Advanced Studies in Pure Mathematics 30, 2001
Class Field Theory – Its Centenary and Prospect
pp. 177–195

Hecke Module Structure of Quaternions

David R. Kohel

Abstract.

The arithmetic of quaternions is recalled from a constructive point of view. A Hecke module is introduced, defined as a free abelian group on right ideal classes of a quaternion order, together with a natural action of Hecke operators. An equivalent construction in terms of Shimura curves is then introduced, and the quaternion construction is applied to the analysis of specific modular and Shimura curves.

§1. Introduction

The arithmetic of quaternion algebras underlies a number of areas of modern mathematics, from number theory and algebraic geometry to graph theory. A motivation for the present article, in particular, is the interplay with the arithmetic of Shimura curves. Thus in this article we present the arithmetic of quaternion algebras and describe the construction of the associated Hecke modules. Then we discuss the geometric relation with modular curves and Shimura curves and conclude with some calculations. In order to motivate what follows we begin here with an overview of the algebraic and geometric facets of the theory.

The Hecke modules of this study are defined alternatively as divisor groups on right ideal classes of a level m order $\mathcal{O}$ for a definite quaternion algebra of discriminant Dp, or as the monodromy group at p of a Néron model for the Jacobian of a Shimura curve $X_0^D(mp)$. The curve $X_0^D(mp)$ parameterizes abelian surfaces whose endomorphism rings admit a fixed embedding of a level mp order R in an indefinite quaternion algebra of discriminant D. The supersingular points of reduction modulo p correspond, by definition, to those abelian surfaces which split into a product of supersingular elliptic curves. By results of Buzzard [2], the singular points of the reduction modulo p are the supersingular points.

Received September 22, 1998.
Revised December 11, 1998.

The monodromy group, measuring winding numbers about these points, can be identified with the supersingular divisor group. The enhanced supersingular surfaces are functorially equivalent to the right ideals over the quaternion order $\mathcal{O}$. Moreover the Hecke operators, as with classical modular curves, are determined by the morphisms in the supersingular category. Thus the monodromy group can be formally replaced with a free abelian group on a basis of right ideals classes for $\mathcal{O}$, allowing one to work with a Hecke module of quaternions as a proxy for the supersingular divisor subgroup.

This paper is organized as follows. Section 2 contains the background machinery for quaternion algebras from a constructive point of view, with explicit examples given. In Section 3 we define Hecke modules in terms of supersingular elliptic curves as in Mestre [10] and its generalization in terms of quaternions. Section 4 recalls the definition of Shimura curves as well as relevant theorems which establish the connection with the quaternion algebras. The final section is devoted to the analysis of specific Shimura curves using the corresponding Hecke modules. By demonstration, we show that the arithmetic of quaternion algebras is effective for computation, in contrast to the difficulty of computing Shimura curves and their Jacobians (see Elkies [6]). Moreover, by means of the geometric interpretation, Hecke modules of quaternions provide a means of elucidating the theory of Shimura curves.

§2. Quaternion algebras

A finite dimensional algebra H over a field K is *simple* if it has no proper, nontrivial left or right ideals. If the center of H is K, then H is said to be *central* over K. With these prior definitions, we make the following definition of a quaternion algebra.

Definition 2.1. A quaternion algebra H over K is a central simple algebra of dimension four over K.

Since K is the center of H, it is clear that H must be a noncommutative ring. Throughout this work, the field K will be $\mathbb{Q}$ or one of its completions $\mathbb{Q}_p$ or $\mathbb{R}$.

Quaternion algebras are the simplest of noncommutative rings, and in this realm, are the analogues of quadratic field extensions. As in the case of number fields, the principle questions of arithmetic interest regard the orders in a quaternion algebra and the left and right ideal theory of such orders.

Example 2.2. The following three algebras are examples of quaternion algebras over $\mathbb{Q}$.

1. The matrix algebra $\mathbb{M}_2(\mathbb{Q})$ is the *split* quaternion algebra over $\mathbb{Q}$.
2. The $\mathbb{Q}$-algebra defined by generators i and j with relations
$$i^2 = j^2 = -1,$$
$$ij + ji = 0.$$
3. The $\mathbb{Q}$-algebra defined by generators x and y with relations
$$x^2 + 2 = y^2 + y + 5 = 0,$$
$$xy + yx + x + 1 = 0.$$

2.1. Trace, norm, and involutions

Let H be a quaternion algebra over K. Every x in H is contained in a quadratic extension of K. Conversely every maximal commutative extension of K in H is quadratic. It follows that every x in H satisfies an equation
$$x^2 - \mathrm{Tr}(x)x + \mathrm{Nr}(x) = 0,$$
where $\mathrm{Tr}(x)$ and $\mathrm{Nr}(x)$ are elements of K which we call the *reduced trace* and *reduced norm* respectively. The *conjugate* of x is defined to be the element
$$\overline{x} = \mathrm{Tr}(x) - x,$$
and $x \mapsto \overline{x}$ is an involution of H.

Now suppose that $K = \mathbb{Q}$. We define an *order* in H to be a subring which is a $\mathbb{Z}$-module of rank four. Let R be any such order, let $\{x_1, x_2, x_3, x_4\}$ be a basis, and set
$$\langle x, y \rangle = \mathrm{Nr}(x + y) - \mathrm{Nr}(x) - \mathrm{Nr}(y).$$
Then the determinant of the matrix $\left(\langle x_i, x_j \rangle\right)$ is the square of an integer. We define the *discriminant* of R to the positive integer $\mathrm{disc}(R)$ such that
$$\det\left(\langle x_i, x_j \rangle\right) = \mathrm{disc}(R)^2.$$
The discriminant of H is defined to be the discriminant of a maximal order in H, which is well-defined by Theorem 2.6 below.

