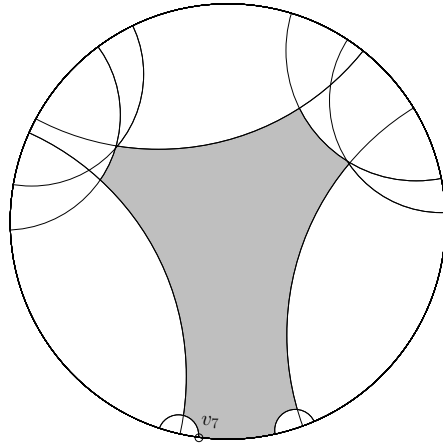
We next enumerate elements in $\mathcal{O}$ moving the center in the direction of the infinite vertex v_7. We find an *enveloper*, an element g such that v_7 lies in the interior of $I(g)$, and reduce to obtain the following.
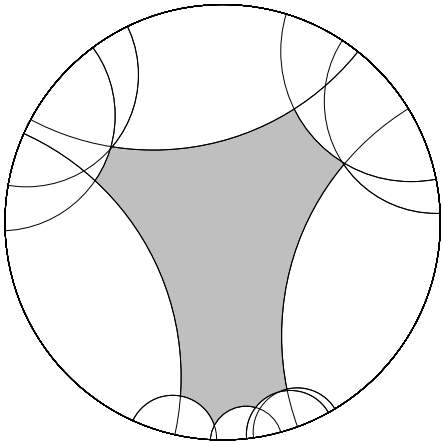
The domain now has finite area. We now attempt to pair each vertex to construct a side pairing.
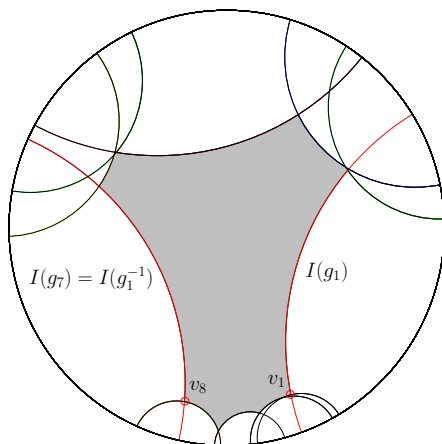

For example, the first vertex v_1 pairs with v_8, pairing the isometric circle $I(g_1)$ of g_1 with $I(g_7)$. We continue, but find that v_9 does not pair with another vertex.
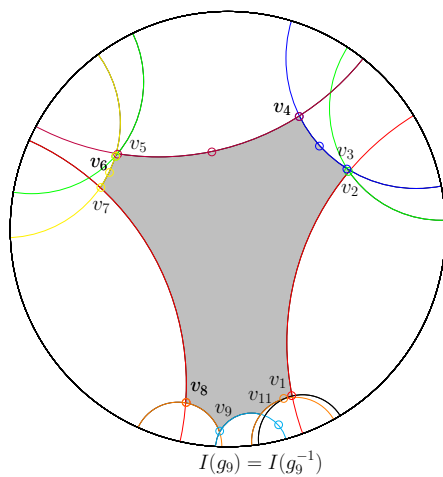
Indeed, $g_9(v_9)$ does not lie in the exterior domain. We compute the reduction $\mathrm{red}_G(g_9; v_9)$, analogously defined. We then obtain a domain with the right area, so we are done!

(In order to get an honest side pairing, we agree to the convention that a side $I(g)$ which is fixed by an element g, necessarily of order 2, is in fact the union of two sides which meet at the unique fixed point of g; the corresponding vertex then appears along such an side.)
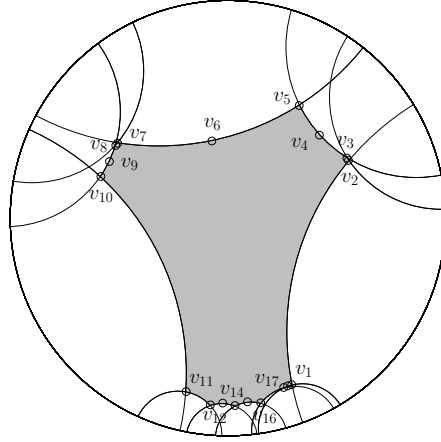
As to the second problem, that of principalizing ideals, we refer to work of Kirschmer and the second author [41, §4], which relies again upon enumeration in a lattice. This method can be improved using the computation of a fundamental domain, which allows one to further effectively reduce lattice elements.

As in the previous section, when the level $\mathfrak{N}$ varies, by changing the coefficient module one can work always with the group $\Gamma(1)$ associated to the maximal order $\mathcal{O}_0(1)$ rather than recomputing a fundamental domain for $\Gamma = \Gamma_0(\mathfrak{N})$ each time. This is a simple application of Shapiro's lemma: the isomorphism

$$H^1(\Gamma, \mathbb{C}) \cong H^1(\Gamma(1), \mathrm{Coind}_\Gamma^{\Gamma(1)} \mathbb{C}),$$

is an isomorphism of Hecke modules: we give $\mathrm{Coind}_\Gamma^{\Gamma(1)} \mathbb{C} = \mathrm{Hom}(\Gamma(1)/\Gamma, \mathbb{C})$ the natural structure as a $\Gamma(1)$-module, and for a cochain $f \in H^1(\Gamma, \mathrm{Coind}_\Gamma^{\Gamma(1)} \mathbb{C})$, we define

(5.6) $$(T_\mathfrak{p} f)(\gamma) = \sum_{\pi_a \in \Theta(\mathfrak{p})} f(\delta_a)$$

as in (5.2). We require still that $\Theta(\mathfrak{p}) \subset \mathcal{O}_+$; after enumerating a set of representatives for $\Gamma \backslash \Gamma(1)$, we can simply multiply elements $\pi_a \in \mathcal{O}_0(1)$ by the representative for its coset.

To conclude, we compare the above method to the method of modular symbols introduced when $F = \mathbb{Q}$. The Shimura curves $X = X_0^B(\mathfrak{N})$ do not have cusps, and so the method of modular symbols does not generalize directly. However, the side pairing of a Dirichlet domain for Γ gives an explicit characterization of the gluing relations which describe X as a Riemann surface, hence one obtains a complete description for the homology group $H_1(X, \mathbb{Z})$. Paths are now written $\{v, \gamma v\}$ for v a vertex on a side paired by $\gamma \in G$. The analogue of the Manin trick in the context of Shimura curves is played by the solution to the word problem in Γ, and so in some sense this can be seen as a partial extension of the Euclidean algorithm to totally real fields. Our point of view is to work dually with cohomology, but computationally these are equivalent [30, §6].

25

6. EXAMPLES

In this section, we provide some detailed examples to illustrate applications of the algorithms introduced in the previous sections.

Our first motivation comes from the association between Hilbert modular forms and abelian varieties. The Eichler-Shimura construction (see Knapp [38, Chap. XII] or Shimura [61, Chapter 7]) attaches to a classical newform $f(z) = \sum_n a_n q^n \in S_2(N)^{\text{new}}$ an abelian variety A_f with several properties. First, A_f has dimension equal to $[E_f : \mathbb{Q}]$ where $E_f = \mathbb{Q}(\{a_n\})$ is the field of Fourier coefficients of f and $\text{End}_{\mathbb{Q}}(A_f) \otimes \mathbb{Q} \cong E_f$. Second, A_f has good reduction for all primes $p \nmid N$. Last, we have an equality of L-functions

$$L(A_f, s) = \prod_{\sigma \in \text{Hom}(E_f, \mathbb{C})} L(f^\sigma, s)$$

where f^σ is obtained by letting σ act on the Fourier coefficients of f, so that

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

The abelian variety A_f arises as the quotient of $J_0(N)$ by the ideal of $\text{End}\, J_0(N)$ generated by $T_n - a_n$.

The simplest example of this construction is the case of a newform f with rational Fourier coefficients $\mathbb{Q}(\{a_n\}) = \mathbb{Q}$. Then A_f is an elliptic curve of conductor N obtained analytically via the map

$$X_0(N) \to A_f$$

$$\tau \mapsto z_\tau = 2\pi i \int_{i\infty}^\tau f(z)\, dz = \sum_{n=1}^\infty \frac{a_n}{n} e^{2\pi i \tau}.$$

The equality of L-functions is equivalent to the statement $\#A_f(\mathbb{F}_p) = p+1-a_p$ for all primes p, and this follows in the work of Eichler and Shimura by a comparison of correspondences in characteristic p with the Frobenius morphism.

The Eichler-Shimura construction extends to the setting of totally real fields in the form of the following conjecture (see e.g. Darmon [11, Section 7.4]).

Conjecture 6.1 (Eichler-Shimura). *Let $f \in S_2(\mathfrak{N})^{\text{new}}$ be a Hilbert newform of parallel weight 2 and level $\mathfrak{N}$ over F. Let $E_f = \mathbb{Q}(\{a_{\mathfrak{n}}\})$ be the field of Fourier coefficients of f. Then there exists an abelian variety A_f of dimension $g = [E_f : \mathbb{Q}]$ defined over F of conductor $\mathfrak{N}^g$ such that $\text{End}_F(A_f) \otimes \mathbb{Q} \cong E_f$ and*

$$L(A_f, s) = \prod_{\sigma \in \text{Hom}(E_f, \mathbb{C})} L(f^\sigma, s).$$

In particular, if f has rational Fourier coefficients, Conjecture 6.1 predicts that one can associate to f an elliptic curve A_f defined over F with conductor $\mathfrak{N}$ such that $L(A_f, s) = L(f, s)$.

Conjecture 6.1 is known to be true in many cases. It is known if f appears in the cohomology of a Shimura curve (as in Sections 3 and 5 above; see also Zhang [76]): this holds whenever $n = [F : \mathbb{Q}]$ is odd or if $\mathfrak{N}$ is exactly divisible by a prime $\mathfrak{p}$. If f appears in the

cohomology of a Shimura curve X and f has rational Fourier coefficients, then when the conjecture holds there is a morphism $X \to A_f$ and we say that A_f is *uniformized* by X.

However, Conjecture 6.1 is not known in complete generality: by the Jacquet-Langlands correspondence, one has left exactly those forms f over a field F of even degree n and *squarefull* level (i.e. if $\mathfrak{p} \mid \mathfrak{N}$ then $\mathfrak{p}^2 \mid \mathfrak{N}$), for example $\mathfrak{N} = (1)$. One expects still that the conjecture is true in this case: Blasius [1], for example, shows that the conjecture is true under the hypothesis of the Hodge conjecture.

The converse to the Eichler-Shimura construction (Conjecture 6.1) over $\mathbb{Q}$ is known as the Shimura-Taniyama conjecture. An abelian variety A over a number field F is *of* GL_2*-type* if $\mathrm{End}_F A \otimes \mathbb{Q}$ is a number field of degree $\dim A$. The Shimura-Taniyama conjecture states that given an abelian variety A of GL_2-type over $\mathbb{Q}$, there exists an integer $N \geq 1$ and a surjective morphism $J_0(N) \to A$. This conjecture is a theorem, a consequence of the proof of Serre's conjecture by Khare and Wintenberger [39]. In the setting of totally real fields, the analogous conjecture is as follows.

Conjecture 6.2 (Shimura-Taniyama). *Let A be an abelian variety of GL_2-type over a totally real field F. Then there exists a Hilbert newform f of parallel weight 2 such that $E_f \cong \mathrm{End}_F(A) \otimes \mathbb{Q}$ and*

$$L(A, s) = \prod_{\sigma \in \mathrm{Hom}(E_f, \mathbb{C})} L(f^\sigma, s).$$

If both of these conjectures are true, then by the isogeny theorem of Faltings, the abelian variety A in Conjecture 6.2 would be isogenous to the abelian variety A_f constructed in Conjecture 6.1. An abelian variety of GL_2-type over a totally real field F which satisfies the conclusion of Shimura-Taniyama conjecture (Conjecture 6.2) is called *modular*.

There has been tremendous progress in adapting the techniques initiated by Wiles [73]—which led to the proof of the Shimura-Taniyama conjecture in the case $F = \mathbb{Q}$—to totally real fields. For example, there are modularity results which imply that wide classes of abelian varieties of GL_2-type are modular: see for example work of Skinner and Wiles [63, 64], Kisin [42, 43], Snowden [65] and Geraghty [28], and the results below. However, a complete proof of Conjceture 6.2 remains elusive.

With these conjectures in mind, we turn to some computational examples. We begin with $F = \mathbb{Q}(\sqrt{5})$ and let $w = (1 + \sqrt{5})/2$. For some further discussion on this case, see work of the first author [14].

Example 6.3. We consider the spaces $S_2(\mathfrak{N})$ with $N(\mathfrak{N}) \leq 30$.

We compute using the definite method of Section 4 using the quaternion algebra over F which is ramified at no finite place. We find that $\dim S_2(\mathfrak{N}) = 0$ for all ideals $\mathfrak{N}$ of $\mathbb{Z}_F$ with $N(\mathfrak{N}) \leq 30$ and $\dim S_2(\mathfrak{N}) = 1$ for $\mathfrak{N}$ with norm 31.

Now let $\mathfrak{N}$ be either of the primes above 31. By the Jacquet-Langlands correspondence (Theorem 3.9) and the accompanying discussion, the space $S_2(\mathfrak{N})$ can also be computed using the indefinite quaternion algebra B ramified at $\mathfrak{N}$ and one real place. We find agreeably that the Shimura curve $X_0^B(1)$ has genus one and thus its Jacobian is an elliptic curve. By a search, we find the elliptic curve

$$A : y^2 + xy + wy = x^3 - (1 + w)x^2$$

of conductor $\mathfrak{N} = (5 + 2w)$ of norm 31.

We now show that A is modular. In brief, we verify that the Galois representation $\bar{\rho}_{A,3}$: $\mathrm{Gal}(\overline{F}/F) \to \mathrm{GL}_2(\mathbb{F}_3) \subseteq \mathrm{GL}_2(\mathbb{F}_9)$ is irreducible, solvable, and ordinary since $\#A(\mathbb{F}_9) = 8$ (so $3 \nmid a_3(A) = 9 + 1 - 8 = 2$), so A is modular by Skinner and Wiles [63]. Since A has conductor $\mathfrak{N}$ and the space $S_2(\mathfrak{N})$ has dimension 1, it follows by the isogeny theorem of Faltings that A is isogeneous to the Jacobian of the Shimura curve $X_0^B(1)$.

In particular, the elliptic curves over $F = \mathbb{Q}(\sqrt{5})$ with smallest conductor have prime conductor dividing 31 and are isogenous to A or its Galois conjugate.

Example 6.4. Let $\mathfrak{N} \subseteq \mathbb{Z}_F$ be such that $N(\mathfrak{N}) \leq 100$.

If $\mathfrak{N} \nmid 61$, then $\dim S_2(\mathfrak{N})^{\mathrm{new}} \leq 2$: each newform f of conductor $\mathfrak{N}$ has rational Fourier coefficients and is either the base change of a classical modular form over $\mathbb{Q}$ or associated to an elliptic curve which is uniformized by a Shimura curve.

We compute each space in turn using the definite method. Those forms f which have the property that $a_{\mathfrak{p}}(f) = a_{\bar{\mathfrak{p}}}(f)$, where $^{-}$ denotes the Galois involution, are candidates to arise from base change over $\mathbb{Q}$. For each of these forms f, we find a candidate classical modular form g using the tables of Cremona [9]: such a form will have conductor supported at 5 and the primes dividing $N(\mathfrak{N})$. Each curve comes with a Weierstrass equation, and we find a quadratic twist of the base change of this curve to F which has conductor $\mathfrak{N}$. Since every elliptic curve over $\mathbb{Q}$ is modular, the base change and its quadratic twist are also modular, and since we exhaust the space this way we are done.

For example, when $\mathfrak{N} = (8)$ we have $\dim S_2(8)^{\mathrm{new}} = 1$ and find the form f with Hecke eigenvalues $a_{(w+2)} = -2$, $a_{(3)} = 2$, $a_{(w+3)} = a_{(w+7)} = -4$, $a_{(w-5)} = a_{(w+4)} = 4$, and so on. In the tables of Cremona, we locate the form

$$g(q) = q - 2q^3 - 2q^7 + q^9 - 4q^{11} - 4q^{13} - 4q^{19} + \cdots \in S_2(200)$$

associated to an elliptic curve A_g with label 200b and equation $y^2 = x^3 + x^2 - 3x - 2$. We find that the quadratic twist of (the base change of) A_g by $-(w + 2) = -\sqrt{5}$ given by the equation $y^2 = x^3 + (w - 1)x^2 - wx$ has conductor (8), so we conclude that f is the base change of g. Note that this example is not covered by the known cases of the Eichler-Shimura construction, since the level $(8) = (2)^3$ is squarefull.

Example 6.5. Now consider the prime level $\mathfrak{N} = (3w + 7) \mid 61$, then $S_2(\mathfrak{N})^{\mathrm{new}}$ is a 2-dimensional irreducible Hecke module arising from the Jacobian of the Shimura curve $X_0^B(1)$ where B is the quaternion algebra ramified at one of the infinite places and $\mathfrak{N}$. This follows from Examples 4.4 and 5.4.

One is naturally led to ask, can one identify the genus 2 Shimura curve $X = X_0^B(1)$ with B of discriminant $\mathfrak{N}$?

