

# On the Curves Associated to Certain Rings of Automorphic Forms

Kamal Khuri-Makdisi

*Abstract.* In a 1987 paper, Gross introduced certain curves associated to a definite quaternion algebra  $B$  over  $\mathbf{Q}$ ; he then proved an analog of his result with Zagier for these curves. In Gross' paper, the curves were defined in a somewhat *ad hoc* manner. In this article, we present an interpretation of these curves as projective varieties arising from graded rings of automorphic forms on  $B^\times$ , analogously to the construction in the Satake compactification. To define such graded rings, one needs to introduce a "multiplication" of automorphic forms that arises from the representation ring of  $B^\times$ . The resulting curves are unions of projective lines equipped with a collection of Hecke correspondences. They parametrize two-dimensional complex tori with quaternionic multiplication. In general, these complex tori are not abelian varieties; they are algebraic precisely when they correspond to CM points on these curves, and are thus isogenous to a product  $E \times E$ , where  $E$  is an elliptic curve with complex multiplication. For these CM points one can make a relation between the action of the  $p$ -th Hecke operator and Frobenius at  $p$ , similar to the well-known congruence relation of Eichler and Shimura.

## 1 Introduction

Algebraic geometry on modular curves plays an essential role in most of the arithmetic properties of modular forms on the upper half-plane  $\mathcal{H}$ . For instance, given a cuspidal weight 2 Hecke eigenform  $f \in S_2(\Gamma_0(N))$ , it is well-known that one can find a corresponding  $\ell$ -adic Galois representation  $\rho_{f,\ell}: \text{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \rightarrow \text{GL}(2, \overline{\mathbf{Q}}_\ell)$  on a subspace of the étale cohomology group  $H^1(X_0(N), \mathbf{Q}_\ell)$  of the modular curve  $X_0(N)$ . Underlying this well-known construction are the following facts (see Chapters 6 and 7 of [S]):

1. The space of cusp forms  $S_2(\Gamma_0(N))$  is isomorphic to the space of holomorphic differentials on the Riemann surface  $X_0(N)$ . For general weight  $k$ , the space of cuspforms  $S_k(\Gamma_0(N))$  and the space of all modular forms  $M_k(\Gamma_0(N))$  are spaces of holomorphic sections of some line bundle on  $X_0(N)$ . Moreover, the structure of  $X_0(N)$  as a complex algebraic curve is captured by the multiplicative structure of the graded ring  $R$  of all modular forms on  $\Gamma_0(N)$ : namely,  $R = \bigoplus_{n \geq 0} M_n(\Gamma_0(N))$ .
2. The Riemann surface  $X_0(N)$ , initially defined analytically as a compactification of  $\Gamma_0(N) \backslash \mathcal{H}$ , is in fact an algebraic curve defined over  $\mathbf{Q}$ , or, in more general contexts, over a number field (this is what allows us to look for Galois representations in its étale cohomology); furthermore, Hecke operators arise from algebraic correspondences on  $X_0(N)$ , which are also defined over  $\mathbf{Q}$ . Essentially, this is saying that the graded ring  $R$  comes from a graded  $\mathbf{Q}$ -algebra, or that there is a rational structure on  $M_n(\Gamma_0(N))$  compatible with multiplication of modular forms.

---

Received by the editors March 12, 1999.

AMS subject classification: 11F.

©Canadian Mathematical Society 2001.

3. In addition to being an algebraic curve,  $X_0(N)$  has an interpretation as a moduli space for elliptic curves with a distinguished cyclic subgroup of order  $N$ , whence one can get a finer version of fact 2 above. Importantly, one can then understand the reduction of  $X_0(N)$  modulo a prime  $p$  (say  $p \nmid N$ ), and determine the effect of a Frobenius element  $\text{Frob } p$  on  $H^1(X_0(N), \mathbf{Q}_\ell)$ .
4. In particular, one has the Eichler-Shimura congruence, relating  $\text{Frob } p$  to the reduction modulo  $p$  of the Hecke operator  $T_p$ . This allows us to relate the trace of  $\rho_{f,\ell}(\text{Frob } p)$  to the eigenvalue of  $f$  under  $T_p$ .