2.2. Completions, ramification, and splitting

Let $M_{\mathbb{Q}}$ denote the set of finite and infinite places of $\mathbb{Q}$. For each place v in $M_{\mathbb{Q}}$, we define
$$H_v = H \otimes_{\mathbb{Q}} \mathbb{Q}_v \cong \begin{cases} \mathbb{M}_2(\mathbb{Q}_v) \text{ or} \\ \mathcal{D}_v \end{cases}$$

where $\mathcal{D}_v$ is the unique central division algebra of dimension 4 over $\mathbb{Q}_v$. In the former case v is said to *split* in H and in the latter v is said to *ramify*. Quaternion algebras can be classified in terms of their ramification by means of the Brauer group.

The Brauer group $\mathrm{Br}(K)$ of a field K is an abelian group defined on a set of classes $[A]$ of central simple K-algebras A. The equivalence relation is defined such that $[A] = [B]$ if and only if

$$A \otimes_K \mathbb{M}_r(K) \cong B \otimes_K \mathbb{M}_s(K),$$

for positive integers r and s. The group operation in $\mathrm{Br}(K)$ is the tensor product, and for any central division algebra, the *opposite algebra* lies in the inverse class of the Brauer group.

By the Wedderburn theorem every central simple K-algebra is isomorphic to an algebra of the form $\mathbb{M}_n(\mathcal{D})$ for a unique central division algebra $\mathcal{D}/K$ and positive integer n. It follows that the classes in $\mathrm{Br}(K)$ are in bijection with the isomorphism classes of central division algebras. From the description of the inverse operation, it follows that the 2-torsion subgroup $\mathrm{Br}(K)[2]$ is in bijection with the isomorphism classes of central division algebras with involution.

Theorem 2.3. *The Hasse invariant defines canonical isomorphisms*

$$\text{(i) } \mathrm{inv}_p : \mathrm{Br}(\mathbb{Q}_p) \longrightarrow \mathbb{Q}/\mathbb{Z} \qquad \text{(ii) } \mathrm{inv}_\infty : \mathrm{Br}(\mathbb{R}) \longrightarrow \frac{1}{2}\mathbb{Z}/\mathbb{Z}$$

for all finite places p and the infinite place, respectively, such that the sequence

$$0 \longrightarrow \mathrm{Br}(\mathbb{Q}) \xrightarrow{\iota} \bigoplus_{v \in M_{\mathbb{Q}}} \mathrm{Br}(\mathbb{Q}_v) \xrightarrow{\mathrm{inv}} \mathbb{Q}/\mathbb{Z} \longrightarrow 0,$$

defined by $\iota([A]) = ([A \otimes Q_v])_v$ and $\mathrm{inv}(([A_v])_v) = \sum_v \mathrm{inv}_v(A_v)$, is exact.

In fact the 2-torsion group $\mathrm{Br}(\mathbb{Q})[2]$ has representatives among the quaternion algebras over $\mathbb{Q}$, giving the following classification theorem (see Vignéras [20] II.3 Theorem 3.1).

Theorem 2.4. *Every quaternion algebra over $\mathbb{Q}$ ramifies at an even number of places. Conversely for every finite set consisting of an even number of places of $\mathbb{Q}$, there exists a unique quaternion algebra $H/\mathbb{Q}$ ramifying at exactly this set.*

Example 2.5. As noted, the quaternion algebras lie in the 2-torsion subgroup of the Brauer group. From Theorem 2.3 and 2.4 we note that in particular that there exists a unique quaternion division algebra over $\mathbb{R}$. This algebra is the classical *Hamilton* quaternions

$$\mathbb{H} = \mathbb{R} + \mathbb{R}i + \mathbb{R}j + \mathbb{R}k,$$

where $i^2 = j^2 = -1$ and $k = ij = -ji$.

If a quaternion algebra ramifies at infinity, we say that it is *positive definite*, otherwise we say it is *indefinite*. It follows that a quaternion algebra is positive definite if and only if it embeds in the Hamilton quaternion algebra.

The following theorem, together with the definition of the discriminant, serves to determine the primes ramifying in a quaternion algebra H.

Theorem 2.6. *Let H be a quaternion algebra over $\mathbb{Q}$. The discriminant of an order R in H is $m\,\mathrm{disc}(\mathcal{O})$, where $\mathcal{O}$ is any maximal order containing R and m is the index $[\mathcal{O} : R]$. The discriminant of $\mathcal{O}$ is equal to the product of the finite primes ramifying in H.*

Proof. This is the content of Vignéras [20], Chapitre I, Lemme 4.7 and Chapitre III, Corollaire 5.3 and the discussion following. □

Example 2.7. In Example 2.2 we see that by definition the *split* quaternion algebra (1) ramifies nowhere. The discriminant of the order $R = \mathbb{Z}\langle i, j\rangle$ of the quaternion algebra (2) is 4, so has index two in a maximal order in the algebra ramified at 2 and ∞. The order generated by x and y in the algebra (3) is maximal. Indeed for the basis $\{x_1, x_2, x_3, x_4\} = \{1, x, y, xy\}$ we have

$$\big(\langle x_i, x_j\rangle\big) = \begin{bmatrix} 2 & 0 & -1 & -1 \\ 0 & 4 & 1 & -2 \\ -1 & 1 & 10 & 0 \\ -1 & -2 & 0 & 20 \end{bmatrix},$$

which has determinant 37^2. Therefore R is maximal and the algebra ramifies at 37 and ∞.

2.3. Orders and ideals

An order in a finite dimensional algebra $H/\mathbb{Q}$ is a subring containing a basis for H and which is finitely generated as a $\mathbb{Z}$-module. In number fields there exists a unique maximal order. For noncommutative algebras this uniqueness property fails. In the split quaternion algebra

$\mathbb{M}_2(\mathbb{Q})$ for example, the order $\mathbb{M}_2(\mathbb{Z})$ is maximal, but the same is true for $x^{-1}\mathbb{M}_2(\mathbb{Z})x$ for all x in $\mathrm{GL}_2(\mathbb{Q})$.