Consider the hyperelliptic curve $C : y^2 + Q(x)y = P(x)$ over F with

$$P(x) = -wx^4 + (w - 1)x^3 + (5w + 4)x^2 + (6w + 4)x + 2w + 1$$
$$Q(x) = x^3 + (w - 1)x^2 + wx + 1.$$

This curve was obtained via specialization of the Brumer-Hashimoto family [4, 31] of curves (see also Wilson [75]) whose Jacobian has real multiplication by $\mathbb{Q}(\sqrt{5})$, so in particular so does the Jacobian $J = \mathrm{Jac}(C)$ of C. The discriminant of C is $\mathrm{disc}(C) = \mathfrak{N}^2$. One can show that J is modular using the theorem of Skinner and Wiles [64, Theorem A] and the fact that J has a torsion point of order 31. Since C is hyperelliptic of genus 2, we compute that

the conductor of (the abelian surface) J is $\mathfrak{N}^2$ and that its level is $\mathfrak{N}$. Since J is modular of level $\mathfrak{N}$, it corresponds to the unique Hecke constituent of that level. It follows then by the isogeny theorem of Faltings that J and the Jacobian of the Shimura curve X are isogenous.

These examples exhaust all modular abelian varieties of GL_2-type over $\mathbb{Q}(\sqrt{5})$ with level $\mathfrak{N}$ of norm $N(\mathfrak{N}) \leq 100$ (up to isogeny).

We conclude with some (further) cases where Conjectures 6.1 and 6.2 are not known.

Example 6.6. The first case of squarefull level with a form that is not a base change is level $\mathfrak{N} = (w+36) = (w+3)^2$ so $N(\mathfrak{N}) = 121$. We have $\dim S_2(w+36) = 1$ and the corresponding newform f has the following eigenvalues (where $t^2 = 3$):

$\mathfrak{p}$	(2)	$(w+2)$	(3)	$(w+3)$	$(w-4)$	$(w-5)$	$(w+4)$	$(w+5)$	$(w-6)$
$N\mathfrak{p}$	4	5	9	11	11	19	19	29	29
$a_{\mathfrak{p}}(f)$	t	$-t$	-1	0	$-2t$	$4t$	-2	$-5t$	-3

In this case, the Eichler-Shimura conjecture predicts the existence of an abelian surface defined over $F = \mathbb{Q}(\sqrt{5})$ with good reduction away from $\mathfrak{p} = (w+3)$ and with real multiplication by $\mathbb{Q}(\sqrt{3})$. The form f is not a base change from $\mathbb{Q}$ since $a_{\mathfrak{p}}(f) \neq a_{\bar{\mathfrak{p}}}(f)$ in general. Can one find an explicit genus 2 curve over F, analogous to the previous example, with the L-function of its Jacobian given by the above Frobenius data?

Example 6.7. We next consider a situation when we are successful in establishing the correspondence in a case which is not covered by known results. Consider $\mathfrak{N} = (17w-8) = (w+4)^2$ so $N(\mathfrak{N}) = 361$. There exist forms $f, g \in S_2(\mathfrak{N})$ with Hecke eigenvalues as follows:

$\mathfrak{p}$	(2)	$(w+2)$	(3)	$(w+3)$	$(w-4)$	$(w-5)$	$(w+4)$	$(w+5)$	$(w-6)$
$N\mathfrak{p}$	4	5	9	11	11	19	19	29	29
$a_{\mathfrak{p}}(f)$	2	-3	1	3	3	-1	0	3	-6
$a_{\mathfrak{p}}(g)$	-2	-3	-1	-3	-3	-1	0	3	6

The form g is a quadratic twist of f by $w(w+4)$, and the forms f, g are not base changes from $\mathbb{Q}$.

We use the method of Cremona and Lingham [10]—without an attempt to be exhaustive—to find an elliptic curve E over F with good reduction away from $\mathfrak{p} = (w+4)$. We find the curve

$$E : y^2 + (w+1)y = x^3 + wx^2 - x - w$$

(which could also be found by a naive search) with conductor $\mathfrak{N}$. We verify that $\#E(\mathbb{F}_{\mathfrak{p}}) = N\mathfrak{p} + 1 - a_{\mathfrak{p}}(f)$ for all primes $\mathfrak{p}$ up to the limit of the computation. We prove that E is modular using the fact that E has a 3-isogeny, with kernel defined over $F' = F(\sqrt{w(w+4)})$ generated by the points with $x = w - 1$, so we can apply the theorem of Skinner and Wiles. Therefore indeed E corresponds to f.

We now turn to the existence of elliptic curves with everywhere good reduction over totally real fields. The Shimura-Taniyama conjecture predicts that such curves arise from cusp forms of level (1).

Example 6.8. Let $F = \mathbb{Q}(\lambda) = \mathbb{Q}(\zeta_{13})^+$ be the totally real subfield of the cyclotomic field $\mathbb{Q}(\zeta_{13})$ with $\lambda = \zeta_{13} + \zeta_{13}^{-1}$.

The space $S_2(1)$ over F has dimension 1, represented by the cusp form f. Conjecture 6.1 predicts the existence of an elliptic curve A_f over F with everywhere good reduction. We note that A_f must be a $\mathbb{Q}$-curve since the twist f^σ of f by an element $\sigma \in \mathrm{Gal}(F/\mathbb{Q})$ is again a form of level 1 and so (since $\dim S_2(1) = 1$) $f^\sigma = f$ and consequently A_f must be isogenous its Galois conjugates.

Indeed, let

$$A : y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6$$

be the elliptic curve with the following coefficients:

$$a_1 = \lambda^2 + \lambda + 1,$$
$$a_2 = -\lambda^3 + \lambda^2 + \lambda,$$
$$a_3 = \lambda^5 + \lambda^3 + \lambda,$$
$$a_4 = \lambda^5 - \lambda^4 - 11\lambda^3 - \lambda^2 + 3\lambda,$$
$$a_6 = 13\lambda^5 - 31\lambda^4 - 48\lambda^3 + 52\lambda^2 + 33\lambda - 10.$$

We verify that A has everywhere good reduction and that $\#A(F)_{\mathrm{tors}} = 19$ with $A(F)_{\mathrm{tors}}$ generated by the point

$$(\lambda^5 - \lambda^4 - 4\lambda^3 + 3\lambda^2 + 2\lambda - 1, -\lambda^5 + \lambda^4 + \lambda^2).$$

Therefore, by Skinner and Wiles [63, Theorem 5] applied to the 3-adic representation attached to A or [64, Theorem A] to the 19-adic one, we conclude that A is modular, and thus A is our abelian variety A_f.

The elliptic curve A was obtained from a curve over $\mathbb{Q}(\sqrt{13}) \subseteq F$ as follows. There is a 2-dimensional Hecke constituent g in the space of classical modular forms $S_2(169)^{\mathrm{new}}$ over $\mathbb{Q}$ given by

$$g(q) = q + \sqrt{3}q^2 + 2q^3 + q^4 - \sqrt{3}q^5 + \ldots;$$

let A_g be the associated abelian surface, defined over $\mathbb{Q}$. Roberts and Washington [51] showed that A_g twisted by $\sqrt{13}$ is isomorphic over F to $E \times E^\sigma$, where

$$E : y^2 = x^3 + \frac{3483\sqrt{13} - 12285}{2} + (74844\sqrt{13} - 270270),$$

a $\mathbb{Q}$-curve of conductor (13) and σ is the nontrivial automorphism of $\mathbb{Q}(\sqrt{13})$.

The abelian variety A_g is related to the elliptic curve A as follows. Roberts and Washington show that $J_1(13)$ and A_g are isogenous over $\overline{\mathbb{Q}}$. The abelian surface $J_1(13)$ is isogenous over F to $A \times A$, since $J_1(13)$ obtains good reduction over F (see Mazur and Wiles [47, Chapter 3.2, Proposition 2] and Schoof [54]). Indeed, Ogg showed that the abelian surface $J_1(13)$ has a rational point of order 19 [49, p. 225] and Mazur and Tate [46] showed that $J_1(13)$ twisted by $\mathbb{Q}(\sqrt{13})$ is a product of two elliptic curves. We thereby determine an equation for A by showing that it is a quadratic twist of E by some unit in F. We would like to thank Elkies and Watkins for pointing us to the rich history of this curve.

The next example gives the list of all modular elliptic curves (up to isogeny) with everywhere good reduction over a real quadratic field F of discriminant ≤ 1000 and having strict class number one.

Example 6.9. Let $0 \leq D \leq 1000$ be a fundamental discriminant such that $F = \mathbb{Q}(\sqrt{D})$ has strict class number one. We have $\mathbb{Z}_F = \mathbb{Z}[w]$ with $w = \sqrt{D}, (1 + \sqrt{D})/2$, according as $D \equiv 0, 1 \pmod{4}$. Let A be a modular elliptic curve over F with everywhere good reduction. Then A corresponds to a cusp form f of level 1 with rational Fourier coefficients. Computing the spaces $S_2(1)$, we find that either A is a $\mathbb{Q}$-curve (so A is isogenous to its Galois conjugate), or $D \in \{509, 853, 929, 997\}$ and the isogeny class of A is represented by the curve with coefficients as below, up to Galois conjugacy:

D	a_1	a_2	a_3	a_4	a_6
509	-1	$2 + 2w$	$-w$	$162 + 3w$	$71 + 34w$
853	w	$-1 - w$	0	$-5921 + 429w$	$145066 - 9437w$
929	w	$1 - w$	$1 + 20w$	$-1738 - 82w$	$-11808 - 201w$
997	0	w	1	$-289 - 24w$	$-2334 - 144w$

The $\mathbb{Q}$-curves over F are listed in Cremona [8]: for example, the curve $y^2 + xy + uy = x^3$ with $u = (5 + \sqrt{29})/2$ is the smallest such and was discovered by Tate [56].

The curve for discriminant $D = 509$ was discovered by Pinch [54, p. 415]: it was the first example of an elliptic curve having everywhere good reduction which is not a $\mathbb{Q}$-curve, and it was proven to be modular by Socrates and Whitehouse [62] using the method of Faltings and Serre. The curve for $D = 853$ was discovered by Cremona and Watkins independently; the one for $D = 929$ by Elkies; and the one for $D = 997$ by Cremona. Their modularity can be established by applying the theorem of Skinner and Wiles [63, Theorem 5] to the associated 3-adic representation.

As a third and final application, we consider the existence of number fields with small ramification—these are linked to Hilbert modular forms via their associated Galois representations.

In the late 1990s, Gross proposed the following conjecture.

Conjecture 6.10. *For every prime p, there exists a nonsolvable Galois number field K ramified only at p.*

Conjecture 6.10 is true for $p \geq 11$ by an argument due to Serre and Swinnerton-Dyer [55]. For $k = 12, 16, 18, 20, 22$ or 26, let $\Delta_k \in S_k(1)$ be the unique newform of level 1 and weight k. For each such k and every prime p, there is an associated Galois representation $\overline{\rho}_{k,p} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F}_p)$ ramified only at p. In particular, the field K fixed by the kernel of $\rho_{k,p}$ is a number field ramified only at p with Galois group $\mathrm{Gal}(K/\mathbb{Q}) = \mathrm{img}\,\overline{\rho}_{k,p}$.

We say that the prime p is *exceptional* for k if ρ_k is not surjective. The "open image" theorem of Serre [57] implies that the set of primes where $\overline{\rho}_k$ is exceptional is finite. Serre and Swinnerton-Dyer produced the following table of exceptional primes:

k	Exceptional p
12	$2, 3, 5, 7, 23, 691$
16	$2, 3, 5, 7, 11, 31, 59, 3617$
18	$2, 3, 5, 7, 11, 13, 43867$
20	$2, 3, 5, 7, 11, 13, 283, 617$
22	$2, 3, 5, 7, 13, 17, 131, 593$
26	$2, 3, 5, 7, 11, 17, 19, 657931$

31

(The large primes that occur are divisors of the numerators of Bernoulli numbers.) It follows that for every $p \geq 11$ that Conjecture 6.10 is true.

Conversely, it is a consequence of the proof of Serre's conjecture by Khare and Wintenberger [39] together with standard level lowering arguments that if $p \leq 7$ then any odd representation of the absolute Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ to $\mathrm{GL}_2(\overline{\mathbb{F}}_p)$ which is ramified only at p is necessarily reducible (and thus solvable).

To address the conjecture of Gross, we instead look at the residual representations associated to Hilbert cusp forms of parallel weight 2 and level 1 over fields F ramified only at a prime $p \leq 7$. This idea was first pursued by the first author [16] following a suggestion of Gross, who found such a form with $F = \mathbb{Q}(\zeta_{32})^+$, the totally real subfield of the cyclotomic field $\mathbb{Q}(\zeta_{32})$, settling the case $p = 2$. This line of inquiry was followed further by the authors with Matthew Greenberg [17], settling the cases $p = 3, 5$. (The case $p = 7$ was recently settled by Dieulefait [20] by considering the mod 7 Galois representation attached to a genus 2 Siegel cusp form of level 1 and weight 28. Therefore the conjecture of Gross is now a theorem.)

We sketch below the resolution of the case $p = 5$. We take the base field $F = \mathbb{Q}(b)$ to be the subfield of $\mathbb{Q}(\zeta_{25})$ of degree 5, where $b^5 + 5b^4 - 25b^2 - 25b - 5 = 0$. The field F has strict class number 1. Let E be the elliptic curve over F with j-invariant given by

$$(5 \cdot 7^{11})j = -16863524372777476b^4 - 88540369937983588b^3 + 11247914660553215b^2 \\ + 464399360515483572b + 353505866738383680$$

and minimal conductor $\mathfrak{N}$. Then $\mathfrak{N} = \mathfrak{p}_5\mathfrak{p}_7$, where $\mathfrak{p}_5 = ((-2b^3 - 12b^2 + 31b + 25)/7)$ is the unique prime above 5 and $\mathfrak{p}_7 = ((-2b^4 - 9b^3 + 8b^2 + 53b + 6)/7)$ is one of the five primes above 7. Roberts [52] showed that the mod 5 Galois representation

$$\overline{\rho}_{E,5} : \mathrm{Gal}(\overline{F}/F) \to \mathrm{End}(E[5]) \cong \mathrm{GL}_2(\mathbb{F}_{\mathfrak{p}_5}) = \mathrm{GL}_2(\mathbb{F}_5)$$

has projective image $\mathrm{PGL}_2(\mathbb{F}_5)$ and is ramified only at the prime $\mathfrak{p}_5$ (and not $\mathfrak{p}_7$). (We will verify below that E has indeed the right conductor.) The representation $\overline{\rho}_{E,5}$ and its Galois conjugates gives an extension K of $\mathbb{Q}$ with Galois group

$$\mathrm{Gal}(K/\mathbb{Q}) \cong \mathrm{PSL}_2(\mathbb{F}_5)^5 \rtimes \mathbb{Z}/10\mathbb{Z}.$$

By work of Skinner and Wiles (as in Example 6.3), we prove that the 3-adic representation $\rho_{E,3}$ associated to E is modular, and hence E itself is modular. Since E is modular and F has odd degree, E is uniformized by a Shimura curve. Namely, let B be the quaternion algebra over F ramified at four of the five real places. Let $X_0^B(\mathfrak{p}_5\mathfrak{p}_7)$ be the Shimura curve associated to an Eichler order of level $\mathfrak{p}_5\mathfrak{p}_7$ contained in a maximal order $\mathcal{O}$, and let $J_0^B(\mathfrak{p}_5\mathfrak{p}_7)$ be the Jacobian of $X_0^B(\mathfrak{p}_5\mathfrak{p}_7)$. We compute that $J_0^B(\mathfrak{p}_5\mathfrak{p}_7)^{\mathrm{new}}$ has dimension 203. We then find the unique Hilbert newform f_E of parallel weight 2 and level $\mathfrak{p}_5\mathfrak{p}_7$ with integer Fourier coefficients which corresponds to E.

The elliptic curve E found by Roberts [52] was obtained from our computations of Hilbert modular forms at level $\mathfrak{p}_5$ over F. The space $S_2(\mathfrak{p}_5)^{\mathrm{new}}$ has 2 Hecke constituents of dimension 10 and 20, respectively. Let f be a newform in the 20-dimensional constituent. Let $\mathbb{T}_f$ be the restriction of the Hecke algebra $\mathbb{T} = \mathbb{Z}[T_\mathfrak{p}]_\mathfrak{p}$ to this constituent: this is the constituent which yields the Galois representation obtained in the 5-torsion of Roberts's curve. Let $E_f = \mathbb{T}_f \otimes \mathbb{Q} = \mathbb{Q}(a_\mathfrak{p}(f))$ be the field of Fourier coefficients of f and let $\Delta = \mathrm{Aut}(E_f)$. By

direct calculations, we see that $K_f = E_f^\Delta$ is the (totally real) quartic field generated by a root of the polynomial $x^4 + 2x^3 - 75x^2 - 112x + 816$.

The Galois group $\mathrm{Gal}(F/\mathbb{Q})$ acts on $\mathbb{T}$ via its action on ideals of $\mathbb{Z}_F$, namely $\sigma(T_\mathfrak{p}) = T_{\sigma(\mathfrak{p})}$. This action preserves the decomposition of $\mathbb{T}$ into Hecke-irreducible components. By work of Shimura, the action of Δ on Fourier expansions preserves the Hecke constituents. In particular, both these actions preserve $\mathbb{T}_f$ and hence K_f and must be compatible. Therefore, for each $\sigma \in \mathrm{Gal}(F/\mathbb{Q})$, there is a unique $\tau = \tau(\sigma) \in \Delta$ such that, for all prime ideals $\mathfrak{p} \subset \mathbb{Z}_F$, we have

$$a_{\sigma(\mathfrak{p})}(f) = \tau(a_\mathfrak{p}(f)).$$

The map τ thus yields a homomorphism

(6.11)
$$\mathrm{Gal}(F/\mathbb{Q}) \to \Delta$$
$$\sigma \mapsto \tau(\sigma)$$

By direct calculation, we show that this map is an isomorphism. Since $\mathrm{Gal}(F/\mathbb{Q})$ is abelian, the field E_f must be a ray class field over K_f; in fact, we compute that it has conductor equal to a prime above 71 which splits completely in E_f. The ideal $5\mathbb{Z}_{K_f}$ factors as $5\mathbb{Z}_{K_f} = \mathfrak{P}^2\mathfrak{P}'$. The prime $\mathfrak{P}$ splits completely in E_f, and the primes above it in E_f are permuted by $\mathrm{Gal}(E_f/K_f) = \mathrm{Aut}(E_f)$; the prime $\mathfrak{P}'$ is inert.