For automorphic forms on more general groups than  $\text{GL}(2)$ , partial analogs of facts 1–4 above still hold when the symmetric space of the group in question is Hermitian; this is the case of Shimura varieties. (The analog of fact 4 needs a bit more than a congruence, and is usually expressed in terms of counting points on a Shimura variety over a finite field.) The known arithmetic results for automorphic forms on groups whose symmetric spaces are not Hermitian generally rely on transferring the automorphic forms to groups with Hermitian symmetric spaces, in ways predicted by Langlands functoriality. An example of this occurs in the case of forms on an inner form of  $\text{PGL}(2)$  attached to a definite quaternion algebra  $B$ , as recalled below.

In this article, we present analogs of facts 1 and 2 above for automorphic forms on groups  $G$  with  $G(\mathbf{R})$  compact, so their symmetric space consists of a point. Nonetheless, we can define a certain graded ring  $R$  of modular forms on  $G$ , and take  $X = \mathbf{Proj} R$  as our analog of the Satake compactification of a modular curve. The resulting variety  $X$  is then defined over  $\mathbf{Q}$  (no larger number field is needed), and the Hecke operators are correspondences on  $X$ . The graded ring  $R$  arises from the tensor product operation on finite-dimensional representations of  $G$ , and the underlying rational structure on  $R$  comes from a rational structure on the spaces of “algebraic modular forms” defined in [G2]. Our construction of  $R$  and of  $X$  suggests that one wants to replace the one-point symmetric space  $G(\mathbf{R})/G(\mathbf{R})$  by the flag variety  $Y = G(\mathbf{R})/T(\mathbf{R})$ , where  $T(\mathbf{R})$  is a maximal torus of  $G(\mathbf{R})$ . The variety  $X$  is then a finite union of quotients of  $Y$  by finite groups; the arithmetic complexity of  $X$  seems to lie in its connected components (in  $H^0(X)$ ), rather than in its higher cohomology. Hence the mere fact that  $X$  is defined over  $\mathbf{Q}$  does not provide us with a ready-made source of Galois representations that might be attached to automorphic forms on  $G$ . The hope remains, though, that some deeper construction will work, especially if we can find an appropriate analog of facts 3 and 4.

We do in fact establish loose but intriguing analogs of facts 3 and 4 in the special case where  $G$  is the inner form of  $\text{PGL}(2)$  corresponding to a definite quaternion algebra  $B$  over  $\mathbf{Q}$ . In this case, corresponding to a fixed “level” of automorphic forms on  $G$ , we obtain a curve  $X$ , defined over  $\mathbf{Q}$ , such that  $X(\mathbf{C})$  is essentially a union of finitely many projective lines  $\mathbf{P}^1(\mathbf{C})$ . This type of curve  $X$  was originally introduced by B. Gross in [G1], using an *ad hoc* construction; its arithmetic has also been exploited in recent papers by M. Bertolini and H. Darmon, for example in [BD]. We hope that our definition of  $X$  as the projective variety attached to a graded ring of automorphic forms will shed light on the structure of  $X$ , as will our analogs of facts 3 and 4. Our analog of fact 3 is the fact that  $X$  has an interpretation as “moduli” for a non-algebraic problem: namely, the complex points of  $X$  parametrize two-

dimensional complex tori with endomorphisms by an order  $\mathcal{O}$  in our definite quaternion algebra  $B$ . These complex tori are rarely abelian varieties, in marked contrast to the situation that would have arisen had  $B$  been indefinite: in that case, all complex tori with endomorphisms by  $\mathcal{O}$  would have been abelian varieties, and their moduli space would have been a Shimura curve attached to  $B$ . In our case, where  $B$  is definite, a special case of a theorem of Shimura implies that a two-dimensional complex torus with an  $\mathcal{O}$ -action is an abelian variety if and only if it is isogenous to  $E \times E$ , where  $E$  is an elliptic curve with complex multiplication. Thus only the CM-points of  $X$  parametrize abelian varieties; however, the CM-points with CM-field  $K$  are always defined over  $K$ , even though the corresponding abelian varieties are typically defined over a nontrivial abelian extension of  $K$ . This even further reinforces the difference between  $X$  and a more traditional moduli space.