Let H be definite, and let R be a maximal order in H. Define $\widehat{\mathbb{Q}}$ to be the finite adele ring of $\mathbb{Q}$ and $\widehat{\mathbb{Z}}$ to be the subring of integral adeles, then set

$$\widehat{H} = H \otimes_{\mathbb{Q}} \widehat{\mathbb{Q}}, \qquad \widehat{R} = R \otimes_{\mathbb{Z}} \widehat{\mathbb{Z}}.$$

As with number fields, we have a local-global principle for ideals. Under the inverse maps

$$\begin{array}{ccc} I & \longrightarrow & I\widehat{R} \\ H \cap \hat{x}\widehat{R} & \longleftarrow & \hat{x}\widehat{R} \end{array}$$

every nonzero right ideal I corresponds to a subset $I\widehat{R}$ of of $\widehat{H}$ of the form $\hat{x}\widehat{R}$ for an element $\hat{x}$ of $\widehat{H}^*$.

Every fractional right ideal of R is a locally free, rank one module over R, and conversely every such module embeds in H. Thus the isomorphism classes of locally free, right modules of rank one over R are in bijection with the set

$$H^* \backslash \widehat{H}^* / \widehat{R}^*.$$

Since $H^* \backslash \widehat{H}^*$ is compact in the topology on the idele group $\widehat{H}^*$, and $\widehat{R}^*$ is open, the set of isomorphism classes is finite.

Definition 2.8. Let I be a right ideal for R. The *left order* of I is defined to be the subring $S = \{x \in H \mid xI \subseteq I\}$ of H.

It is clear that S is an order of H. Locally it is conjugate to R at all finite primes, so in fact S is also maximal.

Proposition 2.9. *Every maximal order of H appears up to isomorphism as the left order of a right ideal for R.*

Proof. Let S be another maximal order in H, and set

$$I = \{x \in H \mid Sx \subseteq R\}.$$

Then I is a right ideal for R and a left ideal for S. □

Corollary 2.10. *The number of maximal orders of H, up to isomorphism, is bounded above by the number of right ideals of R, up to isomorphism.*

Definition 2.11. The *norm* of a right R-ideal I, denoted $\mathrm{N}(I)$, is the positive integer generating the ideal $\{\mathrm{Nr}(x) \mid x \in I\}\mathbb{Z}$.

Lemma 2.12. *Let R and S be maximal orders in H. Then the ideals $I = \{x \in H \mid Sx \subseteq R\}$ and $J = \{x \in H \mid Rx \subseteq S\}$ satisfy $N(I) = N(J) = m$ and $JI = mR$ and $IJ = mS$.*

Proof. From the definition of I it is clear that I is a right ideal for R and a left ideal for S, and that moreover $I \subseteq R$. Set $\overline{I} = \{\overline{x} \mid x \in I\}$. Locally at each prime l we have $I_l = S_l x_l = y_l R_l$ for x_l and y_l in H_l^*. Then

$$I_l \overline{I}_l = S_l x_l \overline{x}_l S_l = \mathrm{Nr}(x_l) S_l \quad \text{and} \quad \overline{I}_l I_l = R_l \overline{y}_l y_l R_l = \mathrm{Nr}(y_l) R_l.$$

But the norm of an ideal is locally defined, so we have $\mathrm{Nr}(x_l)\mathbb{Z}_l = \mathrm{Nr}(y_l)\mathbb{Z}_l = m\mathbb{Z}_l$. Thus globally we have $I\overline{I} = mS$ and $\overline{I}I = mR$.

It remains only to show that $J = \overline{I}$. Combining the equalities $I\overline{I} = mS$ and $\overline{I}I = mR$ with the inclusion $I \subseteq R$, we obtain $mR \subset \overline{I}$. Continuing similarly, we have $mI \subseteq mS$, so $I \subseteq S$. But then $\overline{I} \subseteq \overline{S} = S$. Moreover $\overline{I}$ is a left R-ideal, so $R\overline{I} = \overline{I} \subseteq S$, and by the definition of J we have $\overline{I} \subseteq J$. By symmetry we conclude that $\overline{J} \subseteq I$, hence $J \subseteq \overline{I}$, so the desired equality $J = \overline{I}$ holds. □

Proposition 2.13. *The number of right ideal classes for a maximal order of H is independent of the maximal order and is the same for left ideals.*

Proof. For two maximal orders R and S, set $I = \{x \in H \mid Sx \subseteq R\}$ and $J = \{x \in H \mid Rx \subseteq S\}$ as above, and let $I_1, \ldots, I_h$ be a collection of representatives for the distinct right ideal classes of R. Then $I_1 J, \ldots, I_h J$ is a collection of distinct right ideals for S. Since $JI = mR$ and $IJ = mS$, for $m = \mathrm{N}(I)$, the maps $I_i \mapsto I_i J$ and $J_i \mapsto J_i I$ compose to give $I_i \mapsto mI_i \cong I_i$. Thus the ideals I and J determine bijections of the ideal classes for R and S. The second statement follows by taking conjugates. □

Let I a right ideal for a maximal order R, with left order S, then $R \cap S$ is the left order of the pair (R, I) of right R-modules. This motivates the following definition.

Definition 2.14. An *Eichler order* R in H is defined to be the intersection of two maximal orders in H. The level m of R is the index of R in any maximal order containing it.

Example 2.15. Returning again to the quaternion algebras of Example 2.2, we have the following examples of maximal orders and ideals.

1. Let $H = \mathbb{M}_2(\mathbb{Z})$ be the split quaternion algebra, and set $R = \mathbb{M}_2(\mathbb{Z})$. Then every right ideal is principle, and R is conjugate to every maximal order in H.
2. Let $H = \mathbb{Q} + \mathbb{Q}i + \mathbb{Q}j + \mathbb{Q}ij$, where $i^2 = j^2 = -1$ and $ij + ji = 0$, and set $R = \mathbb{Z}\langle i, j, \omega \rangle$, where
$$\omega = \frac{1 + i + j + ij}{2}.$$
Then R is a right principle ideal ring, and up to isomorphism, the unique maximal order in H.