We have a Galois representation

$$\overline{\rho}_f : \mathrm{Gal}(\overline{F}/F) \to \mathrm{GL}_2(\mathbb{T}_f \otimes \mathbb{F}_5)$$

with $\mathrm{Tr}(\overline{\rho}_f(\mathrm{Frob}_\mathfrak{p})) \equiv a_\mathfrak{p}(f) \pmod 5$ and $\det(\overline{\rho}_f(\mathrm{Frob}_\mathfrak{p})) \equiv N\mathfrak{p} \pmod 5$ for all $\mathfrak{p} \nmid 5$. Let $\mathfrak{m}_f^{(i)}$, $i = 1, \dots, 5$ be the five maximal ideals above (the image of) $\mathfrak{P}$. They give rise to the 5 residual representations

$$\overline{\rho}_f^{(i)} : \mathrm{Gal}(\overline{F}/F) \to \mathrm{GL}_2(\mathbb{F}_5).$$

Let L_i be the fixed field of $\ker(\overline{\rho}_f^{(i)})$, and L the compositum of the L_i. Then L is a Galois extension of F and is ramified only at 5. Since F is Galois and ramified only at 5, and by the above $\mathrm{Gal}(F/\mathbb{Q})$ permutes the fields L_i so preserves L, we see that L is a Galois extension of $\mathbb{Q}$ ramified only at 5. By a result of Shepherd-Barron and Taylor [58], each extension L_i can be realized in the 5-torsion of an elliptic curve E_i/F.

Recall the projective representation $P\overline{\rho}_{E,5}$ from Roberts's elliptic curve E is surjective, ramified at $\mathfrak{p}_5$ but unramified at $\mathfrak{p}_7$. Therefore, the level $\mathfrak{p}_5\mathfrak{p}_7$ is a nonoptimal level for $\overline{\rho}_{E,5}$; thus, by Mazur's Principle [37], we have $\overline{\rho}_{E,5} \cong \overline{\rho}_f^{(i)}$ for some $1 \le i \le 5$. In other words, the extension constructed by Roberts is isomorphic to our field L.

Roberts [52] has given an explicit equation for the number field L (obtained from the 5-division polynomial of the elliptic curve E): the field L is the the splitting field of the polynomial

$$x^{25} - 25x^{22} + 25x^{21} + 110x^{20} - 625x^{19} + 1250x^{18} - 3625x^{17}$$
$$+ 21750x^{16} - 57200x^{15} + 112500x^{14} - 240625x^{13} + 448125x^{12}$$
$$- 1126250x^{11} + 1744825x^{10} - 1006875x^9 - 705000x^8 + 4269125x^7$$
$$- 3551000x^6 + 949625x^5 - 792500x^4 + 1303750x^3 - 899750x^2$$
$$+ 291625x - 36535.$$

To conclude, we consider a question that touches on each of the above three subjects. We reconsider Gross's conjecture (Conjecture 6.10) in the case $p = 2$ [16]. The nonsolvable field which is ramified only at 2 arises from the Galois representation associated to a constituent eigenform $f \in S_2(1)$ in a 16-dimensional subspace of the space of Hilbert cusp forms of parallel weight 2 and level 1 over $F = \mathbb{Q}(\zeta_{32})^+$. Let $E_f = \mathbb{Q}(a_{\mathfrak{p}})$ be the field of Fourier coefficients of f and let $\Delta = \mathrm{Aut}(E_f)$. Let K_f be the fixed field of Δ so that $\mathrm{Gal}(E_f/K_f) = \Delta$. The map (6.11) in this context is again an isomorphism, and so E_f is abelian over K_f and $8 = [F : \mathbb{Q}]$ divides $[E_f : \mathbb{Q}] = 16$. By direct calculations, we show that $K_f = \mathbb{Q}(\sqrt{5})$.

The Eichler-Shimura construction (Conjecture 6.2) predicts the existence a 16-dimensional abelian variety A_f defined over F with everywhere good reduction and real multiplication by E_f associated to f. More should be true, as communicated to us by Gross (private communication). In fact, A_f should descend to an abelian variety of dimension 16 over $\mathbb{Q}$, and we should have $L(A_f, s) = L(f, s)L(f^\sigma, s)$, where $\sigma \in \mathrm{Gal}(E_f/\mathbb{Q})$ is any element that restricts to the nontrivial element of $K_f = \mathbb{Q}(\sqrt{5})$. The endomorphisms of A_f over $\mathbb{Q}$ should be the ring of integers of K_f, and over $\mathbb{Q}$, the variety A_f would have bad reduction only at the prime 2; the nonsolvable extension would then arise as its 2-division field. The conductor $N = 2^{124} = d^4$ of A_f over $\mathbb{Q}$ can be computed from the functional equation of $L(f, s)$, where we note $d = 2^{31}$ is the discriminant of F. We note that A_f is not of GL_2-type over $\mathbb{Q}$ itself as it would be modular by the proof of Serre's conjecture.

Although one knows that the associated Galois representation exists by work of Taylor [67], as Gross says, "With such nice properties, it's a shame that we can't even prove that the abelian variety A_f exists! That's an advantage you have when F has odd degree."

7. ADELIC QUATERNIONIC MODULAR FORMS

In this section, we begin again, and we revisit the definition of Hilbert and quaternionic modular forms allowing F to have arbitrary class number; we refer to Hida [34] as a reference for this section.

We renew our notation. Let F be a totally real field of degree $n = [F : \mathbb{Q}]$ with ring of integers $\mathbb{Z}_F$. Let B be a quaternion algebra over F of discriminant $\mathfrak{D}$. Let $v_1, \ldots, v_n$ be the real places of F (abbreviating as before $x_i = v_i(x)$ for $x \in F$), and suppose that B is split at $v_1, \ldots, v_r$ and ramified at $v_{r+1}, \ldots, v_n$, i.e.

$$(7.1) \qquad B \hookrightarrow B_\infty = B \otimes_{\mathbb{Q}} \mathbb{R} \xrightarrow{\sim} \mathrm{M}_2(\mathbb{R})^r \times \mathbb{H}^{n-r}.$$

Let ι_i denote the ith projection $B \to \mathrm{M}_2(\mathbb{R})$ and $\iota = (\iota_1, \ldots, \iota_r)$. Let

$$F_+^\times = \{x \in F : x_i > 0 \text{ for all } i\}$$

be the group of totally positive elements of F and let $\mathbb{Z}_{F,+}^\times = \mathbb{Z}_F^\times \cap F_+^\times$.

Let $\mathcal{O}_0(1) \subseteq B$ be a maximal order. Let $\mathfrak{N}$ be an ideal of $\mathbb{Z}_F$ coprime to $\mathfrak{D}$ and let $\mathcal{O} = \mathcal{O}_0(\mathfrak{N}) \subseteq \mathcal{O}_0(1)$ be an Eichler order of level $\mathfrak{N}$.

With a view towards generalizations, rather than viewing modular forms as functions on (a Cartesian power of) the upper half-plane which transform in a certain way, we now view them instead more canonically as functions on $B_\infty^\times$. Let $\mathcal{H}^\pm = \mathbb{C} \setminus \mathbb{R}$ be the union of the upper and lower half-planes. Via the embeddings $v_1, \ldots, v_r$, corresponding to the first r factors in (7.1), the group $B_\infty^\times$ acts on $(\mathcal{H}^\pm)^r$ on the right transitively with the stabilizer of

$(\sqrt{-1}, \ldots, \sqrt{-1}) \in \mathcal{H}^r$ being

$$K_\infty = (\mathbb{R}^\times \operatorname{SO}_2(\mathbb{R}))^r \times (\mathbb{H}^\times)^{n-r}.$$

Therefore we can identify

(7.2)
$$\begin{aligned} B_\infty^\times / K_\infty &\to (\mathcal{H}^\pm)^r \\ g &\mapsto z = g(\sqrt{-1}, \ldots, \sqrt{-1}). \end{aligned}$$

From this perspective, it is natural to consider the other (nonarchimedean) places of F at the same time. Let

$$\widehat{\mathbb{Z}} = \varprojlim_n \mathbb{Z}/n\mathbb{Z} = \prod_p{}' \mathbb{Z}_p$$

(where $'$ denotes the restricted direct product) and let $\widehat{}$ denote tensor with $\widehat{\mathbb{Z}}$ over $\mathbb{Z}$. We will define modular forms on B as analytic functions on $B_\infty^\times \times \widehat{B}^\times$ which are invariant on the left by $B^\times$ and transform by $K_\infty \times \widehat{\mathcal{O}}^\times$ in a specified way.

We must first define the codomain of these functions to obtain forms of arbitrary weight. Let $k = (k_1, \ldots, k_n) \in (\mathbb{Z}_{\geq 2})^n$ and suppose that the k_i have the same parity; we call k a *weight*. Let

$$k_0 = \max_i k_i, \quad m_i = (k_0 - k_i)/2, \quad \text{and} \quad w_i = k_i - 2.$$

For an integer $w \geq 0$, let $P_w = P_w(\mathbb{C})$ be the subspace of $\mathbb{C}[x, y]$ consisting of homogeneous polynomials of degree w. For $\gamma \in \operatorname{GL}_2(\mathbb{C})$, let $\overline{\gamma}$ be the adjoint of γ, so that $\gamma\overline{\gamma} = \overline{\gamma}\gamma = \det \gamma$. Define a right action of $\operatorname{GL}_2(\mathbb{C})$ on $P_w(\mathbb{C})$ by

$$(q \cdot \gamma)(x, y) = q((x\ y)\overline{\gamma}) = q(dx - cy, -bx + ay)$$

for $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \operatorname{GL}_2(\mathbb{C})$ and $q \in P_w(\mathbb{C})$. For $m \in \mathbb{Z}$, $\operatorname{GL}_2(\mathbb{C})$ also acts on $P_w(\mathbb{C})$ via the character $\gamma \mapsto (\det \gamma)^m$. By twisting the above action by this character, we get a right $\operatorname{GL}_2(\mathbb{C})$-module denoted by $P_w(m)(\mathbb{C})$. Define the right $\operatorname{GL}_2(\mathbb{C})^{n-r}$-module

(7.3)
$$W_k(\mathbb{C}) = W(\mathbb{C}) = P_{w_{r+1}}(m_{r+1})(\mathbb{C}) \otimes \cdots \otimes P_{w_n}(m_n)(\mathbb{C}).$$

(By convention, if $r = n$ then we set $W_k(\mathbb{C}) = \mathbb{C}$.) For the ramified real places $v_{r+1}, \ldots, v_n$ of F, we choose splittings

$$\iota_i : B \hookrightarrow B \otimes_F \mathbb{C} \cong \operatorname{M}_2(\mathbb{C}).$$

We abbreviate as above $\gamma_i = \iota_i(\gamma)$ for $\gamma \in B$. Then $W_k(\mathbb{C})$ becomes a right $B^\times$-module via $\gamma \mapsto (\gamma_{r+1}, \ldots, \gamma_n) \in \operatorname{GL}_2(\mathbb{C})^{n-r}$. From now on, $W_k(\mathbb{C})$ will be endowed with this action, which we denote by $x \mapsto x^\gamma$ for $x \in W_k(\mathbb{C})$ and $\gamma \in B^\times$. One may identify $W_k(\mathbb{C})$ with the subspace of the algebra $\mathbb{C}[x_{r+1}, y_{r+1}, \ldots, x_n, y_n]$ consisting of those polynomials q which are homogeneous in (x_i, y_i) of degree w_i but with a twisted action.

We consider the space of functions $\phi : B_\infty^\times \times \widehat{B}^\times \to W_k(\mathbb{C})$, with a right action of $K_\infty^\times \times \widehat{B}^\times$ defined by

(7.4)
$$(\phi \mid_k (\kappa, \widehat{\beta}))(g, \widehat{\alpha}) = \left(\prod_{i=1}^r \frac{j(\kappa_i, \sqrt{-1})^{k_i}}{(\det \kappa_i)^{m_i + k_i - 1}} \right) \phi(g\kappa^{-1}, \widehat{\alpha}\widehat{\beta}^{-1})^\kappa.$$

where recall $j(\kappa_i, \sqrt{-1}) = c_i\sqrt{-1} + d_i \in \mathbb{C}$ if $\kappa_i = \begin{pmatrix} a_i & b_i \\ c_i & d_i \end{pmatrix}$. (The presence of the inverses is forced as we want a right action on functions via multiplication of the argument on the right. This almost extends to a right action of $B_\infty^\times \times \widehat{B}^\times$, except that $j(gh, z) = j(g, hz)j(h, z) \neq j(g, z)j(h, z)$ unless h fixes z.)

Definition 7.5. *A* (quaternionic) modular form *of weight k and level $\mathfrak{N}$ for B is an analytic function*

$$\phi : B_\infty^\times \times \widehat{B}^\times \to W_k(\mathbb{C})$$

such that for all $(g, \widehat{\alpha}) \in B_\infty^\times \times \widehat{B}^\times$ we have:

(i) $(\phi\,|_k (\kappa, \widehat{u}))(g, \widehat{\alpha}) = \phi(g, \widehat{\alpha})$ *for all $\kappa \in K_\infty$ and $\widehat{u} \in \widehat{\mathcal{O}}^\times$; and*
(ii) $\phi(\gamma g, \gamma\widehat{\alpha}) = \phi(g, \widehat{\alpha})$ *for all $\gamma \in B^\times$.*

In other words, Definition 7.5 says that a quaternionic modular form of weight k and level $\mathfrak{N}$ is an analytic function which is $B^\times$-invariant on the left and $(K_\infty \times \widehat{\mathcal{O}}^\times)$-equivariant on the right under the action (7.4). In particular, we have

$$(7.6) \qquad\qquad \phi(g, \widehat{\alpha}\widehat{u}) = (\phi\,|_k (1, \widehat{u}))(g, \widehat{\alpha}\widehat{u}) = \phi(g, \widehat{\alpha})$$

for all $\widehat{u} \in \widehat{\mathcal{O}}^\times$ and

$$(7.7) \qquad \phi(g\kappa, \widehat{\alpha}) = (\phi\,|_k (\kappa, 1))(g\kappa, \widehat{\alpha}) = \left(\prod_{i=1}^r \frac{j(\kappa_i, \sqrt{-1})^{k_i}}{(\det \kappa_i)^{m_i + k_i - 1}} \right) \phi(g, \widehat{\alpha})^\kappa.$$

We denote by $M_k^B(\mathfrak{N})$ the space of quaternionic modular forms of weight k and level $\mathfrak{N}$ for B.

Let ϕ be a quaternionic modular form. For $(z, \widehat{\alpha}\widehat{\mathcal{O}}^\times) \in (\mathcal{H}^\pm)^r \times \widehat{B}^\times/\widehat{\mathcal{O}}^\times$, choose $g \in B_\infty^\times$ such that $g(\sqrt{-1}, \dots, \sqrt{-1}) = z$ and define

$$f : (\mathcal{H}^\pm)^r \times \widehat{B}^\times/\widehat{\mathcal{O}}^\times \to W_k(\mathbb{C})$$

$$(7.8) \qquad\qquad f(z, \widehat{\alpha}\widehat{\mathcal{O}}^\times) = \left(\prod_{i=1}^r \frac{(\det g_i)^{m_i + k_i - 1}}{j(g_i, \sqrt{-1})^{k_i}} \right) \phi(g, \widehat{\alpha})^{g^{-1}}.$$

The map f in (7.8) is well-defined by (7.6) and (7.7): we have

$$\left(\prod_{i=1}^r \frac{(\det g_i\kappa_i)^{m_i + k_i - 1}}{j(g_i\kappa_i, \sqrt{-1})^{k_i}} \right) \phi(g\kappa, \widehat{\alpha}\widehat{u})^{(g\kappa)^{-1}} = \left(\prod_{i=1}^r \frac{(\det g_i)^{m_i + k_i - 1}}{j(g_i, \sqrt{-1})^{k_i}} \right) \phi(g, \widehat{\alpha})^{g^{-1}}$$

using the fact that $j(g_i\kappa_i, \sqrt{-1}) = j(g_i, \sqrt{-1})j(\kappa_i, \sqrt{-1})$.