As for the analog of fact 4, we can show an analog of the Eichler-Shimura congruence precisely for the CM-points of  $X$ . Namely, if  $x$  is a CM-point corresponding to the abelian variety  $A$  (isogenous to  $E \times E$ ), then  $T_p x$  is a collection of  $p + 1$  points corresponding to abelian varieties  $A_0, \dots, A_p$ ; when we reduce all these abelian varieties modulo a prime above  $p$ , we get that the effect of  $T_p$  is the same “modulo  $p$ ” as that of the combination of Frob  $p$  and its transpose (see Theorem 4.22). Note that the analog of the diamond operator  $\langle p \rangle$  does not appear, or rather is trivial in our setting, because we deal with a situation for  $X$  similar to that of  $X_0(N)$ . It is well-known that one can pass indirectly from a Hecke eigenform on  $G$  to a Galois representation: first produce a related Hecke eigenform on  $GL(2)$ , by the Jacquet-Langlands correspondence (due in this case to Eichler and to Shimizu); then from the resulting modular form on  $GL(2)$ , pass to a Galois representation as usual. In the context of a larger group than  $G$ , however, the analogs of both the transitions from  $G$  to  $GL(2)$  and from modular forms on  $GL(2)$  to Galois representations are problematic, to say the least. Although this author does not currently see how to use these analogs of facts 1–4 to directly produce Galois representations from Hecke eigenforms on  $G$ , the results in this paper were originally motivated by the hope that this example might be a useful test case for seeking a direct construction of Galois representations from algebraic modular forms, as conjectured in [G2].

**Acknowledgements** I would like to acknowledge several useful conversations with B. Gross and H. Darmon. I am also grateful to E. Goren for some comments on an earlier draft of this article. The results in this article were almost all obtained, and the first part of the article initially written up, while I was at the Mathematics Department of Harvard University. I am also grateful to McGill and Concordia Universities, as well as the CICMA group in Montréal, for their hospitality during the 1998–99 academic year, during which I completed this article and greatly benefited from the special year in number theory there and at the Centre de Recherches Mathématiques at the Université de Montréal.

## Notation

We write  $\mathbf{A}$  for the ring of adèles of  $\mathbf{Q}$ , and  $\mathbf{A}_f$  for the finite adèles; so  $\mathbf{A} = \mathbf{R} \times \mathbf{A}_f$ . Then  $\mathbf{A}^\times$  is the group of ideles of  $\mathbf{Q}$ , and generally  $R^\times$  is the group of units of a ring

$R$ ; we also write  $M(n, R)$  for the algebra of  $n \times n$  matrices with entries in  $R$ . If  $G$  is an algebraic group over  $\mathbf{Q}$ , we write  $G(\mathbf{A}) = G(\mathbf{R}) \times G(\mathbf{A}_f)$  for the adelization of  $G$ , and view  $G(\mathbf{Q})$  as a discrete subgroup of  $G(\mathbf{A})$ . We also write  $G(\mathbf{Q})_f$  for the image of  $G(\mathbf{Q})$  under the projection  $G(\mathbf{A}) \rightarrow G(\mathbf{A}_f)$ . If  $R$  is a  $\mathbf{Q}$ -algebra, we write  $R_{\mathbf{A}}$  for the adelization  $R \otimes_{\mathbf{Q}} \mathbf{A}$  of  $R$ . For example,  $K_{\mathbf{A}}^{\times}$  is the group of ideles of an extension  $K$  of  $\mathbf{Q}$ . Given a commutative ring  $R$ , we write  $R_p$ , with  $p$  a prime, for the  $p$ -adic completion  $R_p = R \otimes_{\mathbf{Z}} \mathbf{Z}_p$  of  $R$ . We view  $R_p$  as a subset of  $R_{\mathbf{A}}$ .

## 2 Rings of Automorphic Forms

Our first goal in this section is to define a product structure on some spaces of automorphic forms. Take  $G$  a connected reductive group over  $\mathbf{Q}$  (the reader is invited to generalize this theory to totally real number fields), and assume throughout that  $G(\mathbf{R})$  is compact. Automorphic forms on  $G$  are certain functions on  $G(\mathbf{A})$  (really, on  $G(\mathbf{Q}) \backslash G(\mathbf{A})$ ) that can be classified by their “level” and “weight” as follows. Here we borrow some ideas from the recent article [G2].