   It is also known that the order $\mathbb{Z}\langle i, j \rangle$ is a principle ideal ring, and up to isomorphism, the unique order of level 2 in H. It is not, however, an Eichler order since locally there is a unique maximal order at a ramifying prime, so the intersection of two maximal orders is always maximal at the ramifying primes.
3. Let $R = \mathbb{Z}\langle x, y \rangle$ where
$$\begin{aligned} x^2 + 2 &= 0 \\ y^2 + y + 5 &= 0 \\ xy + yx + x + 1 &= 0 \end{aligned}$$
in the previously defined quaternion algebra ramified at 37 and ∞. Then there are three ideal classes, with representatives:
$$I_1 = R, \qquad I_2 = (2, 1 - x + y)R, \qquad I_3 = (2, x - y)R.$$
Set $z = 1 - x + y$. We note that $\overline{z} = x - y$, and the subring $\mathbb{Z}[z]$ is a maximal order of discriminant -23 in a quadratic imaginary extension of $\mathbb{Q}$ of class number 3. The ideals I_1, I_2, and I_3 are generated by the ideal representatives (1), $(2, z)$, and $(2, \overline{z})$ of this subring.

§3. Hecke modules

Let $\widetilde{\mathbb{T}}$ be the infinite dimensional *Hecke algebra* $\mathbb{Z}[\ldots, T_n, \ldots]$ generated by commuting indeterminates T_n, indexed by the positive integers. We define a *Hecke module* to be a $\widetilde{\mathbb{T}}$-module M, which is free of finite rank over $\mathbb{Z}$. We set $\widetilde{\mathbb{T}}_{(N)}$ equal to the subalgebra of $\widetilde{\mathbb{T}}$ generated by T_n for all n relatively prime to N. We say that a homomorphism $M_1 \longrightarrow M_2$ is compatible with Hecke operators T_n relatively prime to N if it is a homomorphism of $\widetilde{\mathbb{T}}_{(N)}$-modules.

In this section we describe two constructions of Hecke modules. The first construction, due to Mestre and Oesterlé [10], is defined in terms

of supersingular points on classical modular curves. The second is a generalization in terms of quaternion algebras. We conclude the section by recalling a map of these modules to the standard Hecke module of classical modular forms.

3.1. Hecke modules on supersingular points

Let k be an algebraic closure of a finite field of characteristic p, let E/k be a supersingular elliptic curve over k, and let C be a cyclic subgroup of order m. We denoted by $\mathbf{E}$ the pair (E, C), which we will call an enhanced elliptic curve. Then the endomorphism ring $\mathrm{End}_k(\mathbf{E})$ of the pair is an Eichler order of level m in the quaternion algebra ramified at p and ∞.

We define $\mathcal{S}$ to be a set of representatives of the isomorphism classes of enhanced elliptic curves of level m over k. Then an element $\mathbf{E}$ of $\mathcal{S}$ determines a point on $X_0(mp)/k$, in fact a double point of the reduction to k, so we can form the divisor group

$$M = \bigoplus_{\mathbf{E}\in\mathcal{S}} \mathbb{Z}\cdot[\mathbf{E}] \subseteq \mathrm{Div}_k(X_0(mp)),$$

and let X be the subgroup of degree zero divisors in M. The Hecke operators act on M and X by:

$$T_n([\mathbf{E}]) = \sum_{\varphi} [\mathbf{F}] = \sum_{\mathbf{F}\in\mathcal{S}} a_n(\mathbf{E},\mathbf{F})\,[\mathbf{F}],$$

for all $(n, mp) = 1$, where the first sum is over the cyclic isogenies $\varphi : \mathbf{E} \longrightarrow \mathbf{F}$ of degree n, up to isomorphism of the image curve $\mathbf{F}$.

For two enhanced elliptic curves $\mathbf{E}$ and $\mathbf{F}$ let $\mathrm{Isom}(\mathbf{E},\mathbf{F})$ be the set of isomorphisms from $\mathbf{E}$ to $\mathbf{F}$. We define an inner product on M by

$$\langle[\mathbf{E}],[\mathbf{F}]\rangle = \frac{1}{2}\,|\mathrm{Isom}(\mathbf{E},\mathbf{F})|,$$

extending $\langle\ ,\ \rangle$ bilinearly to $M \times M$. The Hecke operators T_n are Hermitian with respect to the inner product:

$$\langle[\mathbf{E}], T_n([\mathbf{F}])\rangle = \langle T_n([\mathbf{E}]),[\mathbf{F}]\rangle.$$

The orthogonal complement to X in M is the rank one space generated over $\mathbb{Q}$ by the element

$$\mathcal{E}is = \sum_{\mathbf{E}\in\mathcal{S}} \langle[\mathbf{E}],[\mathbf{E}]\rangle^{-1}[\mathbf{E}]$$

of $M \otimes_{\mathbb{Z}} \mathbb{Q}$, which we call the *Eisenstein* subspace of M.

3.2. Hecke modules on quaternion ideals

Let $\mathcal{E}ll$ be the category of enhanced supersingular elliptic curves over k, let $\mathbf{E}$ be a fixed object, and set $R = \mathrm{End}_k(\mathbf{E})$. Then R is an Eichler order in the definite quaternion algebra $H = R \otimes_{\mathbb{Z}} \mathbb{Q}$ ramified at p and ∞. Define $\mathcal{M}od_R$ to be the category of right locally free rank one modules over R. Then $\mathrm{Hom}_k(\mathbf{E}, -) : \mathcal{E}ll \longrightarrow \mathcal{M}od_R$ is a functor and determines an equivalence of categories. The previous construction of Hecke modules was functorially defined hence carries over in terms of objects and maps in $\mathcal{M}od_R$.