36

The identity 7.5(ii) is translated as follows. Let $\gamma \in B^\times$. Then $g(\sqrt{-1}, \dots, \sqrt{-1}) = z$ is equivalent to $(\gamma g)(\sqrt{-1}, \dots, \sqrt{-1}) = \gamma z$, so

$$
\begin{aligned}
f(\gamma z, \gamma \widehat{\alpha}\widehat{\mathcal{O}}^\times) &= \left(\prod_{i=1}^r \frac{j(\gamma_i g_i, \sqrt{-1})^{k_i}}{(\det \gamma_i g_i)^{m_i + k_i - 1}} \right) \phi(\gamma g, \gamma \widehat{\alpha})^{(\gamma g)^{-1}} \\
(7.9) \qquad &= \left(\prod_{i=1}^r \frac{j(\gamma_i, z_i)^{k_i}}{(\det \gamma_i)^{m_i + k_i - 1}} \right) \left(\prod_{i=1}^r \frac{j(g_i, \sqrt{-1})^{k_i}}{(\det g_i)^{m_i + k_i - 1}} \right) \phi(g, \widehat{\alpha})^{g^{-1} \gamma^{-1}} \\
&= \left(\prod_{i=1}^r \frac{j(\gamma_i, z_i)^{k_i}}{(\det \gamma_i)^{m_i + k_i - 1}} \right) f(z, \widehat{\alpha}\widehat{\mathcal{O}}^\times)^{\gamma^{-1}}
\end{aligned}
$$

where now $j(\gamma_i, z_i) = c_i z_i + d_i \in \mathbb{C}$ if $\gamma_i = \begin{pmatrix} a_i & b_i \\ c_i & d_i \end{pmatrix}$ for all $\gamma \in B^\times$ and we have the relation $j(\gamma\delta, z) = j(\gamma, \delta z) j(\delta, z)$ for all $z \in \mathcal{H}$ and $g, h \in B^\times$. Accordingly, we define a right action of $B^\times$ on the space of functions in (7.8) by

$$
(7.10) \qquad (f \mid_k \gamma)(z, \widehat{\alpha}\widehat{\mathcal{O}}^\times) = \left(\prod_{i=1}^r \frac{(\det \gamma_i)^{m_i + k_i - 1}}{j(\gamma_i, z_i)^{k_i}} \right) f(\gamma z, \gamma \widehat{\alpha}\widehat{\mathcal{O}}^\times)^\gamma.
$$

Then

$$
(f \mid_k \gamma)(z, \widehat{\alpha}\widehat{\mathcal{O}}^\times) = f(z, \widehat{\alpha}\widehat{\mathcal{O}}^\times).
$$

Note that the central subgroup $F^\times \subseteq B^\times$ acts by $(f \mid_k a)(z, \widehat{\alpha}\widehat{\mathcal{O}}^\times) = N_{F/\mathbb{Q}}(a)^{k_0 - 2} f(z, a\widehat{\alpha}\widehat{\mathcal{O}}^\times)$ for $a \in F^\times$.

The $\mathbb{C}$-vector space of modular forms of weight k and level $\mathfrak{N}$ on B is finite-dimensional and is denoted $M_k^B(\mathfrak{N})$.

Lemma 7.11. *There is a bijection between $M_k^B(\mathfrak{N})$ and the space of functions $f : (\mathcal{H}^\pm)^r \times \widehat{B}^\times/\widehat{\mathcal{O}}^\times \to W_k(\mathbb{C})$ that are holomorphic in the first variable and locally constant in the second variable and such that*

$$
f \mid_k \gamma = f \text{ for all } \gamma \in B^\times.
$$

From now on, we will only work with modular forms f as presented in Lemma 7.11.

We define the *quaternionic Shimura variety of level $\mathfrak{N}$* associated to B as the double coset

$$
X_0^B(\mathfrak{N})(\mathbb{C}) = B^\times \backslash (B_\infty^\times/K_\infty \times \widehat{B}^\times/\widehat{\mathcal{O}}^\times) = B^\times \backslash ((\mathcal{H}^\pm)^r \times \widehat{B}^\times/\widehat{\mathcal{O}}^\times);
$$

the set $X_0^B(\mathfrak{N})(\mathbb{C})$ can be equipped the structure of a complex (possibly disconnected) Riemannian manifold of dimension r.

Example 7.12. We recover first the definition of classical modular forms when $F = \mathbb{Q}$ and $B = M_2(\mathbb{Q})$. For simplicity, we take $N = 1$. In this case, $r = 1$ so $W_k(\mathbb{C}) = \mathbb{C}$ and $m = 0$.

The action (7.10) is simply

$$
(f \mid_k \gamma)(z, \widehat{\alpha}\widehat{\mathcal{O}}^\times) = \frac{(\det \gamma)^{k-1}}{j(\gamma, z)^k} f(\gamma z, \gamma \widehat{\alpha}\widehat{\mathcal{O}}^\times).
$$

We take the definition (7.8) as our starting point. The element $\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \in B^\times = GL_2(\mathbb{Q})$ identifies the upper and lower half-planes, so a modular form $f : \mathcal{H}^\pm \times GL_2(\widehat{\mathbb{Q}})/GL_2(\widehat{\mathbb{Z}}) \to \mathbb{C}$

is determined by its restriction $f : \mathcal{H} \times \mathrm{GL}_2(\widehat{\mathbb{Q}})/\widehat{\Gamma}_0(N) \to \mathbb{C}$ and the subgroup of $\mathrm{GL}_2(\mathbb{Q})$ which preserves $\mathcal{H}$ is exactly $\mathrm{GL}_2^+(\mathbb{Q})$.

We wish to recover the classical action using this new action of $\mathrm{GL}_2^+(\mathbb{Q})$, so we are led to consider the double coset $\mathrm{GL}_2^+(\mathbb{Q})\backslash\mathrm{GL}_2(\widehat{\mathbb{Q}})/\mathrm{GL}_2(\widehat{\mathbb{Z}})$. An element of this double coset is specified by an element $\widehat{\alpha} \in \mathrm{GL}_2(\widehat{\mathbb{Q}})$ up to right-multiplication by $\mathrm{GL}_2(\widehat{\mathbb{Z}})$, i.e. a $\widehat{\mathbb{Z}}$-lattice in $\widehat{\mathbb{Q}}^2$, i.e. $\widehat{\Lambda} \in \mathrm{Lat}(\widehat{\mathbb{Q}}^2)$, specified by the rows of $\widehat{\alpha}$. But the map $\mathrm{Lat}(\mathbb{Q}^2) \to \mathrm{Lat}(\widehat{\mathbb{Q}}^2)$ by $\Lambda \mapsto \widehat{\Lambda}$ is a bijection, with inverse $\widehat{\Lambda} \mapsto \widehat{\Lambda} \cap \mathbb{Q}^2$. And since $\mathrm{GL}_2^+(\mathbb{Q})$ acts transitively on the left on the set of lattices $\mathrm{Lat}(\mathbb{Q}^2)$, we conclude that $\# \mathrm{GL}_2^+(\mathbb{Q})\backslash\mathrm{GL}_2(\widehat{\mathbb{Q}})/\mathrm{GL}_2(\widehat{\mathbb{Z}}) = 1$.

It follows that f is uniquely specified by the function $f(z, \widehat{\mathcal{O}}^\times)$ for $z \in \mathcal{H}$, which by abuse of notation we write simply $f : \mathcal{H} \to \mathbb{C}$. The stabilizer of $\mathrm{GL}_2^+(\mathbb{Q})$ acting on $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ by multiplication on the left is $\mathrm{GL}_2^+(\mathbb{Z})$, so we recover the condition

$$(f\,|_k\,\gamma)(z) = \frac{(\det\gamma)^{k-1}}{j(\gamma, z)^k} f(\gamma z)$$

for all $\gamma \in \mathrm{GL}_2^+(\mathbb{Z})$, which is exactly the definition given in Section 1.

The interested reader can modify this argument for $N > 1$; alternatively, we give a general derivation below.

We now define cusp forms. If $B \cong \mathrm{M}_2(F)$, then we are in the situation of Hilbert modular forms (but over a field with arbitrary class number): so we define a *cusp form* to be a form f such that $f(z) \to 0$ whenever z tends to a cusp $\mathbb{P}^1(F) \hookrightarrow \mathbb{P}^1(\mathbb{R})^n$. Otherwise, the Shimura variety $X_0^B(\mathfrak{N})(\mathbb{C})$ is compact. If B is indefinite, so $0 < r \leq n$, then there are no cusps, and we define the space of cusp forms to be $S_k^B(\mathfrak{N}) = M_k^B(\mathfrak{N})$. Finally, suppose B is definite; then $r = 0$. If $k = (2, \ldots, 2)$, then we define $E_k^B(\mathfrak{N})$ to be the space of those $f \in M_k^B(\mathfrak{N})$ such that f factors through $\mathrm{nrd} : \widehat{B}^\times \to \widehat{F}^\times$; otherwise, we set $E_k^B(\mathfrak{N}) = 0$. Then there is an orthogonal decomposition $M_k^B(\mathfrak{N}) = S_k^B(\mathfrak{N}) \oplus E_k^B(\mathfrak{N})$ and we call $S_k^B(\mathfrak{N})$ the space of *cusp forms* for B.

The spaces $M_k^B(\mathfrak{N})$ and $S_k^B(\mathfrak{N})$ come equipped with an action of pairwise commuting diagonalizable *Hecke operators* $T_\mathfrak{n}$ indexed by the nonzero ideals $\mathfrak{n}$ of $\mathbb{Z}_F$, defined as follows. Given $f \in S_k^B(\mathfrak{N})$ and $\widehat{\pi} \in \widehat{B}^\times$, we define a Hecke operator associated to $\widehat{\pi}$ as follows: we write

$$(7.13) \qquad\qquad \widehat{\mathcal{O}}^\times \widehat{\pi} \widehat{\mathcal{O}}^\times = \bigsqcup_i \widehat{\mathcal{O}}^\times \widehat{\pi}_i$$

and let

$$(7.14) \qquad\qquad (T_\pi f)(z, \widehat{\alpha}\widehat{\mathcal{O}}^\times) = \sum_i f(z, \widehat{\alpha}\widehat{\pi}_i^{-1}\widehat{\mathcal{O}}^\times).$$

(Again, although it may seem unnatural, the choice of inverse here is to make the definitions agree with the classical case.)

For a prime $\mathfrak{p}$ of $\mathbb{Z}_F$ with $\mathfrak{p} \nmid \mathfrak{D}\mathfrak{N}$, we denote by $T_\mathfrak{p}$ the Hecke operator $T_{\widehat{\pi}}$ where $\widehat{\pi} \in \widehat{B}^\times$ is such that $\widehat{\pi}_v = 1$ for $v \neq \mathfrak{p}$ and $\widehat{\pi}_\mathfrak{p} = \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix} \in \mathcal{O} \otimes_{\mathbb{Z}_F} \mathbb{Z}_{F,\mathfrak{p}} \cong \mathrm{M}_2(\mathbb{Z}_{F,\mathfrak{p}})$ where $p \in \mathbb{Z}_{F,\mathfrak{p}}$ is a uniformizer at $\mathfrak{p}$.

Equivalently, for a prime $\mathfrak{p}$ and $\widehat{p} \in \widehat{\mathbb{Z}}_F$ such that $\widehat{p}\widehat{\mathbb{Z}}_F \cap \mathbb{Z}_F = \mathfrak{p}$, we define

$$\Theta(\mathfrak{p}) = \widehat{\mathcal{O}}^\times \backslash \{\widehat{\pi} \in \widehat{\mathcal{O}} : \mathrm{nrd}(\widehat{\pi}) = \widehat{p}\}.$$

a set of cardinality $N\mathfrak{p} + 1$, and define

$$(7.15) \qquad (T_\mathfrak{p}f)(z, \widehat{\alpha}\widehat{\mathcal{O}}^\times) = \sum_{\widehat{\pi} \in \Theta(\mathfrak{p})} f(z, \widehat{\alpha}\widehat{\pi}^{-1}\widehat{\mathcal{O}}^\times)$$

where we have implicitly chosen representatives $\widehat{\pi} \in \widehat{\mathcal{O}}$ for the orbits in $\Theta(\mathfrak{p})$. For an ideal $\mathfrak{n}$ of $\mathbb{Z}_F$, the operator $T_\mathfrak{n}$ is defined analogously.

We say that a cusp form f is a *newform* if it is an eigenvector of the Hecke operators which does not belong to $M_k(\mathfrak{M})$ for $\mathfrak{M} \mid \mathfrak{N}$.

To unpack this definition further, and to relate this definition with the definitions given previously, we investigate the structure of the Shimura variety

$$X_0^B(\mathfrak{N})(\mathbb{C}) = B^\times \backslash (B_\infty^\times/K_\infty \times \widehat{B}^\times/\widehat{\mathcal{O}}^\times) = B^\times \backslash ((\mathcal{H}^\pm)^r \times \widehat{B}^\times/\widehat{\mathcal{O}}^\times).$$

By Eichler's theorem of norms [68, Théorème III.4.1], we have

$$\mathrm{nrd}(B^\times) = F_{(+)}^\times = \{a \in F^\times : v_i(a) > 0 \text{ for } i = r+1, \dots, n\},$$

i.e. the norms from $B^\times$ consists of the subgroup of elements of F which are positive at all real places which are ramified in B. In particular, $B^\times/B_+^\times \cong (\mathbb{Z}/2\mathbb{Z})^r$, where

$$B_+^\times = \{\gamma \in B : \mathrm{nrd}(\gamma) \in F_+^\times\}$$

is the subgroup of $B^\times$ whose elements have totally positive reduced norm.

The group $B_+^\times$ acts on $\mathcal{H}^r$, therefore we may identify

$$X_0^B(\mathfrak{N})(\mathbb{C}) = B_+^\times \backslash (\mathcal{H}^r \times \widehat{B}^\times/\widehat{\mathcal{O}}^\times)$$

and a modular form on $(\mathcal{H}^\pm)^r \times \widehat{B}^\times/\widehat{\mathcal{O}}^\times$ can be uniquely recovered from its restriction to $\mathcal{H}^r \times \widehat{B}^\times/\widehat{\mathcal{O}}^\times$. Now we have a natural (continuous) projection map

$$X_0^B(\mathfrak{N})(\mathbb{C}) \to B_+^\times \backslash \widehat{B}^\times/\widehat{\mathcal{O}}^\times.$$

The reduced norm gives a surjective map

$$(7.16) \qquad \mathrm{nrd} : B_+^\times \backslash \widehat{B}^\times/\widehat{\mathcal{O}}^\times \to F_+^\times \backslash \widehat{F}^\times/\widehat{\mathbb{Z}}_F^\times \cong \mathrm{Cl}^+ \mathbb{Z}_F.$$

where $\mathrm{Cl}^+ \mathbb{Z}_F$ denotes the strict class group of $\mathbb{Z}_F$, i.e. the ray class group of $\mathbb{Z}_F$ with modulus equal to the product of all real (infinite) places of F. The theorem of strong approximation [68, Théorème III.4.3] implies that (7.16) is a bijection if B is indefinite. So our description will accordingly depend on whether B is indefinite or definite.

First, suppose that B is indefinite. Then space $X_0^B(\mathfrak{N})(\mathbb{C})$ is the disjoint union of connected Riemannian manifolds indexed by $\mathrm{Cl}^+ \mathbb{Z}_F$, which we identify explicitly as follows. Let the ideals $\mathfrak{a} \subseteq \mathbb{Z}_F$ form a set of representatives for $\mathrm{Cl}^+ \mathbb{Z}_F$, and let $\widehat{a} \in \widehat{\mathbb{Z}}_F$ be such that $\widehat{a}\widehat{\mathbb{Z}}_F \cap \mathbb{Z}_F = \mathfrak{a}$. (For the trivial class $\mathfrak{a} = \mathbb{Z}_F$, we choose $\widehat{a} = \widehat{1}$). By (7.16), there exists $\widehat{\alpha} \in \widehat{B}^\times$ such that $\mathrm{nrd}(\widehat{\alpha}) = \widehat{a}$. We let $\mathcal{O}_\mathfrak{a} = \widehat{\alpha}\widehat{\mathcal{O}}\widehat{\alpha}^{-1} \cap B$ so that $\mathcal{O}_{(1)} = \mathcal{O}$, and we put $\Gamma_\mathfrak{a} = \mathcal{O}_{\mathfrak{a},+}^\times = \widehat{\mathcal{O}}_\mathfrak{a}^\times \cap B_+^\times$. Then we have

$$(7.17) \qquad X_0^B(\mathfrak{N})(\mathbb{C}) = \bigsqcup_{[\mathfrak{a}] \in \mathrm{Cl}^+(\mathbb{Z}_F)} B_+^\times (\mathcal{H}^r \times \widehat{\alpha}\widehat{\mathcal{O}}^\times) \xrightarrow{\sim} \bigsqcup_{[\mathfrak{a}] \in \mathrm{Cl}^+(\mathbb{Z}_F)} \Gamma_\mathfrak{a} \backslash \mathcal{H}^r,$$

where the last identification is obtained via the bijection

$$B_+^\times \backslash (\mathcal{H}^r \times \widehat{\alpha}\widehat{\mathcal{O}}^\times) \xrightarrow{\sim} \Gamma_\mathfrak{a} \backslash \mathcal{H}^r$$

(7.18)

$$B_+^\times(z, \widehat{\alpha}\widehat{\mathcal{O}}^\times) \mapsto z$$

Now let $f \in M_k^B(\mathfrak{N})$, so that $f : (\mathcal{H}^\pm)^r \times \widehat{B}^\times / \widehat{\mathcal{O}}^\times \to W_k(\mathbb{C})$ satisfies $f \mid_k \gamma = f$ for all $\gamma \in B^\times$. Let $M_k^B(\mathfrak{N}, \mathfrak{a})$ be the space of functions $f_\mathfrak{a} : \mathcal{H}^r \to W_k(\mathbb{C})$ such that $f_\mathfrak{a} \mid_k \gamma = f_\mathfrak{a}$ for all $\gamma \in \Gamma_\mathfrak{a}$, where we define

$$(f_\mathfrak{a} \mid \gamma)(z) = \left(\prod_{i=1}^r \frac{(\det \gamma_i)^{m_i + k_i - 1}}{j(\gamma_i, z)^{k_i}} \right) f_\mathfrak{a}(\gamma z)^\gamma$$

for $\gamma \in B^\times$. Then by (7.18), the map

(7.19)

$$M_k^B(\mathfrak{N}) \to \bigoplus_{[\mathfrak{a}] \in \mathrm{Cl}^+(\mathbb{Z}_F)} M_k^B(\mathfrak{N}, \mathfrak{a})$$

$$f \mapsto (f_\mathfrak{a})$$

where

$$f_\mathfrak{a} : \mathcal{H}^r \to W_k(\mathbb{C})$$

$$f_\mathfrak{a}(z) = f(z, \widehat{\alpha}\widehat{\mathcal{O}}^\times)$$

is an isomorphism.