### Definition 2.1

1. A *level* is an open compact subgroup  $U$  of  $G(\mathbf{A}_f)$ , and a *weight* is an irreducible complex representation  $W$  of  $G(\mathbf{R})$ . Note that as  $G(\mathbf{R})$  is compact,  $W$  is finite-dimensional.
2. The space of automorphic forms on  $G$  of level  $U$  and weight  $W$  is the space

$$(2.1) \quad \mathcal{A}_W(U) = \text{Hom}_{G(\mathbf{R})} \left( W, L^2(G(\mathbf{Q}) \backslash G(\mathbf{A})/U) \right).$$

This definition is analogous to Scholies 2.1.2 and 2.1.3 in [D]. In the setting there,  $G$  is  $\text{SL}(2)$  and  $W$  is a “weight  $k$ ” discrete series representation of  $\text{SL}(2, \mathbf{R})$ ; then  $\mathcal{A}_W(U)$  is the space of classical holomorphic modular forms of weight  $k$  and level corresponding to  $U$ .

**Lemma 2.2** *Let  $W^*$  be the representation contragredient to  $W$ . Then  $\mathcal{A}_W(U)$  can be identified with the space of functions  $f: G(\mathbf{Q}) \backslash G(\mathbf{A})/U \rightarrow W^*$  that are  $G(\mathbf{R})$ -equivariant, in the sense that*

$$(2.2) \quad f(gg_{\infty}) = g_{\infty}^{-1}f(g), \quad \text{whenever } g \in G(\mathbf{A}) \text{ and } g_{\infty} \in G(\mathbf{R}).$$

**Proof** An  $f$  satisfying (2.2) above corresponds to the  $G(\mathbf{R})$ -homomorphism  $\varphi$  from  $W$  to  $L^2(G(\mathbf{Q}) \backslash G(\mathbf{A})/U)$ , sending  $w \in W$  to  $\varphi_w \in L^2(G(\mathbf{Q}) \backslash G(\mathbf{A})/U)$  given by  $\varphi_w(g) = \langle f(g), w \rangle$ . Note that  $\varphi_w$  is in  $L^2$  because of two facts: first, for fixed  $g \in G(\mathbf{A})$  and varying  $g_{\infty} \in G(\mathbf{R})$ , the function  $\varphi_w(gg_{\infty})$  is a matrix coefficient of  $G(\mathbf{R})$ , and hence is  $\mathcal{C}^{\infty}$ ; second,  $G(\mathbf{Q}) \backslash G(\mathbf{A})/U$  has only finitely many connected components, which are all compact (see for example the following lemma). ■

From now on, the letters  $U$ ,  $W$ , and  $W^*$  will refer to a level, a weight, and its contragredient representation, as defined above.

**Lemma 2.3** Using the weak approximation theorem, choose a finite set of representatives for  $G(\mathbf{Q})_f \backslash G(\mathbf{A}_f)/U$ , such that  $G(\mathbf{A}_f) = \bigsqcup_{i=1}^k G(\mathbf{Q})_f g_i U$ . Define  $\Gamma_i = G(\mathbf{Q}) \cap g_i U g_i^{-1}$ ; note that  $\Gamma_i$  is a finite group, as it embeds discretely into the compact group  $G(\mathbf{R})$ . Then

$$(2.3) \quad \mathcal{A}_W(U) \cong \bigoplus_{i=1}^k (W^*)^{\Gamma_i}.$$

Here  $(W^*)^{\Gamma_i}$  refers to the vectors in  $W^*$  invariant by  $\Gamma_i$ .

**Proof** View a form  $f \in \mathcal{A}_W(U)$  as a  $W^*$ -valued function on  $G(\mathbf{Q}) \backslash G(\mathbf{A})/U$ , satisfying (2.2). The function  $f$  is determined by its values on  $g_1, \dots, g_k$ ; furthermore, requiring  $f$  to be simultaneously invariant by  $G(\mathbf{Q})$  on the left and by  $U$  on the right is equivalent to requiring each value  $f(g_i)$  to be invariant under  $\Gamma_i$ . Thus, the isomorphism of (2.3) simply sends  $f$  to the tuple  $(f(g_i))_{i=1}^k$ . ■

**Remark 2.4** We are being somewhat cavalier with our notation concerning representatives of double cosets. When we write  $g \in G(\mathbf{Q}) \backslash G(\mathbf{A})/U$ , for example, we usually mean that  $g$  is an element of  $G(\mathbf{A})$ , viewed as a representative of the double coset  $G(\mathbf{Q})gU$  in  $G(\mathbf{Q}) \backslash G(\mathbf{A})/U$ . Of course, we shall only put the representative  $g$  to uses where the choice of representative is immaterial.