We thus present the following construction as a generalization of the previous one. For a definite quaternion algebra H of discriminant D and an Eichler order R of level m, define $\mathcal{S}$ to be a set of representatives for the isomorphism classes of locally free, rank one right modules over R. Define the formal divisor group M to be the free abelian group

$$M = \bigoplus_{I \in \mathcal{S}} \mathbb{Z} \cdot [I],$$

on the basis $\mathcal{S}$. As before, we set X equal to the subgroup of formal degree zero elements. We say that a nonzero homomorphism $\varphi : I \longrightarrow J$ is *cyclic* of degree n if

$$J/\varphi(I) \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}.$$

We note that with this definition $J/\varphi(I)$ is a principle R-module. Based on the analysis of the torsion structure of supersingular elliptic curves by Lenstra [9], when R is the endomorphism ring of an enhanced supersingular elliptic curve $\mathbf{E}$, this agrees, under the equivalence of categories with $\mathcal{M}od_R$, with the definition of a cyclic isogeny in $\mathcal{E}ll$.

The Hecke operators T_n are defined as before as the operators

$$T_n([I]) = \sum_{\varphi} [J] = \sum_{J \in \mathcal{S}} a_n(I, J)\,[J],$$

for $(n, Dm) = 1$ where the first sum is over cyclic R-module homomorphisms $\varphi : I \longrightarrow J$ of degree n, up to isomorphism of J. In practice, I and J can be embedded in H as fractional right R-ideals such that the homomorphism φ is an inclusion, which gives

$$I \xhookrightarrow{\varphi} J \hookrightarrow n^{-1}I.$$

and we can equivalently sum over the inclusions of cyclic submodules $J \longrightarrow n^{-1}I$.

As in the supersingular elliptic curve construction, we define an inner product on M by

$$\langle [I], [J] \rangle = \frac{1}{2} |\mathrm{Isom}(I, J)|,$$

extending $\langle\ ,\ \rangle$ bilinearly to $M \times M$. One verifies as before that the Hecke operators T_n satisfy:

$$\langle [I], T_n([J]) \rangle = \langle T_n([I]), [J] \rangle,$$

and the orthogonal complement to X in M is the rank one subgroup E generated by a constant multiple of the element

$$\mathcal{E}is = \sum_{I \in \mathcal{S}} \langle [I], [I] \rangle^{-1} [I]$$

of $M \otimes_{\mathbb{Z}} \mathbb{Q}$, defining the Eisenstein subspace of M.

3.3. Hecke modules of classical modular forms

The relation between Hecke modules of quaternions and modular forms is given by the theory of the classical Brandt matrices developed by Eichler [5]. Further aspects of the theory and computation were developed by Pizer [11]. The present formulation follows that of Kohel [8]. In this theory, there exists a Hecke-bilinear pairing with image in the space of modular forms:

$$\Theta : M \times M \longrightarrow M_2(\Gamma_0(N), \mathbb{Z}),$$

where M is the Hecke module defined relative to an Eichler order of level m and discriminant D and $N = Dm$. In defining the pairing Θ, one first defines operators

$$A_n = \sum_{kr^2 = n} T_k$$

such that $A_{ns} = A_n A_s$ for relatively prime n and s, and otherwise $A_{nr^2} = A_r A_{rn} - r A_n$ for primes r not dividing N. Then Θ is defined by

$$\Theta([I], [J]) = 1 + 2 \sum_{n=1}^{\infty} \langle A_n([I]), [J] \rangle\, q^n,$$

extended bilinearly to $M \times M$. This pairing takes $M \times X$ and $X \times M$ to the space of cusp forms and takes $E \times M$ and $M \times E$ into the space of Eisenstein series.

For each pair of elements I and J in the basis $\mathcal{S}$, the coefficients of $\Theta([I]), [J])$ are obtained as the representation numbers of the degree map

on the rank four $\mathbb{Z}$-module $\mathrm{Hom}_R(I,J)$, a quaternary quadratic form over $\mathbb{Z}$. By standard results for theta functions (see for instance Chapter IX of Schoeneberg [17]), the series $\Theta([I],[J])$ lies in $M_2(\Gamma_0(N),\mathbb{Z})$.

In terms of the basis $\mathcal{S}$, the matrices of the operators A_n are the classical Brandt matrices, B_n, and the matrices $\big(\Theta([I],[J])_n\big)$ of n-th coefficients equal $2WB_n$, where $W = \big(\langle [I],[J]\rangle\big)$ is the diagonal Gram matrix of the inner product on M. Since the representation numbers are well-defined, we obtain operators A_n for all n, and in particular define Hecke operators $T_p = A_p$ also for p dividing N. By the recursions for A_n, for all p not dividing N we have

$$T_p(\Theta([I],[J])) = \Theta(T_p([I]),[J]) = \Theta([I],T_p([J])),$$

where we denote also by T_p the p-th Hecke operator on $M_2(\Gamma_0(N),\mathbb{Z})$.

§4. Shimura curves

Shimura curves provide a generalization of modular curves on which the previous construction has a natural interpretation. For an Eichler order R in an indefinite quaternion algebra, there is an associated Shimura curve which is the moduli space of abelian surfaces with a prescribed embedding of R in the endomorphism ring. For the present purpose we define a Shimura curve as a quotient of the upper half plane and discuss arithmetic constructions on the Jacobian varieties of these curves.

4.1. Construction of Shimura curves

Let B/Q be an indefinite quaternion algebra over $\mathbb{Q}$ of discriminant D, and let R be an Eichler order of level m in B. We fix once and for all an isomorphism

$$B \otimes \mathbb{R} \cong \mathbb{M}_2(\mathbb{R}).$$

Under this isomorphism there exists a well-defined left action of $B^* \cong \mathrm{GL}(\mathbb{R})$ on the upper half plane $\mathcal{H}$. We set

$$\Gamma_0^D(m) = \{x \in R^* \mid \mathrm{Nr}(x) = 1\},$$

and define the Shimura curve to be a model for the quotient

$$X_0^D(m) = \overline{\Gamma_0^D(m)\backslash\mathcal{H}},$$

where the bar indicates the compactification. When $D = 1$, then $\Gamma_0^1(m) = \Gamma_0(m)$, so this generalizes the standard definition of the modular curve $X_0(m)$. When D is greater than one, then the quotient $\Gamma_0^D(m)\backslash\mathcal{H}$ is already compact.