We now explain how the Hecke module structure on the left-hand side of (7.19), defined in (7.14)–(7.15), is carried over to the right-hand side. We follow Shimura [59, Section 2]. We consider the action on the summand corresponding to $[\mathfrak{a}] \in \mathrm{Cl}^+(\mathbb{Z}_F)$. Extending the notation above, among the representatives chosen, let $\mathfrak{b}$ be such that $[\mathfrak{b}] = [\mathfrak{a}\mathfrak{p}^{-1}]$, let $\widetilde{b}\mathbb{Z}_F \cap \mathbb{Z}_F = \mathfrak{b}$, and let $\widehat{\beta} \in \widehat{B}^\times$ be such that $\mathrm{nrd}(\widehat{\beta}) = \widehat{b}$.

By definition,

$$(T_\mathfrak{p}f)_\mathfrak{a}(z) = (T_\mathfrak{p}f)(z, \widehat{\alpha}\widehat{\mathcal{O}}^\times) = \sum_{\widehat{\pi} \in \Theta(\mathfrak{p})} f(z, \widehat{\alpha}\widehat{\pi}^{-1}\widehat{\mathcal{O}}^\times).$$

Let $\widehat{\pi} \in \Theta(\mathfrak{p})$. Then by strong approximation, we have

(7.20)

$$\widehat{\alpha}\widehat{\pi}^{-1}\widehat{\mathcal{O}}\widehat{\beta}^{-1} \cap B = \varpi^{-1}\mathcal{O}_\mathfrak{b}$$

with $\varpi \in B^\times$, since this lattice has reduced norm $[\mathfrak{a}\mathfrak{p}^{-1}(\mathfrak{a}\mathfrak{p}^{-1})^{-1}] = [(1)]$. Therefore, there exists $\widehat{u} \in \widehat{\mathcal{O}}$ such that $\widehat{\alpha}\widehat{\pi}^{-1}\widehat{u}\widehat{\beta}^{-1} = \varpi^{-1}$ whence

(7.21)

$$(T_\mathfrak{p}f)_\mathfrak{a}(z) \sum_{\widehat{\pi} \in \Theta(\mathfrak{p})} f(z, \widehat{\alpha}\widehat{\pi}^{-1}\widehat{\mathcal{O}}^\times) = \sum_\varpi f(z, \varpi^{-1}\widehat{\beta}\widehat{\mathcal{O}}^\times);$$

the second sum runs over a choice of ϖ as in equation (7.20) corresponding to each $\widehat{\pi} \in \Theta(\mathfrak{p})$. This latter sum can be identified with a sum over values of $f_\mathfrak{b}$ as follows. We have

$$f(z, \varpi^{-1}\widehat{\beta}\widehat{\mathcal{O}}^\times) = (f \mid_k \varpi)(z, \varpi^{-1}\widehat{\beta}\widehat{\mathcal{O}}^\times)$$

$$= \left(\prod_{i=1}^r \frac{(\det \varpi_i)^{m_i + k_i - 1}}{j(\varpi_i, z_i)^{k_i}} \right) f(\varpi z, \widehat{\beta}\widehat{\mathcal{O}}^\times)^\varpi = (f_\mathfrak{b} \mid_k \varpi)(z).$$

The first equality follows from the $B^\times$-invariance of f and the others by definition of the slash operators. Putting these together, we have

$$(7.22) \qquad (T_\mathfrak{p} f)_\mathfrak{a}(z) = \sum_{\varpi} (f_\mathfrak{b} \,|_k\, \varpi)(z).$$

(The naturality of this definition explains the choice of inverses above.)

This adelic calculation can be made global as follows. Let $I_\mathfrak{a} = \widehat{\alpha}\widehat{\mathcal{O}} \cap B$ and $I_\mathfrak{b} = \widehat{\beta}\widehat{\mathcal{O}} \cap B$. For $\widehat{\pi} \in \Theta(\mathfrak{p})$, we have

$$\widehat{\alpha}\widehat{\pi}^{-1}\widehat{\mathcal{O}}\widehat{\beta}^{-1} \cap B = \varpi^{-1}\mathcal{O}_\mathfrak{b}$$

hence

$$(7.23) \qquad \mathcal{O}_\mathfrak{b}\varpi = \widehat{\beta}\widehat{\mathcal{O}}\widehat{\pi}\widehat{\alpha}^{-1} = (\widehat{\beta}\widehat{\mathcal{O}})\widehat{\alpha}^{-1}(\widehat{\alpha}\widehat{\mathcal{O}}\widehat{\alpha}^{-1})\widehat{\alpha}\widehat{\pi}\widehat{\alpha}^{-1} \cap B = I_\mathfrak{b}I_\mathfrak{a}^{-1}J.$$

The elements ϖ thus obtained are characterized by their norms (in the right lattice), as with the Hecke operators defined previously (5.1): we analogously define

$$(7.24) \qquad \begin{aligned} \Theta(\mathfrak{p})_{\mathfrak{a},\mathfrak{b}} &= \Gamma_\mathfrak{b} \backslash \{\varpi \in I_\mathfrak{b}I_\mathfrak{a}^{-1} \cap B_+^\times : \mathrm{nrd}(I_\mathfrak{b}I_\mathfrak{a}^{-1})\mathfrak{p} = (\mathrm{nrd}(\varpi))\} \\ &= \Gamma_\mathfrak{b} \backslash \{\varpi \in I_\mathfrak{b}I_\mathfrak{a}^{-1} \cap B_+^\times : \mathrm{nrd}(\varpi)\mathfrak{b} = \mathfrak{a}\mathfrak{p}\}. \end{aligned}$$

Then for $f_\mathfrak{b} \in M_k^B(\mathfrak{N}, \mathfrak{b})$, we have $T_\mathfrak{p} f_\mathfrak{b} \in M_k^B(\mathfrak{N}, \mathfrak{a})$ and

$$T_\mathfrak{p} f_\mathfrak{b} = \sum_{\varpi \in \Theta(\mathfrak{p})_{\mathfrak{a},\mathfrak{b}}} f_\mathfrak{b} \,|_k\, \varpi$$

where $[\mathfrak{b}] = [\mathfrak{a}\mathfrak{p}^{-1}]$.

Example 7.25. If F has strict class number 1, then $I_\mathfrak{a} = I_\mathfrak{b} = \mathcal{O} = \mathcal{O}_a$ so $\mathcal{O}_\mathfrak{b}\varpi_a = \mathcal{O}\pi_a$ as in Section 5.

We note that the isomorphism (7.19) preserves the subspace of cusp forms in a way that is compatible with the Hecke action, so we have a decomposition

$$S_k^B(\mathfrak{N}) \xrightarrow{\sim} \bigoplus_{[\mathfrak{a}] \in \mathrm{Cl}^+(\mathbb{Z}_F)} S_k^B(\mathfrak{N}, \mathfrak{a}).$$

Example 7.26. Let $B = \mathrm{M}_2(F)$, and let $\mathcal{O} = \mathcal{O}_0(\mathfrak{N}) \subset \mathcal{O}_0(1) = \mathrm{M}_2(\mathbb{Z}_F)$. Then we may take $\widehat{\alpha} = \begin{pmatrix} \widehat{a} & 0 \\ 0 & 1 \end{pmatrix} \in \mathrm{GL}_2(\widehat{F})$, and so we find simply that

$$\mathcal{O}_\mathfrak{a} = \widehat{\alpha}\,\mathrm{M}_2(\mathbb{Z}_F)\widehat{\alpha}^{-1} \cap B = \begin{pmatrix} \mathbb{Z}_F & \mathfrak{a} \\ \mathfrak{N}\mathfrak{a}^{-1} & \mathbb{Z}_F \end{pmatrix} = \mathcal{O}_0(\mathfrak{N}, \mathfrak{a})$$

Let

$$\Gamma_0(\mathfrak{N}, \mathfrak{a}) = \mathcal{O}_0(\mathfrak{N}, \mathfrak{a})_+^\times = \left\{ \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathcal{O}_0(\mathfrak{N}, \mathfrak{a}) : \det\gamma \in \mathbb{Z}_{F,+}^\times \right\}.$$

Then

$$X_0^B(\mathfrak{N})(\mathbb{C}) = \bigsqcup_{[\mathfrak{a}] \in \mathrm{Cl}^+(\mathbb{Z}_F)} \Gamma_0(\mathfrak{N}, \mathfrak{a})\backslash \mathcal{H}^n$$

is a disjoint union.

A *Hilbert modular form of weight k and level* $\mathfrak{N}$ is a tuple $(f_{\mathfrak{a}})$ of holomorphic functions $f_{\mathfrak{a}} : \mathcal{H}^n \to \mathbb{C}$, indexed by $\mathrm{Cl}^+ \mathbb{Z}_F$, such that for all $\mathfrak{a}$ we have

$$(f_{\mathfrak{a}} \mid_k \gamma)(z) = f_{\mathfrak{a}}(z) \text{ for all } \gamma \in \Gamma_0(\mathfrak{N}, \mathfrak{a})$$

(with the extra assumption that f is holomorphic at the cusps if $F = \mathbb{Q}$). Or, put another way, let $M_k(\mathfrak{N}, \mathfrak{a})$ be the set of holomorphic functions $\mathcal{H}^n \to \mathbb{C}$ such that $(f \mid_k \gamma)(z) = f(z)$ for all $\gamma \in \Gamma_0(\mathfrak{N}, \mathfrak{a})$; then

$$M_k(\mathfrak{N}) = \bigoplus_{[\mathfrak{a}]} M_k(\mathfrak{N}, \mathfrak{a}).$$

In particular, we recover the definitions in Section 2 when F has strict class number 1.

A modular form $f \in M_k(\mathfrak{N}, \mathfrak{a})$ admits a Fourier expansion

$$f(z) = a_0 + \sum_{\mu \in (\mathfrak{a}\mathfrak{d}^{-1})_+} a_\mu e^{2\pi i \mathrm{Tr}(\mu z)}$$

analogous to (2.5). We say that $f \in M_k(\mathfrak{N}, \mathfrak{a})$ is a *cusp form* if $f(z) \to 0$ as z tends to any cusp. Letting $S_k(\mathfrak{N}, \mathfrak{a})$ be the space of such cusp forms, we have

$$S_k(\mathfrak{N}) = \bigoplus_{[\mathfrak{a}]} S_k(\mathfrak{N}, \mathfrak{a}).$$

Let $f = (f_{\mathfrak{a}}) \in S_k(\mathfrak{N})$ be a Hilbert cusp form and let $\mathfrak{n} \subseteq \mathbb{Z}_F$ be an ideal. Suppose that $[\mathfrak{n}] = [\mathfrak{a}\mathfrak{d}^{-1}]^{-1}$ amongst the representatives chosen for $\mathrm{Cl}^+(\mathbb{Z}_F)$, and let $\nu \in \mathbb{Z}_F$ be such that $\mathfrak{n} = \nu(\mathfrak{a}\mathfrak{d}^{-1})^{-1} = \nu\mathfrak{d}\mathfrak{a}^{-1}$. We define $a_{\mathfrak{n}} = \nu^m a_\nu(f_{\mathfrak{a}})$; the transformation rule implies that $a_{\mathfrak{n}}$ only depends on $\mathfrak{n}$ and we call $a_{\mathfrak{n}}$ the *Fourier coefficient* of f at $\mathfrak{n}$.

Now suppose that B is definite. Then the Shimura variety is simply

$$X_0^B(\mathfrak{N})(\mathbb{C}) = B^\times \backslash \widehat{B}^\times / \widehat{\mathcal{O}}^\times = \mathrm{Cl}\,\mathcal{O}$$

and so is canonically identified with the set of right ideal classes of $\mathcal{O}$. Note that the reduced norm map (7.16) here is the map $\mathrm{nrd} : \mathrm{Cl}\,\mathcal{O} \to \mathrm{Cl}^+ \mathbb{Z}_F$ which is surjective but not a bijection, in general. A modular form $f \in M_k^B(\mathfrak{N})$ is then just a map $f : \widehat{B}^\times / \widehat{\mathcal{O}}^\times \to W_k(\mathbb{C})$ such that $f \mid_k \gamma = f$ for all $\gamma \in B^\times$. Such a function is completely determined by its values on a set of representatives of $\mathrm{Cl}\,\mathcal{O}$; moreover, given any right ideal $I = \widehat{\alpha}\widehat{\mathcal{O}} \cap B$, the stabilizer of $B^\times$ acting on $\widehat{\alpha}\widehat{\mathcal{O}}$ by left multiplication is $\mathcal{O}_L(I)^\times = \widehat{\alpha}\widehat{\mathcal{O}}^\times\widehat{\alpha}^{-1} \cap B^\times$. Therefore, there is an isomorphism of complex vector spaces given by

(7.27)
$$M_k^B(\mathfrak{N}) \to \bigoplus_{\substack{[I] \in \mathrm{Cl}(\mathcal{O}) \\ I = \widehat{\alpha}\widehat{\mathcal{O}} \cap B}} W_k(\mathbb{C})^{\Gamma(I)}$$

$$f \mapsto (f(\widehat{\alpha})),$$

where $\Gamma(I) = \widehat{\alpha}\widehat{\mathcal{O}}^\times\widehat{\alpha}^{-1} \cap B^\times = \mathcal{O}_L(I)^\times$ and $W_k(\mathbb{C})^{\Gamma(I)}$ is the $\Gamma(I)$-invariant subspace of $W_k(\mathbb{C})$.

Having now discussed both the definite and indefinite cases in turn, we return to a general quaternion algebra B. Let $f \in S_k^B(\mathfrak{N})^{\mathrm{new}}$ be a newform. A theorem of Shimura states that

the coefficients $a_{\mathfrak{n}}$ are algebraic integers and $E_f = \mathbb{Q}(\{a_{\mathfrak{n}}\})$ is a number field. The Hecke eigenvalues $a_{\mathfrak{n}}$ determine the L-series

$$L(f,s) = \sum_{\mathfrak{n} \subseteq \mathbb{Z}_F} \frac{a_{\mathfrak{n}}}{N\mathfrak{n}^s} = \prod_{\mathfrak{p} \nmid \mathfrak{N}} \left(1 - \frac{a_{\mathfrak{p}}}{N\mathfrak{p}^s} + \frac{1}{N\mathfrak{p}^{2s+1-k_0}}\right)^{-1} \prod_{\mathfrak{p} \mid \mathfrak{N}} \left(1 - \frac{a_{\mathfrak{p}}}{N\mathfrak{p}^s}\right)^{-1}$$

associated to f (defined for $\operatorname{Re} s > 1$). Moreover, associated to f is a Galois representation: for $\mathfrak{l}$ a prime of $\mathbb{Z}_{E_f}$ and $E_{f,\mathfrak{l}}$ the completion of E_f at $\mathfrak{l}$, there is an absolutely irreducible, totally odd Galois representation

$$\rho_{f,\mathfrak{l}} : \operatorname{Gal}(\overline{F}/F) \to \operatorname{GL}_2(E_{f,\mathfrak{l}})$$

such that, for any prime $\mathfrak{p} \nmid \mathfrak{l}\mathfrak{N}$, we have

$$\operatorname{Tr}(\rho_{f,\mathfrak{l}}(\operatorname{Frob}_{\mathfrak{p}})) = a_{\mathfrak{p}}(f) \quad \text{and} \quad \det(\rho_{f,\mathfrak{l}}(\operatorname{Frob}_{\mathfrak{p}})) = N\mathfrak{p}^{k_0-1}.$$

The existence of this representation is due to work of Blasius-Rogawski [2], Carayol [6], Deligne [13], Saito [53], Taylor [67], and Wiles [74].

The statement of the Jacquet-Langlands correspondence (3.9) reads the same in this more general context.

Theorem 7.28 (Jacquet-Langlands). *There is an injective map of Hecke modules*

$$S_k^B(\mathfrak{N}) \hookrightarrow S_k(\mathfrak{D}\mathfrak{N})$$

whose image consists of those forms which are new at all primes dividing $\mathfrak{D}$.

We are now ready to state the main general result of this article, generalizing the result of Theorem 2.8 to arbitrary class number and arbitrary weight.

Theorem 7.29 (Dembélé-Donnelly [18], Voight [71]). *There exists an algorithm which, given a totally real field F, a nonzero ideal $\mathfrak{N} \subseteq \mathbb{Z}_F$, and a weight $k \in (\mathbb{Z}_{\geq 2})^{[F:\mathbb{Q}]}$, computes the space $S_k(\mathfrak{N})$ of Hilbert cusp forms of level $\mathfrak{N}$ over F as a Hecke module.*

The proof of this theorem is discussed in the next two sections. It falls again naturally into two methods, definite and indefinite, which overlap just as in Remark 3.10.

8. Definite method, arbitrary class number

In this section, we return to the totally definite case but allow arbitrary class number. As explained above, the space $M_k^B(\mathfrak{N})$ of modular forms of level $\mathfrak{N}$ and weight k on B is the space of functions $f : \widehat{B}^\times / \widehat{\mathcal{O}}^\times \to W_k(\mathbb{C})$ such that $f \mid_k \gamma = f$ for all $\gamma \in B^\times$.

We can use the identification (7.27) to compute the space $S_k^B(\mathfrak{N})$ as in the direct approach of Section 4, with the appropriate modifications. Let $I_1, \ldots, I_H$ be a set of representatives for $\operatorname{Cl}\mathcal{O}$ such that $\operatorname{nrd}(I_i)$ is coprime to $\mathfrak{D}\mathfrak{N}$ for all i. Let $\widehat{\alpha}_i \in \widehat{\mathcal{O}}$ be such that $\widehat{\alpha}_i\widehat{\mathcal{O}} \cap \mathcal{O} = I_i$, and let $\Gamma_i = \mathcal{O}_L(I_i)^\times$. Then dualizing the isomorphism (7.27), we have

$$M_k^B(\mathfrak{N}) \cong \bigoplus_{i=1}^H W_k(\mathbb{C})^{\Gamma_i}.$$

The Hecke module structure on this space is defined similarly as in Section 4, as the following example illustrates.