We now wish to define a multiplication of automorphic forms. Let  $f \in \mathcal{A}_W(U)$  and  $f' \in \mathcal{A}_{W'}(U)$  be forms of the same level but possibly different weights. As in the case of modular forms, the product  $ff'$  should still have level  $U$ , but the weight of the product should be the “sum” of the weights  $W$  and  $W'$ , in some suitable sense. With hindsight and with the guidance of Remark 2.1.4 in [D], we make the following definitions.

**Definition 2.5** Let  $\lambda$  and  $\lambda'$  be the highest weights (in the sense of representation theory) of the irreducible representations  $W$  and  $W'$  of  $G(\mathbf{R})$ . Then define the sum of  $W$  and  $W'$  to be the irreducible representation  $W''$  of  $G(\mathbf{R})$ , with highest weight  $\lambda + \lambda'$ . Note that  $W''$  occurs inside  $W \otimes W'$ , with multiplicity one; similarly,  $(W'')^*$  occurs inside  $W^* \otimes (W')^*$ .

We shall often write  $W = W_\lambda$ ,  $W' = W_{\lambda'}$ , and  $W'' = W_{\lambda+\lambda'}$ .

**Definition 2.6** Let  $W''$  be the sum of  $W$  and  $W'$ , as above. Take  $f \in \mathcal{A}_W(U)$  and  $f' \in \mathcal{A}_{W'}(U)$ . Then define the product  $ff' \in \mathcal{A}_{W''}(U)$  in either of the following two equivalent ways:

1. View  $f$  as a  $W^*$ -valued function on  $G(\mathbf{Q}) \backslash G(\mathbf{A})/U$ , and similarly for  $f'$ . Then define, for  $g \in G(\mathbf{Q}) \backslash G(\mathbf{A})/U$ ,

$$(2.4) \quad (ff')(g) = \text{pr}(f(g) \otimes f'(g)),$$

where  $\text{pr}: W^* \otimes (W')^* \rightarrow (W'')^*$  is the projection.

2. View  $f$  as a  $G(\mathbf{R})$ -homomorphism from  $W$  to  $L^2(G(\mathbf{Q}) \backslash G(\mathbf{A})/U)$ , sending  $w \in W$  to  $\varphi_w \in L^2$ ; similarly for  $f'$ , sending  $w' \in W'$  to  $\varphi'_{w'} \in L^2$ . First define  $f \otimes f': W \otimes W' \rightarrow L^2$  by

$$(2.5) \quad [(f \otimes f')(w \otimes w')](g) = \varphi_w(g)\varphi'_{w'}(g).$$

Then define

$$(2.6) \quad ff' = (f \otimes f') \circ i,$$

where  $i: W'' \rightarrow W \otimes W'$  is the injection.

At this point,  $ff'$  is only defined up to a constant factor, since  $pr$  and  $i$  are. We shall make the product well-defined, in such a way as to obtain a graded ring of automorphic forms. Then the projective variety associated to this graded ring should be analogous to the Satake compactification of a Shimura variety. The simplest way to obtain such a graded ring is to fix a (nontrivial) representation  $W = W_\lambda$  of  $G(\mathbf{R})$ , with highest weight  $\lambda \neq 0$ . For an integer  $n \geq 0$ , let  $W_{n\lambda}$  be the representation of  $G(\mathbf{R})$  with highest weight  $n\lambda$ . Thus, the product of a form of weight  $W_{n\lambda}$  with a form of weight  $W_{m\lambda}$  is a form of weight  $W_{(m+n)\lambda}$ . We now invoke the following well-known fact.