4.2. Semistable reduction and monodromy groups

For the construction of analogous Hecke modules on the Jacobians of Shimura curves, we recall some general constructions of Grothendieck [7] on abelian varieties.

Let $A/\mathbb{Q}$ be an abelian variety with semistable reduction at a prime p, and let k be an algebraic closure of $\mathbb{F}_p$. We define a finite subgroup $\Phi = \Phi(A,p)$ as the component group of the fiber at p of the Néron model for A, and let $T = T(A,p)$ be the toric part of the same fiber. We define the *monodromy* group of A at p to be

$$\mathcal{X}(A,p) = \mathrm{Hom}_k(T, \mathbb{G}_m).$$

We note that T/k is isomorphic to a finite product of copies of $\mathbb{G}_m$, and thus $\mathcal{X}(A,p)$ is a free abelian group.

Let $A^\vee$ be the dual abelian variety of A, and suppose that there exists a canonical principal polarization $\xi : A \longrightarrow A^\vee$. Such is the case, for instance, if A is the Jacobian of a curve. There exists a canonical bilinear pairing,

$$u : \mathcal{X}(A,p) \times \mathcal{X}(A^\vee,p) \longrightarrow \mathbb{Z},$$

such that $\langle x, y\rangle = u(x, \xi(y))$ defines a symmetric positive definite pairing on $\mathcal{X}(A,p)$. By the following result, Theorem 11.5 of Grothendieck [7], the monodromy pairing permits the determination of the component group $\Phi(A,p)$ of an abelian variety A.

Theorem 4.1. *There exists a natural exact sequence*

$$0 \longrightarrow \mathcal{X}(A,p) \longrightarrow \mathrm{Hom}(\mathcal{X}(A,p), \mathbb{Z}) \longrightarrow \Phi \longrightarrow 0,$$

taking $x \in \mathcal{X}(A,p)$ *to* $u(-, \xi(x))$.

4.3. Hecke modules on Shimura curves

We now apply the previous constructions to the Jacobians of Shimura curves. As for classical modular curves, the Jacobian of a Shimura curve $X_0^D(m)$ is naturally equipped with Hecke operators T_n for all n relatively prime to the level $N = Dm$. As defined by correspondences on divisor groups (see §7.4 of Shimura [16]), the Hecke operators embed naturally in the endomorphism ring of the Jacobian $J_0^D(m)$. Following the exposition of Takahashi [18], we summarize here results of Ribet [13], by which we can interpret the previous constructions of Hecke modules.

Theorem 4.2. *Let D be a product of an even number of primes, and let p and q be distinct primes coprime to D. Then there exists a canonical exact sequence*

$$0 \longrightarrow \mathcal{X}(A',p) \xrightarrow{\iota} \mathcal{X}(A,q) \longrightarrow \mathcal{X}(A'',q) \times \mathcal{X}(A'',q) \longrightarrow 0$$

where

$$A' = J_0^{Dpq}(m), \qquad A = J_0^D(mpq), \qquad A'' = J_0^D(mq).$$

The homomorphisms are compatible with the Hecke operators T_n for all n relatively prime to $Dpqm$. With respect to the monodromy pairings on $\mathcal{X}(A', p)$ and $\mathcal{X}(A, q)$, the map ι is an isometry with its image.

Proof. This exact sequence was proved by Ribet for $D = 1$ in [13], and the general case holds following the work of Buzzard [2]. □

By means of the following theorem we may interpret the construction of Hecke modules of quaternions in terms of the monodromy groups of the Jacobians of Shimura curves.

Theorem 4.3. *Let H be a positive definite quaternion algebra of discriminant Dp, and let $X(Dp, m)$ be the Hecke module for an Eichler order R of level m. Then there exists a canonical isomorphism*

$$X(Dp, m) \cong \mathcal{X}(J_0^D(mp), p).$$

The isomorphism is compatible with Hecke operators T_n for all n relatively prime to Dpm, and is an isometry with respect to the respective inner products. In particular, $\mathcal{X}(J_0^{Dqr}(mp), p)$, $\mathcal{X}(J_0^{Dpr}(mq), q)$, and $\mathcal{X}(J_0^{Dpq}(mr), r)$ are canonically isomorphic for distinct primes p, q, and r relatively prime to D.

Proof. This is a consequence of Theorem 4.7 and Theorem 4.10 of Buzzard [2], which prove the results analogous to Deligne and Rapoport [4]. The present formulation appears in Takahashi [18]. □

§5. Examples and computations

Let $X(Dp, m)$ denote the Hecke module constructed for an Eichler order of level m in the definite quaternion algebra of discriminant Dp. As in Theorem 7.14 of Shimura [16], the decomposition of the Hecke modules $X(Dp, m)$ into its Hecke-stable subspaces give isogeny factors of the Jacobian $J_0^D(m)$. Of particular interest are the rank one factors, corresponding to elliptic curves covered by the curve $X_0^D(m)$.