Example 8.1. Consider the totally real quartic field $F = \mathbb{Q}(w)$ where $w^4 - 5w^2 - 2w + 1 = 0$. Then F has discriminant $5744 = 2^4 359$ and Galois group S_4. We have $\mathrm{Cl}^+ \mathbb{Z}_F = 2$ (but $\mathrm{Cl}\,\mathbb{Z}_F = 1$).

The quaternion algebra $B = \left(\dfrac{-1, -1}{F}\right)$ is unramified at all finite places (and ramified at all real places). We compute a maximal order $\mathcal{O}$ and find that $\#\,\mathrm{Cl}\,\mathcal{O} = 4$. We compute the action of the Hecke operators as in (3.8): we identify the isomorphism classes of the $N\mathfrak{p} + 1$ right ideals of norm $\mathfrak{p}$ inside each right ideal I in a set of representatives for $\mathrm{Cl}\,\mathcal{O}$. We compute, for example, that

$$T_{(w^3 - 4w - 1)} = \begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 0 & 4 & 4 \\ 2 & 2 & 0 & 0 \\ 3 & 3 & 0 & 0 \end{pmatrix}$$

where $N(w^3 - 4w - 1) = 4$; note this matrix has a block form, corresponding to the fact that $(w^3 - 4w - 1)$ represents the nontrivial class in $\mathrm{Cl}^+ \mathbb{Z}_F$. Correspondingly,

$$T_{(w^2 - w - 4)} = \begin{pmatrix} 6 & 2 & 0 & 0 \\ 8 & 12 & 0 & 0 \\ 0 & 0 & 8 & 4 \\ 0 & 0 & 6 & 10 \end{pmatrix}$$

with $N(w^2 - w - 4) = 13$ is a block scalar matrix, as $(w^2 - w - 4)$ is trivial in $\mathrm{Cl}^+ \mathbb{Z}_F$. In this case, the space $E_2(1)$ of functions that factor through the reduced norm has dimension $\dim E_2(1) = 2$, so $\dim S_2(1) = 2$, and we find that this space is irreducible as a Hecke module and so has a unique constituent f.

We obtain the following table of Hecke eigenvalues:

$\mathfrak{p}$	$(w^3 - 4w - 1)$	$(w - 1)$	$(w^2 - w - 2)$	$(w^2 - 3)$	$(w^2 - w - 4)$	$(w^2 - 2)$
$N\mathfrak{p}$	4	5	7	13	13	17
$a_\mathfrak{p}(f)$	0	t	$-2t$	$-t$	4	$3t$

Here t satisfies the polynomial $t^2 - 6 = 0$. As in Section 6, we predict the existence of an abelian variety over F with real multiplication by $\mathbb{Q}(\sqrt{6})$ and everywhere good reduction.

As in Section 4, the disadvantage of the approach used in Example 8.1 is that for each level $\mathfrak{N}$, one must compute the set of ideal classes $\mathrm{Cl}\,\mathcal{O} = \mathrm{Cl}\,\mathcal{O}_0(\mathfrak{N})$. By working with a more complicated coefficient module we can work with ideal classes only with the maximal order $\mathcal{O}_0(1)$, as follows.

Changing notation, now let $I_1, \ldots, I_h$ be representatives for $\mathrm{Cl}\,\mathcal{O}_0(1)$, with $h = \#\,\mathrm{Cl}\,\mathcal{O}_0(1)$, and let $I_i = \widehat{\alpha}_i \mathcal{O}_0(1) \cap B$. By strong approximation, we may assume that each $\mathrm{nrd}(I_i)$ is coprime to $\mathfrak{D}\mathfrak{N}$: indeed, we may assume each $\mathrm{nrd}(I_i)$ is supported in any set S of primes that generate $\mathrm{Cl}^+ \mathbb{Z}_F$. Let $\mathcal{O}_0(1)_i = \mathcal{O}_L(I_i) = \widehat{\alpha}_i \widehat{\mathcal{O}}_0(1) \widehat{\alpha}_i^{-1} \cap B$ be the left order of I_i. Then $\mathcal{O}_0(1)_i \otimes_{\mathbb{Z}_F} \mathbb{Z}_{F,\mathfrak{N}} \cong \mathcal{O}_0(1) \otimes_{\mathbb{Z}_F} \mathbb{Z}_{F,\mathfrak{N}}$.

Let $\widehat{\beta}_a$ for $a \in \mathbb{P}^1(\mathbb{Z}_F/\mathfrak{N})$ represent the $\mathcal{O}_0(1), \mathcal{O}$-connecting ideals of norm $\mathfrak{N}$: that is, $\widehat{\beta}_a \in \widehat{\mathcal{O}}_0(1)$ and if $J_a = \widehat{\mathcal{O}}_0(1)\widehat{\beta}_a \cap B$ then $\mathcal{O}_R(J_a) = \mathcal{O}$. Then the set $\{I_i J_a\}_{i,a}$, where $I_i J_a = \widehat{\alpha}_i \widehat{\beta}_a \widehat{\mathcal{O}} \cap B$, covers all isomorphism classes of right $\mathcal{O}$-ideals, but not necessarily uniquely: two such ideals $I_i J_a$ and $I_j J_b$ are isomorphic if and only if $i = j$ and there exists

$\gamma \in \mathcal{O}_0(1)_i^\times$ such that $\gamma J_a = J_b$, comparing the elements $\widehat{\alpha}_i \widehat{\beta}_a, \widehat{\alpha}_j \widehat{\beta}_b \in \widehat{\mathcal{O}}_0(1)$. The action of $\mathcal{O}_0(1)_i^\times$ can be equivalently given on the set of indices $a \in \mathbb{P}^1(\mathbb{Z}_F/\mathfrak{N})$: via the (reduction of a) splitting map

$$(8.2) \qquad \iota_{\mathfrak{N}} : \mathcal{O}_0(1) \hookrightarrow \mathcal{O}_0(1) \otimes_{\mathbb{Z}_F} \mathbb{Z}_{F,\mathfrak{N}} \cong \mathrm{M}_2(\mathbb{Z}_{F,\mathfrak{N}}),$$

each $\mathcal{O}_0(1)_i^\times$ acts on the left on $\mathbb{P}^1(\mathbb{Z}_F/\mathfrak{N})$, and we have $\widehat{\mathcal{O}}_0(1)_i^\times/\widehat{\mathcal{O}}_i^\times \xrightarrow{\sim} \mathbb{P}^1(\mathbb{Z}_F/\mathfrak{N})$.

We conclude that $M_k^B(\mathfrak{N}) \cong \mathcal{M}_k^B(\mathfrak{N}) = \bigoplus_{i=1}^h \mathcal{M}_k^B(\mathfrak{N})_i$, where

$$\mathcal{M}_k^B(\mathfrak{N})_i = \left\{ f : \mathbb{P}^1(\mathbb{Z}_F/\mathfrak{N}) \to W_k(\mathbb{C}) : f|_k \gamma = f \text{ for all } \gamma \in \mathcal{O}_0(1)_i^\times \right\}.$$

In this presentation, the Hecke operators act as follows. For a prime $\mathfrak{p}$, let

$$\Theta(\mathfrak{p})_{i,j} = \mathcal{O}_0(1)_i^\times \backslash \left\{ x \in I_i I_j^{-1} : \mathrm{nrd}(x I_i I_j^{-1}) = \mathfrak{p} \right\}.$$

We then define the linear map $T_\mathfrak{p} : \mathcal{M}_k^B(\mathfrak{N}) \to \mathcal{M}_k^B(\mathfrak{N})$ on each component by the rule

$$(T_\mathfrak{p})_{i,j} : \mathcal{M}_k^B(\mathfrak{N})_i \to \mathcal{M}_k^B(\mathfrak{N})_j$$

$$(8.3) \qquad f \mapsto \sum_{\gamma \in \Theta(\mathfrak{p})_{i,j}} f|_k \gamma.$$

This is indeed an isomorphism of Hecke modules. For further details, see work of the first author [15, Theorem 2] which traces these maps under the assumption that F has narrow class number one, but this assumption can be easily removed.

Put another way, by the decomposition

$$\widehat{B}^\times = \bigsqcup_{i=1}^h B^\times \widehat{\alpha}_i \widehat{\mathcal{O}}_0(1)^\times,$$

we decompose the set $X_0^B(\mathfrak{N})$ as

$$X_0^B(\mathfrak{N}) = B^\times \backslash \widehat{B}^\times / \widehat{\mathcal{O}}^\times = \bigsqcup_{i=1}^h B^\times \backslash \left(B^\times \widehat{\alpha}_i \widehat{\mathcal{O}}_0(1)^\times \right) / \widehat{\mathcal{O}}^\times \xrightarrow{\sim} \bigsqcup_{i=1}^h \mathcal{O}_0(1)_i^\times \backslash \widehat{\mathcal{O}}_0(1)_i^\times / \widehat{\mathcal{O}}_i^\times,$$

where the last identification is obtained by sending $\gamma \widehat{\alpha}_i u$ to $\widehat{\alpha}_i u \widehat{\alpha}_i^{-1}$. Thus, analogously to (7.17), we get a decomposition

$$(8.4) \qquad X_0^B(\mathfrak{N}) = \bigsqcup_{i=1}^h X_0^B(\mathfrak{N})_i = \bigsqcup_{i=1}^h \Gamma_i \backslash \mathbb{P}^1(\mathbb{Z}_F/\mathfrak{N}).$$

In particular, this gives $X_0^B(1) = \mathrm{Cl}\, \mathcal{O}_0(1)$. From this, we get an identification

$$(8.5) \qquad \begin{array}{c} M_k^B(\mathfrak{N}) \to \bigoplus_{i=1}^h \mathcal{M}_k^B(\mathfrak{N})_i \\ f \mapsto (f_i)_i, \end{array}$$

where we set $f_i(x) = f(\widehat{\alpha}\widehat{\alpha}_i)$ after choosing $\widehat{\alpha} \in \widehat{\mathcal{O}}_0(1)_i^\times$ such that $x = \widehat{\alpha} \cdot \infty_i$. Again, the decomposition (8.5) is analogous to (7.19), and one shows that it is a Hecke module isomorphism by arguing similarly.

Now $f \in M_k^B(\mathfrak{N})$ is by definition a map $f : \widehat{B}^\times / \widehat{\mathcal{O}}^\times \to W_k(\mathbb{C})$ such that $f|_k \gamma = f$ for all $\gamma \in B^\times$. Associated to such a map, via the identification (8.4), such a map is uniquely

defined by a tuple of maps $(f_i)_i$ with $f_i : \widehat{\mathcal{O}}_0(1)_i^\times / \widehat{\mathcal{O}}_i^\times \to W_k(\mathbb{C})$ such that $f \mid_k \gamma = f$ for all $\gamma \in \Gamma_i = \mathcal{O}_0(1)_i^\times$. In other words,

$$M_k^B(\mathfrak{N}) \xrightarrow{\sim} \bigoplus_{i=1}^{h} H^0(\Gamma_i, \operatorname{Hom}(\widehat{\mathcal{O}}_0(1)_i^\times / \widehat{\mathcal{O}}_i^\times, W_k(\mathbb{C}))) \cong \bigoplus_{i=1}^{h} H^0\big(\Gamma_i, \operatorname{Coind}_{\widehat{\mathcal{O}}_i^\times}^{\widehat{\mathcal{O}}_0(1)_i^\times} W_k(\mathbb{C})\big).$$

But then as in (8.2), we have

$$H^0\big(\Gamma_i, \operatorname{Coind}_{\widehat{\mathcal{O}}_i^\times}^{\widehat{\mathcal{O}}_0(1)_i^\times} W_k(\mathbb{C})\big) \cong \mathcal{M}_k^B(\mathfrak{N})_i.$$

Example 8.6. The real quadratic field $F = \mathbb{Q}(\sqrt{106})$ has strict class number 2 and class number 2. We compute that the space $S_2(1)$ of Hilbert cusp forms of level 1 and parallel weight 2 has dimension 50. It decomposes into four Hecke constituents of dimension 1, six of dimension 2, two of dimension 4 and one of dimension 26. The table below contains the first few Hecke eigenvalues of the one-dimensional constituents.

$\mathfrak{p}$	$(2, w)$	$(3, w+1)$	$(3, w-1)$	$(5, w+1)$	$(5, w-1)$	$(3w+31)$	$(3w-31)$
$N\mathfrak{p}$	2	3	3	5	5	7	7
$a_{\mathfrak{p}}(f_1)$	-1	-2	3	3	-2	4	-1
$a_{\mathfrak{p}}(f_2)$	-1	3	-2	-2	3	-1	4
$a_{\mathfrak{p}}(f_3)$	1	2	-3	-3	2	4	-1
$a_{\mathfrak{p}}(f_4)$	1	-3	2	2	-3	-1	4

The forms f_1 and f_2 (resp. f_3 and f_4) are interchanged by the action of $\operatorname{Gal}(F/\mathbb{Q})$ (on the ideals $\mathfrak{p}$). The forms f_1 and f_3 (resp. f_2 and f_4) are interchanged by the action of $\operatorname{Cl}^+ \mathbb{Z}_F$, so these forms are twists via the strict class character of $\operatorname{Gal}(F^+/F)$, where F^+ denotes the strict class field of F.

Elkies has found a curve E which gives rise to the above data:

$$E : y^2 - wxy - 2wy = x^3 + (-2 - 2w)x^2 + (-10809936 + 1049944w)$$
$$+ (-19477819120 + 1891853024w).$$

The curve E has j-invariant $j(E) = 264235 + 25777w$ and has everywhere good reduction. We conclude that E is modular using Kisin [42, Theorem 2.2.18] (see also Kisin [43, Theorem 3.5.5]): we need to verify that 3 is split in F, that E has no CM, and that the representation $\rho_3 : \operatorname{Gal}(\overline{F}/F) \to \operatorname{GL}_2(\mathbb{Z}_3)$ has surjective reduction $\overline{\rho}_3 : \operatorname{Gal}(\overline{F}/F) \to \operatorname{GL}_2(\mathbb{F}_3)$ which is solvable hence modular.

We find that E matches the form f_1; so its conjugate by $\operatorname{Gal}(F/\mathbb{Q})$ corresponds to f_2 and the quadratic twist of E by the fundamental unit $4005 - 389w$ (of norm -1) corresponds to f_3 (and its conjugate to f_4).

The input of our algorithm is a totally real number field F of degree n, a totally definite quaternion algebra B with discriminant $\mathfrak{D}$, an integral ideal $\mathfrak{N} \subseteq \mathbb{Z}_F$ which is coprime with $\mathfrak{D}$, a weight $k \in \mathbb{Z}^n$ such that $k_i \geq 2$ and $k_i \equiv k_j \pmod{2}$, and a prime $\mathfrak{p} \nmid \mathfrak{D}$. The output is then a matrix giving the action of $T_{\mathfrak{p}}$ in a basis of $M_k^B(\mathfrak{N}) = \bigoplus_{i=1}^{h} \mathcal{M}_k^B(\mathfrak{N})_i$ which is independent of $\mathfrak{p}$. By computing enough $T_{\mathfrak{p}}$ and simultaneously diagonalising, one obtains all Hecke constituents corresponding to Hilbert newforms of level $\mathfrak{N}$ and weight k.

The algorithm starts by finding a maximal order $\mathcal{O}_0(1)$, then computes a set of representatives $\mathrm{Cl}\,\mathcal{O}_0(1)$ of the right ideal classes of $\mathcal{O}_0(1)$ whose norms generate $\mathrm{Cl}^+(\mathbb{Z}_F)$ and are supported outside $\mathfrak{DN}$. This part of the algorithm uses work of the second author and Kirschmer [41], it is the most time consuming part but can be seen as a precomputation. Next, the algorithm finds a fundamental domain for the action of each Γ_i on $\mathbb{P}^1(\mathbb{Z}_F/\mathfrak{N})$, and computes $M_k^B(\mathfrak{N})$ as the direct sum of the

$$\mathcal{M}_k^B(\mathfrak{N})_i = \bigoplus_{[x]\in X_0^B(\mathfrak{N})_i} W_k(\mathbb{C})^{\Gamma_x},$$

where Γ_x is the stabilizer of x in Γ_i. From this, one obtains a basis of $M_k^B(\mathfrak{N})$. Finally, the algorithm computes the sets $\Theta(\mathfrak{p})_{i,j}$, and then the block matrices which give the action of $T_\mathfrak{p}$ in this basis. We refer to [15] and [18] for further details on the implementation.

9. Indefinite method, arbitrary class number

In this section, we generalize the indefinite method to arbitrary class number. We carry over the notation from Section 7, and now take the quaternion algebra B to be ramified at all but one real place.

In this case, from (7.17)–(7.18), the space $X(\mathbb{C}) = X_0^B(\mathfrak{N})(\mathbb{C}) = B_+^\times\backslash(\mathcal{H}\times\widehat{B}^\times/\widehat{\mathcal{O}}^\times)$ is the disjoint union of Riemann surfaces indexed by $\mathrm{Cl}^+\mathbb{Z}_F$. Let $\{\mathfrak{a}\}$ be a set of representatives for $\mathrm{Cl}^+\mathbb{Z}_F$ and let $\widehat{a}\in\widehat{\mathbb{Z}}_F$ be such that $\widehat{a}\widehat{\mathbb{Z}}_F\cap\mathbb{Z}_F = \mathfrak{a}$ for each $\mathfrak{a}$. Then

$$(9.1) \qquad X(\mathbb{C}) = \bigsqcup_{[\mathfrak{a}]\in\mathrm{Cl}^+(\mathbb{Z}_F)} \Gamma_\mathfrak{a}\backslash\mathcal{H} = \bigsqcup_{[\mathfrak{a}]\in\mathrm{Cl}^+(\mathbb{Z}_F)} X_\mathfrak{a}(\mathbb{C})$$

where $\mathcal{O}_\mathfrak{a} = \widehat{a}\widehat{\mathcal{O}}\widehat{a}^{-1}\cap B$ and $\Gamma_\mathfrak{a} = \mathcal{O}_{\mathfrak{a},+}^\times$.