**Lemma 2.7** *Let  $\mathcal{O}_\lambda$  be the orbit of a highest weight vector of  $W_\lambda$  (under the complexification  $G(\mathbf{C})$  of  $G(\mathbf{R})$ ). Write  $\overline{\mathcal{O}_\lambda}$  for its Zariski closure in the affine space  $W_\lambda$ . Then the coordinate ring  $\mathbf{C}[\overline{\mathcal{O}_\lambda}]$  of  $\overline{\mathcal{O}_\lambda}$  decomposes under the action of  $G(\mathbf{C})$  into*

$$(2.7) \quad \mathbf{C}[\overline{\mathcal{O}_\lambda}] \cong \bigoplus_{n \geq 0} W_{n\lambda}^*.$$

Here the action of  $g \in G(\mathbf{C})$  on  $\varphi \in \mathbf{C}[\overline{\mathcal{O}_\lambda}]$  is given by  $g\varphi(x) = \varphi(g^{-1}x)$ , for  $x \in \overline{\mathcal{O}_\lambda}$ .

More precisely,  $\overline{\mathcal{O}_\lambda}$  is the zero set of a homogeneous ideal in the affine algebra  $\mathbf{C}[W_\lambda]$ , and hence  $\mathbf{C}[\overline{\mathcal{O}_\lambda}]$  is a graded ring. Then the degree  $n$  part of  $\mathbf{C}[\overline{\mathcal{O}_\lambda}]$  is exactly  $W_{n\lambda}^*$ .

**Proof** See Proposition 2.5 of [BK] and the references cited there. ■

**Proposition 2.8** *Fix a weight  $W_\lambda$  as above. Then:*

1. The direct sum  $R = \bigoplus_{n \geq 0} \mathcal{A}_{W_{n\lambda}}(U)$  is a graded ring under the multiplication defined above.
2. The multiplication in  $R$  can be explicitly seen as follows: as a (graded) vector space,  $R$  is isomorphic to the space of functions  $f: G(\mathbf{Q}) \backslash G(\mathbf{A})/U \rightarrow \mathbf{C}[\overline{\mathcal{O}_\lambda}]$  satisfying (2.2); the grading on  $R$  comes from the grading on  $\mathbf{C}[\overline{\mathcal{O}_\lambda}]$ . Then, for  $f, f' \in R$  and  $g \in G(\mathbf{A})$ ,  $(ff')(g) = f(g)f'(g)$ , where the multiplication on the right is in the ring  $\mathbf{C}[\overline{\mathcal{O}_\lambda}]$ .

3. Let  $g_1, \dots, g_k$  and  $\Gamma_1, \dots, \Gamma_k$  be as in Lemma 2.3. Define the projective variety  $Y_\lambda = \mathbf{Proj} \mathbf{C}[\overline{\mathcal{O}_\lambda}]$ . The variety  $Y_\lambda$  inherits an action of  $G(\mathbf{R})$  from its affine cone  $\overline{\mathcal{O}_\lambda}$ . Then

$$(2.8) \quad \mathbf{Proj} R \cong \bigsqcup_{i=1}^k \Gamma_i \setminus Y_\lambda.$$

**Proof** The first two statements follow immediately from the previous definitions, especially (2.4) and Lemma 2.7. As for the third statement, Lemma 2.3 identifies  $R$  with the product of graded rings  $\bigoplus_{i=1}^k \mathbf{C}[\overline{\mathcal{O}_\lambda}]^{\Gamma_i}$ . Thus  $\mathbf{Proj} R$  is the disjoint union of varieties  $\mathbf{Proj} \mathbf{C}[\overline{\mathcal{O}_\lambda}]^{\Gamma_i}$ , which are just the quotients  $\Gamma_i \setminus Y_\lambda$ . ■

We remark that the above proposition can be generalized to produce rings of automorphic forms with more esoteric gradings. For example, one could turn the direct sum  $\bigoplus_{\text{all } W} \mathcal{A}_W(U)$  into a ring with a grading by the set of all irreducible representations of  $G(\mathbf{R})$ . Analogously to the second assertion of Proposition 2.8, this ring structure would come from a ring structure on  $\bigoplus_{\text{all } W} W$ , which can be viewed as the coordinate ring of a quotient  $G(\mathbf{C})/N$ . (Here  $N$  is the unipotent radical of a Borel subgroup of  $G(\mathbf{C})$ .)