We consider in this section those Hecke modules $X(Dp, m)$, for which Dpm divides 30. Under the isomorphism of Theorem 4.3, we

identify $X(Dp, m)$ with $\mathcal{X}(J_0^D(mp), p)$. Then from Theorem 4.2 we obtain the following six exact sequences:

$$(1)\quad 0 \longrightarrow \mathcal{X}(J_0^{15}(2), 3) \longrightarrow X(5,6) \longrightarrow X(5,2) \times X(5,2) \longrightarrow 0$$

$$(2)\quad 0 \longrightarrow \mathcal{X}(J_0^{15}(2), 5) \longrightarrow X(3,10) \longrightarrow X(3,2) \times X(3,2) \longrightarrow 0$$

$$(3)\quad 0 \longrightarrow \mathcal{X}(J_0^{6}(5), 2) \longrightarrow X(3,10) \longrightarrow X(3,5) \times X(3,5) \longrightarrow 0$$

$$(4)\quad 0 \longrightarrow \mathcal{X}(J_0^{6}(5), 3) \longrightarrow X(2,15) \longrightarrow X(2,5) \times X(2,5) \longrightarrow 0$$

$$(5)\quad 0 \longrightarrow \mathcal{X}(J_0^{10}(3), 2) \longrightarrow X(5,6) \longrightarrow X(5,3) \times X(5,3) \longrightarrow 0$$

$$(6)\quad 0 \longrightarrow \mathcal{X}(J_0^{10}(3), 5) \longrightarrow X(2,15) \longrightarrow X(2,3) \times X(2,3) \longrightarrow 0$$

The Hecke modules $\mathcal{X}(J_0^{Dpq}(m), q))$ can then be identified as the kernel of the corresponding projections, once the Hecke modules $X(Dp, mq)$ and $X(Dp, m)$ are determined.

By means of the quaternion algebra arithmetic described in Section 2 and the Hecke module construction in Section 3, it is possible to compute the Hecke modules $X(Dp, m)$. Implementing this arithmetic in the computer algebra system Magma [1], the author determined bases for the modules $X(Dp, m)$, together with the representations of the Hecke algebras on these modules.

Since the curves $X_0(2)$, $X_0(3)$, and $X_0(5)$ have genus zero, the corresponding Hecke modules $X(2,1)$, $X(3,1)$, and $X(5,1)$ are zero. Likewise the curves $X_0(6)$ and $X_0(10)$ have genus zero, so $X(2,3)$, $X(3,2)$, $X(2,5)$, and $X(5,2)$ are zero. Each of the remaining modules:

$$X(3,5),\ X(5,3),\ X(2,15),\ X(3,10),\ X(5,6),\ \text{and}\ X(30,1)$$

are nontrivial, and the Hecke-invariant subspaces are all of rank one.

The table below summarizes the arithmetic data. The column denoted class refers to the isogeny class of corresponding isogeny factor in Cremona [3]; the column $\langle v, v \rangle$ gives the self inner product of a generator v of the rank one eigenspace over $\mathbb{Z}$, and a_n is the eigenvalue of the Hecke operator T_n. We also note that the eigenspace generators need not generate $X(Dp, m)$. In the case of $X(3,10)$ and $X(5,6)$ they generate a submodule of index two.

Invariants of X(Dp, m)

$X(Dp,m)$	rank	class	$\langle v,v\rangle$	a_2	a_3	a_5	a_7
$X(3,5)$	1	$15A$	4	-1	-1	1	0
$X(5,3)$	1	$15A$	4	-1	-1	1	0
$X(2,15)$	1	$30A$	2	-1	1	-1	-4
$X(3,10)$	3	$30A$	6	-1	1	-1	-4
		$15A$	4	1	-1	1	0
		$15A$	2	-3	-1	1	0
$X(5,6)$	3	$30A$	2	-1	1	-1	-4
		$15A$	4	1	-1	1	0
		$15A$	2	-3	-1	1	0
$X(30,1)$	1	$30A$	6	-1	1	-1	-4

From the previous exact sequences it is possible to identify kernel submodules of these Hecke modules. The modules $\mathcal{X}(J_0^{15}(2),3)$ and $\mathcal{X}(J_0^{15}(2),5)$ are isomorphic to $X(5,6)$ and $X(3,10)$, respectively. The module $\mathcal{X}(J_0^{6}(5),2)$ can be identified as the rank one kernel of T_2+1 in $X(3,10)$, and both $\mathcal{X}(J_0^{6}(5),3)$ and $\mathcal{X}(J_0^{10}(3),5)$ are canonically isomorphic to $X(2,15)$. The module $\mathcal{X}(J_0^{10}(3),2)$ can be identified with the rank one kernel of T_2+1 in $X(5,6)$. While the Hecke module $X(30,1)$ does not enter into the exact sequences, by Theorem 4.3 it is canonically isomorphic to each of $\mathcal{X}(J_0^{15}(2),2)$, $\mathcal{X}(J_0^{10}(3),3)$, and $\mathcal{X}(J_0^{6}(5),5)$, by which we can identify again the common isogeny factor $30A$ of $J_0^{15}(2)$, $J_0^{10}(3)$, and $J_0^{6}(5)$.

It is also possible to analyze the kernel of the maps of $\mathcal{X}(J_0^D(mp),q)$ to $\mathcal{X}(J_0^D(m),q)$ induced by the quotients $J_0^D(mq) \rightrightarrows J_0^D(m)$ when q divides D. First, to have a concise representation of the above exacts sequences, we express a short exact sequence of the form $0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \times M'' \longrightarrow 0$ in the nonstandard manner

$$0 \longrightarrow M' \longrightarrow M \rightrightarrows M'' \longrightarrow 0,$$

where the double arrows are the projections to the factors. Note that in this notation M' is the intersection of the kernels of the two maps, and the condition of surjectivity is stronger than surjectivity on each of the components M''. By the naturality of these exact sequences with respect to the two projections of $J_0^D(mp)$ to $J_0^D(m)$, we observe that

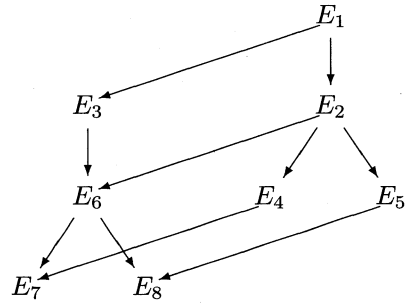
there exist exact sequences of sequences of the form:

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & W & \longrightarrow & \mathcal{X}(J_0^{10}(3),2) & \rightrightarrows & \mathcal{X}(J_0^{10}(1),2) & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \mathcal{X}(J_0^{15}(2),3) & \longrightarrow & X(5,6) & \rightrightarrows & X(5,2) & \longrightarrow & 0 \\
 & & \downarrow\downarrow & & \downarrow\downarrow & & \downarrow\downarrow & & \\
0 & \longrightarrow & \mathcal{X}(J_0^{15}(1),3) & \longrightarrow & X(5,3) & \rightrightarrows & X(5,1) & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}$$

in which W is isomorphic to $\mathcal{X}(J_0^{10}(3),2)$ and identified in $\mathcal{X}(J_0^{15}(2),3) \cong X(5,6)$ as the kernel of the projection to $X(5,3)\times X(5,3)$, corresponding again to the isogeny factor $30A$.