Therefore, a modular form of weight k and level $\mathfrak{N}$ is a tuple $(f_\mathfrak{a})$ of functions $f_\mathfrak{a}: \mathcal{H}\to W_k(\mathbb{C})$, indexed by $[\mathfrak{a}]\in\mathrm{Cl}^+\mathbb{Z}_F$, such that for all $\mathfrak{a}$, we have

$$(f_\mathfrak{a}\,|_k\,\gamma)(z) = f_\mathfrak{a}(z)$$

for all $\gamma\in\Gamma_\mathfrak{a}$ and all $z\in\mathcal{H}$. In particular, if $k = (2,\ldots,2)$ is parallel weight 2, then $(f_\mathfrak{a})$ corresponds to a tuple of holomorphic 1-forms $((2\pi i)f_\mathfrak{a}(z)\,dz)_\mathfrak{a}$, one for each curve $X_\mathfrak{a}(\mathbb{C})$.

We compute with this space of functions by relating them to cohomology, and for that we must modify the coefficient module. Define the right $\mathrm{GL}_2(\mathbb{C})^n = \mathrm{GL}_2(\mathbb{C})\times\mathrm{GL}_2(\mathbb{C})^{n-1}$-module

$$V_k(\mathbb{C}) = \bigotimes_{i=1}^n P_{w_i}(m_i)(\mathbb{C}) = P_{w_1}(m_1)(\mathbb{C})\otimes W_k(\mathbb{C}).$$

The group $B^\times$ acts on $V_k(\mathbb{C})$ via the composite splitting $B^\times\hookrightarrow\mathrm{GL}_2(\mathbb{C})^n$ given by $\gamma\mapsto(\gamma_i)_i$. The Eichler-Shimura theorem, combined with the isomorphism (7.19), applied to each component $X_\mathfrak{a}(\mathbb{C})$ of $X(\mathbb{C})$ in (9.1), gives the isomorphism of Hecke modules

$$(9.2) \qquad S_k^B(\mathfrak{N}) \xrightarrow{\sim} \bigoplus_{[\mathfrak{a}]} H^1(\Gamma_\mathfrak{a}, V_k(\mathbb{C}))^+,$$

where $^+$ denotes the +1-eigenspace for complex conjugation.

In the description (9.2), the Hecke operators act on $\bigoplus H^1(\Gamma_\mathfrak{b}, V_k(\mathbb{C}))$ in the following way; we follow their definition in (7.24). Let $\mathfrak{p}$ be a prime ideal of $\mathbb{Z}_F$ with $\mathfrak{p}\nmid\mathfrak{DN}$. We consider

the [$\mathfrak{b}$]-summand, and given $f \in H^1(\Gamma_{\mathfrak{b}}, V_k(\mathbb{C}))$ we will define $T_{\mathfrak{p}}f \in H^1(\Gamma_{\mathfrak{a}}, V_k(\mathbb{C}))$, where $[\mathfrak{b}] = [\mathfrak{p}^{-1}\mathfrak{a}]$. Let $I_{\mathfrak{a}} = \widehat{\alpha}\widehat{\mathcal{O}} \cap B$ and $I_{\mathfrak{b}} = \widehat{\beta}\widehat{\mathcal{O}} \cap B$ so that $\mathrm{nrd}(I_{\mathfrak{b}}) = \mathfrak{b}$ and $\mathrm{nrd}(I_{\mathfrak{a}}) = \mathfrak{a}$, and let

$$\Theta(\mathfrak{p})_{\mathfrak{a},\mathfrak{b}} = \Gamma_{\mathfrak{b}} \backslash \left\{ \varpi \in B_+^{\times} \cap I_{\mathfrak{b}} I_{\mathfrak{a}}^{-1} : \mathrm{nrd}(I_{\mathfrak{b}} I_{\mathfrak{a}}^{-1})\mathfrak{p} = (\mathrm{nrd}(\varpi)) \right\}$$
$$= \Gamma_{\mathfrak{b}} \backslash \left\{ \varpi \in B_+^{\times} \cap I_{\mathfrak{b}} I_{\mathfrak{a}}^{-1} : \mathrm{nrd}(\varpi)\mathfrak{a} = \mathfrak{p}\mathfrak{b} \right\},$$

where $\Gamma_{\mathfrak{b}} = \mathcal{O}_{\mathfrak{b},+}^{\times}$ acts by multiplication on the left. Let $\gamma \in \Gamma_{\mathfrak{a}}$, so that $\gamma I_{\mathfrak{a}} = I_{\mathfrak{a}}$. Then the map $\varpi \mapsto \varpi\gamma$ on $B^{\times}$ induces a bijection (of the equivalence classes) of $\Theta(\mathfrak{p})_{\mathfrak{a},\mathfrak{b}}$. Therefore, for every $\varpi \in \Theta(\mathfrak{p})_{\mathfrak{a},\mathfrak{b}}$, there exists $\delta_{\varpi} \in \Gamma_{\mathfrak{a}}$ and $\varpi_{\gamma} \in \Theta(\mathfrak{p})_{\mathfrak{a},\mathfrak{b}}$ such that $\varpi\gamma = \delta_{\varpi}\varpi_{\gamma}$. From (7.22) and the Eichler-Shimura theorem, we have

$$(9.3) \qquad\qquad (T_{\mathfrak{p}}f)(\gamma) = \sum_{\varpi \in \Theta(\mathfrak{p})_{\mathfrak{a},\mathfrak{b}}} f(\delta_{\varpi})^{\varpi}.$$

One can similarly define the Atkin-Lehner involutions.

Admittedly, this description is complicated, but it can be summarized simply: a Hecke operator $T_{\mathfrak{p}}$ permutes the summands (9.2) in accordance with translation by $[\mathfrak{p}]$ in $\mathrm{Cl}^+ \mathbb{Z}_F$, and adjusting for this factor one can principalize as before (when the strict class number was 1). The resulting Hecke matrices are consequently block matrices.

We illustrate this with an example; we then give a few more details on the algorithm.

Example 9.4. Let $F = \mathbb{Q}(w)$ be the (totally real) cubic field of prime discriminant 257, with $w^3 - w^2 - 4w + 3 = 0$. Then F has Galois group S_3 and $\mathbb{Z}_F = \mathbb{Z}[w]$. The field F has class number 1 but strict class number 2: the unit $(w-1)(w-2)$ generates the group $\mathbb{Z}_{F,+}^{\times}/\mathbb{Z}_F^{\times 2}$ of totally positive units modulo squares.

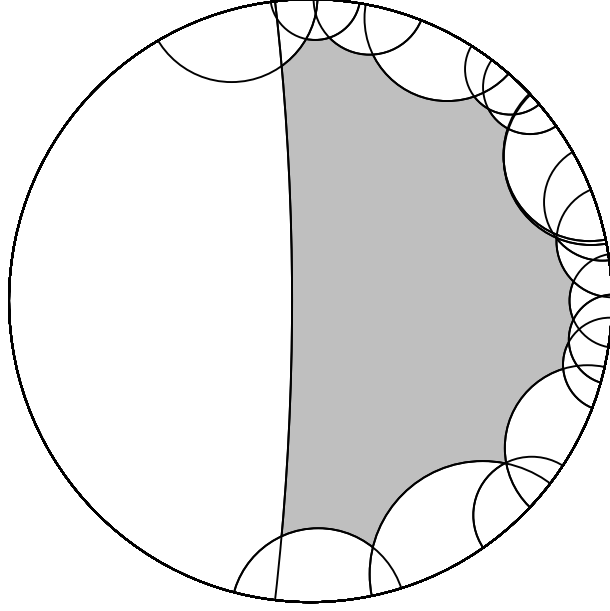Let $B = \left(\dfrac{-1, w-1}{F} \right)$ be the quaternion algebra with $i^2 = -1$, $j^2 = w-1$, and $ji = -ij$. Then B has discriminant $\mathfrak{D} = (1)$ and is ramified at two of the three real places and unramified at the place with $w \mapsto 2.19869\ldots$, corresponding to $\iota_{\infty} : B \hookrightarrow \mathrm{M}_2(\mathbb{R})$. The order

$$\mathcal{O} = \mathbb{Z}_F \oplus (w^2 + w - 3)i\mathbb{Z}_F \oplus ((w^2 + w) - 8i + j)/2\mathbb{Z}_F \oplus ((w^2 + w - 2)i + ij)/2\mathbb{Z}_F$$

is an Eichler order of level $\mathfrak{N} = (w)^2$ where $N(w) = 3$.

A fundamental domain for the action of $\Gamma = \iota_{\infty}(\mathcal{O}_+^{\times})$ on $\mathcal{H}$ is as follows.
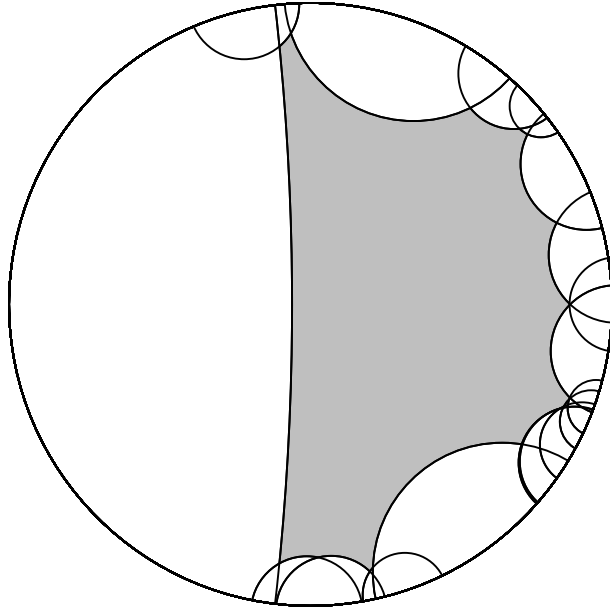
The ideals (1) and $\mathfrak{a} = (w+1)\mathbb{Z}_F$ represent the classes in the strict class group $\mathrm{Cl}^+ \mathbb{Z}_F$. The ideal $J_\mathfrak{a} = 2\mathcal{O} + ((w^2 + w + 2)/2 - 4i + (1/2)j)\,\mathcal{O}$ has $\mathrm{nrd}(J_\mathfrak{a}) = \mathfrak{a}$. The left order of $J_\mathfrak{a}$ is $\mathcal{O}_L(J_\mathfrak{a}) = \mathcal{O}_\mathfrak{a}$ where

$$\mathcal{O}_\mathfrak{a} = \mathbb{Z}_F \oplus (w^2 - 2w - 3)i\mathbb{Z}_F \oplus \big((w^2 + w)/2 - 4i + (1/2)j\big)\,\mathbb{Z}_F$$
$$\oplus\,(1/10)\big((174w^2 - 343w - 348)i + (w^2 - 2w - 2)j + (-w^2 + 2w + 2)ij\big)\,\mathbb{Z}_F.$$

A fundamental domain for the action of $\Gamma_\mathfrak{a} = \iota_\infty(\mathcal{O}_{\mathfrak{a},+}^\times)$ on $\mathcal{H}$ is as follows.

The orders $\mathcal{O}$ and $\mathcal{O}_\mathfrak{a}$ are not isomorphic since the connecting ideal $I_\mathfrak{a}$ (with left order $\mathcal{O}_\mathfrak{a}$ and right order $\mathcal{O}$) is not principal. This implies that the groups Γ and $\Gamma_\mathfrak{a}$ are not conjugate as subgroups of $\mathrm{PSL}_2(\mathbb{R})$ but nevertheless are isomorphic as abstract groups: they both have

signature $(1; 2, 2, 2, 2)$, so that
$$\Gamma \cong \Gamma_{\mathfrak{a}} \cong \langle \gamma, \gamma', \delta_1, \dots, \delta_4 : \delta_1^2 = \cdots = \delta_4^2 = [\gamma, \gamma']\delta_1 \cdots \delta_4 = 1 \rangle.$$

In particular, both $X_{(1)}(\mathbb{C})$ and $X_{\mathfrak{a}}(\mathbb{C})$ have genus 1, so
$$\dim H^1(X(\mathbb{C}), \mathbb{C}) = \dim H^1(X_{(1)}(\mathbb{C}), \mathbb{C}) + \dim H^1(X_{\mathfrak{a}}(\mathbb{C}), \mathbb{C}) = 4 = 2 \dim S_2(\mathfrak{N}).$$

We choose a basis of characteristic functions on γ, γ' as a basis for $H^1(X_{(1)}(\mathbb{C}), \mathbb{C})$ and similarly for $H^1(X_{\mathfrak{a}}(\mathbb{C}), \mathbb{C})$.

We now compute Hecke operators following the above. Let $H = H^1(X(\mathbb{C}), \mathbb{C})$. We compute that complex conjugation acts on H by the matrix

$$H \mid W_\infty = \begin{pmatrix} -1 & -1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}.$$

Note that W_∞ in this case preserves each factor. Now consider the Hecke operator $T_{\mathfrak{p}}$ where $\mathfrak{p} = (2w - 1)$ and $N(\mathfrak{p}) = 7$. Then $\mathfrak{p}$ represents the nontrivial class in $\mathrm{Cl}^+ \mathbb{Z}_F$. We compute that

$$H \mid T_{\mathfrak{p}} = \begin{pmatrix} 0 & 0 & -3 & 2 \\ 0 & 0 & -2 & -4 \\ -4 & -2 & 0 & 0 \\ 2 & -3 & 0 & 0 \end{pmatrix}$$

and restricting we get

$$H^+ \mid T_{\mathfrak{p}} = \begin{pmatrix} 0 & -2 \\ -8 & 0 \end{pmatrix}.$$

Therefore there are two eigenspaces for $T_{\mathfrak{p}}$ with eigenvalues $4, -4$. By contrast, the Hecke operator $T_{(2)}$ acts by the scalar matrix 3 on H, preserving each component.

Continuing in this way, we find the following table of eigenvalues:

$N\mathfrak{p}$	3	7	8	9	19	25	37	41	43	47	49	53	61	61	61
$a_{\mathfrak{p}}(f)$	-1	4	3	-4	-4	-8	4	-6	-8	0	4	12	-8	2	4
$a_{\mathfrak{p}}(g)$	-1	-4	3	4	-4	8	-4	-6	8	0	-4	-12	8	2	-4

Clearly, the form g is the quadratic twist of the form f by the nontrivial character of the strict class group $\mathrm{Gal}(F^+/F)$, where F^+ is the strict class field of F. Note also that these forms do not arise from base change from $\mathbb{Q}$, since $a_{\mathfrak{p}}$ has three different values for the primes $\mathfrak{p}$ of norm 61.

We are then led to search for elliptic curves of conductor $\mathfrak{N} = (w)^2$, and we find two:

$$E_f : y^2 + (w^2 + 1)xy = x^3 - x^2 + (-36w^2 + 51w - 18)x + (-158w^2 + 557w - 317)$$

$$E_g : y^2 + (w^2 + w + 1)xy + y = x^3 + (w^2 - w - 1)x^2 + (4w^2 + 11w - 11)x + (4w^2 + w - 3)$$

Each of these curves have nontrivial $\mathbb{Z}/2\mathbb{Z}$-torsion over F, so as above they are modular and we match Hecke eigenvalues to find that E_f corresponds to f and E_g corresponds to g.

In this situation, although by the theory of canonical models due to Deligne we know that the variety $X(\mathbb{C}) = X_{(1)}(\mathbb{C}) \sqcup X_{\mathfrak{a}}(\mathbb{C})$ has a model X_F over F, the curves themselves are not defined over F—they are interchanged by the action of $\mathrm{Gal}(F^+/F)$. Nevertheless, the

Jacobian of X_F is an abelian variety of dimension 2 defined over F which is isogenous to $E_f \times E_g$—we characterize in this way isogeny classes, not isomorphism classes.

As in the case of class number 1, the application of Shapiro's lemma allows us always to work with the group associated to a maximal order, as follows. Let $\mathcal{O}_0(1) \supseteq \mathcal{O}$ be a maximal order containing $\mathcal{O}$, and for each ideal $\mathfrak{a}$, let $\mathcal{O}_0(1)_{\mathfrak{a}} = \widehat{\alpha}\widehat{\mathcal{O}}_0(1)\widehat{\alpha}^{-1} \cap B$ be the maximal order containing $\mathcal{O}_{\mathfrak{a}}$, and let $\Gamma(1)_{\mathfrak{a}} = \iota_\infty(\mathcal{O}_+^\times)$. Further, define

$$V_k(\mathbb{C})_{\mathfrak{a}} = \mathrm{Coind}_{\Gamma_{\mathfrak{a}}}^{\Gamma(1)_{\mathfrak{a}}} V_k(\mathbb{C})$$

for each $\mathfrak{a}$. Then Shapiro's lemma implies that

$$H^1(\Gamma_{\mathfrak{a}}, V_k(\mathbb{C})) \cong H^1(\Gamma(1)_{\mathfrak{a}}, V_k(\mathbb{C})_{\mathfrak{a}})$$

and so

$$S_k^B(\mathfrak{N}) \xrightarrow{\sim} \bigoplus_{[\mathfrak{a}]} H^1(\Gamma(1)_{\mathfrak{a}}, V_k(\mathbb{C})_{\mathfrak{a}})^+.$$

Our algorithm takes as input a totally real field F of degree $[F : \mathbb{Q}] = n$, a quaternion algebra B over F split at a unique real place, an ideal $\mathfrak{N} \subset \mathbb{Z}_F$ coprime to the discriminant $\mathfrak{D}$ of B, a vector $k \in (2\mathbb{Z}_{>0})^n$, and a prime $\mathfrak{p} \nmid \mathfrak{DN}$, and outputs the matrix of the Hecke operator $T_{\mathfrak{p}}$ acting on the space $H = \bigoplus_{\mathfrak{b}} H^1(\Gamma(1)_{\mathfrak{b}}, V_k(\mathbb{C})_{\mathfrak{b}})^+$ with respect to some fixed basis which does not depend on $\mathfrak{p}$. From these matrices, we decompose the space H into Hecke-irreducible subspaces by linear algebra. We give a short overview of this algorithm.