Coming back to the more prosaic graded rings of Lemma 2.7 and Proposition 2.8, we note that  $Y_\lambda$  is a generalized flag manifold associated to the group  $G(\mathbf{C})$ . To see this, let  $w_\lambda \in W_\lambda$  be a highest weight vector of  $W_\lambda$ , with respect to a system of positive roots for  $G(\mathbf{C})$ ; then  $Y_\lambda$  is the quotient  $G(\mathbf{C})/P_\lambda$ , where  $P_\lambda$  is the parabolic subgroup of  $G(\mathbf{C})$  consisting of elements stabilizing the line  $\mathbf{C}w_\lambda$ . For “generic”  $\lambda$  (i.e.,  $\lambda$  not on a wall of the Weyl chamber),  $P_\lambda$  is the Borel subgroup of  $G(\mathbf{C})$  associated to our choice of positive roots. In that case,  $Y_\lambda$  is the usual flag variety, and we can construct the variety  $\mathbf{Proj} R$  in a more concrete way, that does not depend on the choice of generic  $\lambda$ . This is reminiscent of the construction of modular varieties and more general Shimura varieties, except that here we take a quotient by a compact real torus instead of by a maximal compact subgroup of  $G(\mathbf{R})$ .

**Definition 2.9** Let  $T(\mathbf{R})$  be a maximal torus of  $G(\mathbf{R})$ , and define  $Y = G(\mathbf{R})/T(\mathbf{R})$ . Recall that  $Y$  is isomorphic to the flag variety of  $G(\mathbf{C})$ , and is in particular a complex manifold. Also define

$$(2.9) \quad X(U) = G(\mathbf{Q}) \setminus G(\mathbf{A})/UT(\mathbf{R}).$$

**Proposition 2.10** Define  $g_i$  and  $\Gamma_i$  as in Lemma 2.3, and let  $R$  be the graded ring of automorphic forms defined in Proposition 2.8. Assume that  $\lambda$  in that proposition is generic in the sense of the discussion preceding Definition 2.9. Then

$$(2.10) \quad X(U) \cong \bigsqcup_{i=1}^k \Gamma_i \setminus Y \cong \mathbf{Proj} R.$$

**Proof** Use the decomposition  $G(\mathbf{A}) = \bigsqcup_{i=1}^k G(\mathbf{Q})g_iUG(\mathbf{R})$ . ■

**Remark 2.11** The graded ring  $R$  arises from a natural projective embedding of  $X(U)$ . To see this, use the theorem of Borel-Weil to construct a holomorphic line bundle  $\mathcal{L}_\lambda$  on  $Y$ , such that  $H^0(Y, \mathcal{L}_\lambda)$  is isomorphic to  $W_\lambda^*$ . Let  $\mathcal{L}$  be the corresponding line bundle on the orbifold  $X(U) = \bigsqcup_{i=1}^k \Gamma_i \backslash Y$ . Thus the global sections of  $\mathcal{L}$  on each connected component  $\Gamma_i \backslash Y$  are just  $(W_\lambda^*)^{\Gamma_i}$ . Then we obtain the following corollary of Proposition 2.10.

**Corollary 2.12** *Let  $X(U)$  and  $\mathcal{L}$  be as above, assuming that  $\lambda$  is generic in the sense used above. Then  $\mathcal{L}$  is very ample on  $X(U)$ , and defines the projective embedding of  $X(U)$  associated to the graded ring  $\bigoplus_{n \geq 0} \mathcal{A}_{W_{n\lambda}}(U)$ .*

**Proof** This is just saying that the space of global sections  $H^0(X(U), \mathcal{L}^{\otimes n})$  is isomorphic to  $\bigoplus_{i=1}^k (W_{n\lambda}^*)^{\Gamma_i}$ , and hence to  $\mathcal{A}_{W_{n\lambda}}(U)$ . We incidentally remark that even if  $\lambda$  is not generic, one can still obtain the  $\mathcal{A}_{W_{n\lambda}}(U)$  as global sections of  $\mathcal{L}^{\otimes n}$ , for a possibly nonample  $\mathcal{L}$ . ■

We now show that  $X(U)$  can be defined over  $\mathbf{Q}$ . Interestingly, one does not need to pass to a larger number field. The point is that if  $W$  comes from a rational representation of  $G(\mathbf{Q})$ , then  $\mathcal{A}_W(U)$  has a rational structure. This observation is due to B. Gross in [G2]. We shall see later in this article that it seems nontrivial to get number-theoretic information out of this rational structure.