§6. Further considerations

The above analysis gives a breakdown of the isogeny factors of the Jacobians of Shimura and classical modular curves, but ignores more subtle details omitted by a characterization only up to isogeny. For instance, the isogeny class of elliptic curves of conductor 30 consists of one isogeny class of eight curves, denoted $30A1 - 8$ in the notation of Cremona [3], and which we denote by E_1 through E_8. The curves in this isogeny class are connected by isogenies over $\mathbb{Q}$ of degree 2 and 3 as indicated in the diagram below.



One defines an optimal quotient of an abelian variety to be a quotient with connected kernel, which is unique in its isogeny class, up to isomorphism. For instance, the optimal quotient of $J_0(30)$ is the curve E_1.

Roberts [15] finds the elliptic curves $J_0^6(5)$ and $J_0^{10}(3)$ to be E_6 and E_2, respectively, and the optimal quotient of $J_0^{15}(2)$ in the isogeny class $30A$ to be E_3.

Other arithmetic invariants of Shimura curves may be studied in the setting of quaternions. The component group of a special fiber of the Néron model for $J_0^D(m)$; congruence primes, as in Ribet [12]; and the degree of a parameterization of a modular elliptic curve may also be studied in this context. Theorem 4.1 provides the means for studying component groups. Congruence primes are defined as prime divisors of the index of the subgroup generated by eigenvectors in the Hecke module; it was noted in particular that 2 is a congruence prime for $X(3,10)$ and $X(5,6)$. For classical modular curves the methods for computing degree of modular parameterizations are well-developed, and Cremona [3] has compiled extensive computations. The problem for Shimura curves has been studies by Ribet and Takahashi [14] and Takahashi [18], and this work can be applied in the analysis of the quaternion Hecke modules. Finally, in cases when the level is not square-free, it may be possible to extend the understanding of modular and Shimura curves by computation or proving results for Hecke modules of quaternions.

Acknowledgement. I express thanks for the insight provided by the thesis of Shuzo Takahashi, and for conversations with Ken Ribet on this subject. Diagrams and exact sequences were prepared using Paul Taylor's diagrams package [19] in LaTeX.

References

[1] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system I: The user language. *J. Symb. Comp.*, **24** (1997), no. 3-4, 235–265.

[2] K. Buzzard. Integral models of Shimura curves. *Duke Math Journal*, **87** (1997), no. 3, 591–612.

[3] J. E. Cremona. *Algorithms for modular elliptic curves.* Cambridge University Press, 2nd edition, 1997.

[4] P. Deligne and M. Rapoport. Les schémas de modules de courbes elliptiques. In Lecture Notes in Mathematics, **349**, Springer-Verlag, 1973, 143–316.

[5] M. Eichler. The basis problem for modular forms and the traces of the Hecke operators. In W. Kuyk, editor, *Modular Functions of One Variable I*, Lecture Notes in Mathematics, **320**, Springer-Verlag, 1973, 75–152.

[6] N. Elkies. Shimura curve computations. In J. P. Buhler, editor, *Algorithmic Number Theory*, Lecture Notes in Computer Science, **1423**, Springer, 1998, 1–47.

[7] A. Grothendieck. SGA7 I, Exposé IX. In Lecture Notes in Mathematics, **288**, Springer-Verlag, 1972, 313–523.

[8] D. Kohel. Computing modular curves via quaternions. *Manuscript*, 1998.

[9] H. W. Lenstra, Jr. Complex multiplication structure of elliptic curves. *Journal of Number Theory*, **56** (1996), no. 2, 227–241.

[10] J.-F. Mestre. Sur la méthode des graphes, Exemples et applications. In *Proceedings of the international conference on class numbers and fundamental units of algebraic number fields*, Nagoya University, 1986, 217–242.

[11] A. Pizer. An algorithm for computing modular forms on $\Gamma_0(N)$. *Journal of Algebra*, **64** (1980), 340–390.

[12] K. Ribet. Mod p Hecke operators and congruences between modular forms. *Invent. Math.*, **71** (1983), no. 1, 193–205.

[13] K. Ribet. On modular representations of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ arising from modular forms. *Inventiones Math.*, **100** (1990), 431–476.

[14] K. Ribet and S. Takahashi. Parameterizations of elliptic curves by Shimura curves and by classical modular curves. *Proc. Natl. Acad. Sci.*, **94** (1997), no. 21, 11110–11114.

[15] D. Roberts. Shimura curves analogous to $X_0(N)$. Ph.D. thesis, Harvard University, 1989.

[16] G. Shimura. *Introduction to the Arithmetic Theory of Automorphic Forms*. Princeton University Press, 1971.

[17] B. Schoeneberg. *Elliptic Modular Functions*. Grundlehren der mathematischen Wissenschaften, **203**, Springer-Verlag, 1974.

[18] S. Takahashi. *Degrees of parameterizations of elliptic curves by modular curves and Shimura curves*. PhD thesis, University of California, Berkeley, 1998.

[19] P. Taylor. Commutative diagrams in TEX. CTAN archive at ftp://ftp.tex.ac.uk/ in tex-archive/macros/generic/diagrams/taylor/, diagrams.tex, ver. 3.86, 1998.

[20] M.-F. Vignéras. *Arithmétique des Algèbres de Quaternions*, Lecture Notes in Mathematics, **800**, Springer-Verlag, 1980.

Department of Mathematics, National University of Singapore
E-mail address: kohel@math.nus.edu.sg