First, some precomputation. We precompute a set of representatives $[\mathfrak{a}]$ for the strict class group $\mathrm{Cl}^+ \mathbb{Z}_F$ with each $\mathfrak{a}$ coprime to $\mathfrak{pDN}$. For each representative ideal $\mathfrak{a}$, precompute a right $\mathcal{O}_0(1)$-ideal $I_{\mathfrak{a}}$ such that $\mathrm{nrd}(I_{\mathfrak{a}}) = \mathfrak{a}$ and let $\mathcal{O}_0(1)_{\mathfrak{a}} = \mathcal{O}_L(I_{\mathfrak{a}})$ be the left order of $I_{\mathfrak{a}}$. Next, we compute for each $\mathfrak{a}$ a finite presentation for $\Gamma(1)_{\mathfrak{a}}$ consisting of a (minimal) set of generators $G_{\mathfrak{a}}$ and relations $R_{\mathfrak{a}}$ together with a solution to the word problem for the computed presentation [69]. Then using standard linear algebra techniques, we compute a basis for the space $\bigoplus_{[\mathfrak{a}]} H^1(\Gamma(1)_{\mathfrak{a}}, V_k(\mathbb{C})_{\mathfrak{a}})$.

The main issue then is to make the description (9.3) amenable to explicit computation. First, compute a splitting $\iota_{\mathfrak{p}} : \mathcal{O}_0(1) \hookrightarrow \mathrm{M}_2(\mathbb{Z}_{F,\mathfrak{p}})$. Then for each ideal $\mathfrak{a}$, perform the following steps.

First, compute the ideal $\mathfrak{b}$ with ideal class $[\mathfrak{b}] = [\mathfrak{p}^{-1}\mathfrak{a}]$. Compute the left ideals

$$J_a = \mathcal{O}_a \iota_{\mathfrak{p}}^{-1} \begin{pmatrix} x & y \\ 0 & 0 \end{pmatrix} + \mathcal{O}_a \mathfrak{p}$$

indexed by the elements $a = (x : y) \in \mathbb{P}^1(\mathbb{F}_{\mathfrak{p}})$. Then compute the left $\mathcal{O}_{\mathfrak{b}}$-ideals $I_{\mathfrak{b}} I_{\mathfrak{a}}^{-1} J_a$ and compute totally positive generators $\varpi_a \in \mathcal{O}_{\mathfrak{a}} \cap B_+^\times$ corresponding to $\mathcal{O}_{\mathfrak{b}} \varpi_a = I_{\mathfrak{b}} I_{\mathfrak{a}}^{-1} J_a$ [41].

Now, for each γ in a set of generators $G_{\mathfrak{a}}$ for $\Gamma_{\mathfrak{a}}$, compute the permutation γ^* of $\mathbb{P}^1(\mathbb{F}_{\mathfrak{p}})$ [30, Algorithm 5.8] and then the elements $\delta_a = \varpi_a \gamma \varpi_{\gamma^* a}^{-1}$ for $a \in \mathbb{P}^1(\mathbb{F}_{\mathfrak{p}})$; write each such element δ_a as a word in $G_{\mathfrak{b}}$ and then apply the formula

$$(T_{\mathfrak{p}} f_{\mathfrak{a}})(\gamma) = \sum_{a \in \mathbb{P}^1(\mathbb{F}_{\mathfrak{p}})} f_{\mathfrak{b}}(\delta_a)^{\varpi_a}.$$

The algorithm in its full detail is rather complicated to describe; we refer the reader to work of the second author [71] for the details.

References

[1] Don Blasius, *Elliptic curves, Hilbert modular forms, and the Hodge conjecture*, Contributions to automorphic forms, geometry, and number theory, Johns Hopkins Univ. Press, Baltimore, 2004, 83–103.

[2] Don Blasius and Jonathan Rogawski, *Galois representations for Hilbert modular forms.* Bull. Amer. Math. Soc. (N.S.) **21** (1989), no. 1, 65–69.

[3] Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), vol. 3–4, 235–265.

[4] A. Brumer, *The rank of $J_0(N)$*, Astérisque **228** (1995), 41–68.

[5] Kevin Buzzard, Fred Diamond and Frazer Jarvis, *On Serre's conjecture for mod ℓ Galois representations over totally real fields*, preprint, `arXiv:0810.2106v2`.

[6] Henri Carayol, *Sur les représentations l-adiques associées aux formes modulaires de Hilbert.* Ann. Sci. École Norm. Sup. (4) **19** (1986), no. 3, 409–468.

[7] Henri Cohen, *A course in computational algebraic number theory*, Graduate Texts in Math., vol. 138, Springer-Verlag, Berlin, 1993.

[8] John Cremona, *Modular symbols for $\Gamma_1(N)$ and elliptic curves with everywhere good reduction*, Math. Proc. Cambridge Philos. Soc. **111** (1992), no. 2, 199–218.

[9] John Cremona, *Algorithms for modular elliptic curves*, 2nd ed., Cambridge University Press, Cambridge, 1997, available at `http://www.maths.nott.ac.uk/personal/jec/book/`.

[10] John Cremona and Mark Lingham, *Finding all elliptic curves with good reduction outside a given set of primes*, Exp. Math. **16** (2007), no. 3, 303–312.

[11] Henri Darmon, *Rational points on modular elliptic curves*, CBMS Series in Math., vol. 101, Amer. Math. Soc., Providence, RI, 2004.

[12] Pierre Deligne, *Travaux de Shimura*, Séminaire Bourbaki, Lecture Notes in Math. **244**, no. 389, 123–165.

[13] Pierre Deligne, *Formes modulaires et représentations l-adiques*, Séminaire Bourbaki, vol. 1968/1969, Exposé no. 355, Lecture Notes in Math. **179**, Springer, 1971, p. 139-172).

[14] Lassina Dembélé, *Explicit computations of Hilbert modular forms on $\mathbb{Q}(\sqrt{5})$*, Experiment. Math. **14** (2005), no. 4, 457–466.

[15] Lassina Dembélé, *Quaternionic Manin symbols, Brandt matrices and Hilbert modular forms*, Math. Comp. **76** (2007), no. 258, 1039–1057.

[16] Lassina Dembélé, *A non-solvable Galois extension of $\mathbb{Q}$ ramified at 2 only*, C. R. Acad. Sci. Paris, Ser. I, **347** (2009), 111–116.

[17] Lassina Dembélé, Matthew Greenberg, and John Voight, *Nonsolvable number fields ramified only at 3 and 5*, to appear in Compositio Math.

[18] Lassina Dembélé and Steve Donnelly, *Computing Hilbert modular forms over fields with nontrivial class group*, Algorithmic number theory (Banff, 2008), Lecture Notes in Comput. Sci., vol. 5011, Springer, Berlin, 2008, 371–386.

[19] Fred Diamond and Jerry Shurman, *A first course in modular forms*, Graduate Texts in Math., vol. 228, Springer-Verlag, New York, 2005.

[20] Luis V. Dieulefait, *A non-solvable extension of $\mathbb{Q}$ unramified outside 7*, preprint, `arxiv:1005.4209`.

[21] Steve Donnelly and John Voight, *Tables of Hilbert modular forms and elliptic curves over totally real fields*, in preparation.

[22] Martin Eichler, *On theta functions of real algebraic number fields*, Acta Arith. **33** (1977), no. 3, 269–292.

[23] Martin Eichler, *The basis problem for modular forms and the traces of the Hecke operators*, Modular functions of one variable, I (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972), Lecture Notes in Math., vol. 320, Springer, Berlin, 1973, 75–151.

[24] Martin Eichler, *Correction to: "The basis problem for modular forms and the traces of the Hecke operators"*, Modular functions of one variable, IV (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972), Lecture Notes in Math., vol. 476, Springer, Berlin, 1975, 145–147.

[25] Eberhard Freitag, *Hilbert modular forms*, Springer-Verlag, Berlin, 1990.

[26] Gerard van der Geer, *Hilbert modular surfaces*, Springer-Verlag, Berlin, 1988.

[27] Stephen Gelbart and Hervé Jacquet, *Forms of GL(2) from the analytic point of view*, Automorphic forms, representations and L-functions (Corvallis, OR, 1977), vol. 1, eds. A. Borel and W. Casselman, Proc. Sympos. Pure Math. **33**, Amer. Math. Soc., Providence, RI, 1979, 213–251.

[28] David Geraghty, *Modularity lifting theorems for ordinary Galois representations*, preprint, http://www.math.harvard.edu/~geraghty/oml.pdf.

[29] Eyal Z. Goren, *Lectures on Hilbert modular varieties and modular forms*, CRM Monograph Series, vol. 14, Amer. Math. Soc. Providence, RI, 2002.

[30] Matt Greenberg and John Voight, *Computing systems of Hecke eigenvalues associated to Hilbert modular forms*, to appear in Math. Comp.

[31] Ki-ichiro Hashimoto, *On Brumer's family of RM-curves of genus two*, Tohoku Math. J. (2), **52** (2000), no. 4, 475–488.

[32] Haruzo Hida, *On p-adic Hecke algebras for* GL_2 *over totally real fields*, Ann. of Math. (2) **128** (1988), no. 2, 295–384.

[33] Haruzo Hida, *On abelian varieties with complex multiplication as factors of the Jacobians of Shimura curves*, Amer. J. of Math. **103** (1981), no. 4, 727–776.

[34] Haruzo Hida, *Hilbert modular forms and Iwasawa theory*, Oxford Sci. Publ., Oxford, 2006.

[35] Hiroaki Hijikata, *Explicit formula of the traces of Hecke operators for* $\Gamma_0(N)$, J. Math. Soc. Japan **26** (1974), no. 1, 56–82.

[36] Hervé Jacquet and Robert P. Langlands, *Automorphic forms on GL(2)*, Lectures Notes in Math., vol. 114, Springer-Verlag, Berlin, 1970.

[37] Frazer Jarvis, *Mazur's principle for totally real fields of odd degree.* Compositio Math. **116** (1999), no. 1, 39–79,

[38] Anthony W. Knapp, *Elliptic curves*, Math. Notes, vol. 40, Princeton Univ. Press, Princeton, 1992.

[39] Chandrashekhar Khare and Jean-Pierre Wintenberger, *On Serre's conjecture for* 2-*dimensional* mod p *representations of the absolute Galois group of the rationals*, to appear in Ann. of Math.

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

[41] Markus Kirschmer and John Voight, *Algorithmic enumeration of ideal classes for quaternion orders*, SIAM J. Comput. (SICOMP) **39** (2010), no. 5, 1714–1747.

[42] Mark Kisin, *The Fontaine-Mazur conjecture for* GL_2, J. Amer. Math. Soc. **22** (2009), no. 3, 641–690.

[43] Mark Kisin, *Moduli of finite flat group schemes, and modularity*, Ann. of Math. (2) **170** (2009), no. 3, 1085–1180.

[44] Koopa Tak-Lun Koo, William Stein, and Gabor Wiese, *On the generation of the coefficient field of a newform by a single Hecke eigenvalue*, J. Théorie Nombres Bordeaux **20** (2008), no. 2, 373–384.

[45] David Kohel, *Hecke module structure of quaternions*, Class field theory: its centenary and prospect (Tokyo, 1998), ed. K. Miyake, Adv. Stud. Pure Math., vol. 30, Math. Soc. Japan, Tokyo, 2001, 177–195.

[46] B. Mazur and J. Tate, *Points of order* 13 *on elliptic curves*, Invent. Math. **22** (1973/74), 41–49.

[47] Barry Mazur and Andrew Wiles, *Class fields of abelian extensions of* $\mathbb{Q}$, Invent. Math. **76** (1984), 179–330.

[48] Jean-Francois Mestre, *La méthode des graphes: exemples et applications*, Proceedings of the international conference on class numbers and fundamental units of algebraic number fields (Katata), Nagoya Univ., Nagoya, 1986, 217–242.

[49] A. P. Ogg, *Rational points on certain elliptic modular curves*, Analytic number theory, Proc. Sympos. Pure Math., Vol. XXIV, Amer. Math. Soc., Providence, RI, 1973, 221–231.

[50] Arnold Pizer, *An algorithm for computing modular forms on* $\Gamma_0(N)$, J. Algebra **64** (1980), vol. 2, 340–390.

[51] Boyd B. Roberts; Lawrence C. Washington, *The modularity of some* $\mathbb{Q}$-*curves*, Compositio Math. **111** (1998), no. 1, 35–49.

[52] David P. Roberts, *Nonsolvable polynomials with field discriminant* 5^A, preprint, http://cda.morris.umn.edu/~roberts/research/five.pdf.

[53] Takeshi Saito, *Hilbert modular forms and p-adic Hodge theory.* Compos. Math. **145** (2009), no. 5, 1081–1113.

[54] René Schoof, *Abelian varieties over cyclotomic fields with good reduction everywhere*, Math. Ann. **325** (2003), no. 3, 413–448.

[55] Jean-Pierre Serre, *Congruences et formes modulaires [d'après H. P. F. Swinnerton-Dyer]*, Séminaire Bourbaki, 24e année (1971/1972), exp. no. 416, *Lecture Notes in Math.*, vol. 317, Springer, Berlin, 1973, 319–338.

[56] Jean-Pierre Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), no. 4, 259–331.

[57] Jean-Pierre Serre, *Abelian ℓ-adic representations and elliptic curves*, Research Notes in Mathematics, vol. 7, Wellesley, MA, A.K. Peters, 1997.

[58] N.I. Shepherd-Barron and R. Taylor, mod2 *and* mod5 *icosahedral representations*, J. Amer. Math. Soc. **10** (1997), no. 2, 283–298.

[59] Goro Shimura, *Construction of class fields and zeta functions of algebraic curves*, Ann. of Math. (2) **85** (1967), 58–159.

[60] Goro Shimura, *The special values of the zeta functions associated with Hilbert modular forms*, Duke Math. J. **45** (1978), no. 3, 637–679.

[61] Goro Shimura, *Introduction to the arithmetic theory of automorphic functions*, Publ. Math. Soc. Japan, vol. 11, Princeton Univ. Press, Princeton, 1994.

[62] Jude Socrates and David Whitehouse, *Unramified Hilbert modular forms, with examples relating to elliptic curves*, Pacific J. Math. **219** (2005), no. 2, 333–364.

[63] C. M. Skinner and Andrew J. Wiles, *Nearly ordinary deformations of irreducible residual representations*, Ann. Fac. Sci. Toulouse Math. (6), **10** (2001), no. 1, 185–215.

[64] C. M. Skinner and Andrew J. Wiles, *Residually reducible representations and modular forms*, Inst. Hautes études Sci. Publ. Math. **89** (1999), 5–126.

[65] Andrew Snowden, *On two dimensional weight two odd representations of totally real fields*, preprint, `arXiv:0905.4266`.

[66] William Stein, *Modular forms, a computational approach*, with an appendix by Paul E. Gunnells, Graduate Studies in Math., vol. 79, Amer. Math. Soc., Providence, 2007.

[67] Richard Taylor, *On Galois representations associated to Hilbert modular forms*, Invent. Math, **98** (1989), no. 2, 265–280.

[68] Marie-France Vignéras, *Arithmétique des algèbres de quaternions*, Lecture notes in mathematics, vol. 800, Springer, Berlin, 1980.

[69] John Voight, *Computing fundamental domains for Fuchsian groups*, J. Théorie Nombres Bordeaux (2009), no. 2, 467–489.

[70] John Voight, *Shimura curve computations*, Arithmetic Geometry, Clay Math. Proc., vol. 8, Amer. Math. Soc., Providence, 2009, 103–113.

[71] John Voight, *Computing automorphic forms on Shimura curves over fields with arbitrary class number*, Algorithmic number theory (ANTS IX, Nancy, France, 2010), eds. Guillaume Hanrot, Francois Morain, and Emmanuel Thomé, Lecture Notes in Comp. Sci., vol. 6197, Springer, Berlin, 2010, 357–371.

[72] John Voight, *Identifying the matrix ring: algorithms for quaternion algebras and quadratic forms*, preprint, `arXiv:1004.0994`.

[73] Andrew Wiles, *Modular elliptic curves and Fermat's Last Theorem*, Ann. of Math. (2) **141** (1995), no. 3, 443–551.

[74] Andrew Wiles, *On ordinary λ-adic representations associated to modular forms*, Invent. Math. **94** (1988), no. 3, 529–573.

[75] John Wilson, *Explicit moduli for curves of genus 2 with real multiplication by $\mathbb{Q}(\sqrt{5})$*, Acta Arith. **93** (2000), no. 2, 121–138.

[76] Shou-Wu Zhang, *Heights of Heegner points on Shimura curves*, Ann. of Math. (2) **153** (2001), no. 1, 27–147.

Warwick Mathematics Institute, University of Warwick, Coventry CV4 7AL, UK

Email address: lassina.dembele@gmail.com

Department of Mathematics and Statistics, University of Vermont, 16 Colchester Ave, Burlington, VT 05401, USA

Email address: jvoight@gmail.com