**Definition 2.13** Let  $W_{\mathbf{Q}}$  be an absolutely irreducible rational representation of  $G(\mathbf{Q})$ . View  $W_{\mathbf{Q}}$  as a subset of its complexification  $W = W_{\mathbf{Q}} \otimes_{\mathbf{Q}} \mathbf{C}$ . Further view forms in  $\mathcal{A}_W(U)$  as functions from  $G(\mathbf{Q}) \backslash G(\mathbf{A})/U$  to  $W^*$ . Then define the space  $\mathcal{A}_W(U, \mathbf{Q})$  of  $\mathbf{Q}$ -rational forms in  $\mathcal{A}_W(U)$  by

$$(2.11) \quad \mathcal{A}_W(U, \mathbf{Q}) = \{f \in \mathcal{A}_W(U) \mid f(g) \in W_{\mathbf{Q}}^* \text{ for } g \in G(\mathbf{A}_f)\}.$$

One actually only needs to check that  $f(g_1), \dots, f(g_k) \in W_{\mathbf{Q}}^*$  for the elements  $g_i \in G(\mathbf{A}_f)$  defined in Lemma 2.3. It is clear that

$$(2.12) \quad \mathcal{A}_W(U, \mathbf{Q}) \cong \bigoplus_{i=1}^k (W_{\mathbf{Q}}^*)^{\Gamma_i}.$$

(The action of  $\Gamma_i$  on  $W_{\mathbf{Q}}^*$  is well-defined, as  $\Gamma_i \subset G(\mathbf{Q})$ .)

**Proposition 2.14** *In the situation of Definition 2.13, assume furthermore that  $W = W_\lambda$  with a highest weight  $\lambda$  that is generic in the sense used before.<sup>1</sup> Then  $R_{\mathbf{Q}} = \bigoplus_{n \geq 0} \mathcal{A}_{W_{n\lambda}}(U, \mathbf{Q})$  is a graded ring, and  $\mathbf{Proj} R_{\mathbf{Q}}$  is a model for  $X(U)$  defined over  $\mathbf{Q}$ .*

<sup>1</sup>Such a  $W_{\mathbf{Q}}$  exists. For instance, let  $G$  have  $N$  positive roots, and take  $\lambda = 2\rho$  to be the sum of these positive roots. Then  $W_\lambda$  is a constituent of the  $N$ -th alternating power of the adjoint representation of  $G$ , which is defined over  $\mathbf{Q}$ .

**Proof** This merely amounts to noting that the projection from  $\overline{W_{n\lambda}} \otimes W_{m\lambda}$  to  $W_{(m+n)\lambda}$  is defined over  $\mathbf{Q}$ . Alternatively, one can use the fact that  $\overline{\mathcal{O}_\lambda}$  is a  $\mathbf{Q}$ -rational subvariety of  $W_\lambda$ , whence  $Y_\lambda$  is defined over  $\mathbf{Q}$ . This follows from a theorem of Kostant (Remark 2.6 of [BK]), that states that the ideal defining  $\overline{\mathcal{O}_\lambda}$  is generated by quadratic polynomials that are the complement of the rationally defined subspace  $W_{2\lambda}^*$  of  $\text{Sym}^2 W_\lambda^*$ . ■

Note that  $Y_\lambda$  has no  $\mathbf{Q}$ -rational or even  $\mathbf{R}$ -rational points, despite the fact that it is defined over  $\mathbf{Q}$ . Indeed, the existence of an  $\mathbf{R}$ -rational point of  $Y_\lambda$  would imply the existence of an  $\mathbf{R}$ -rational highest weight vector in  $W_\lambda$ , which is impossible because  $G(\mathbf{R})$  is compact. However, H. Darmon has pointed out to me that the quotients  $\Gamma_i \backslash Y_\lambda$  may well have rational points.

We conclude this section with some remarks on Hecke operators in this formalism. As usual, given  $t \in G(\mathbf{A}_f)$ , we can define the action of the double coset  $UtU$  on  $\mathcal{A}_W(U)$  as follows. Write  $UtU = \bigsqcup_{i=1}^r t_i U$ , with  $t_i \in G(\mathbf{A}_f)$ . Viewing  $f \in \mathcal{A}_W(U)$  as a  $W^*$ -valued function on  $G(\mathbf{Q}) \backslash G(\mathbf{A})/U$ , we define

$$(2.13) \quad f|UtU(g) = \sum_{i=1}^r f(gt_i), \quad \text{for } g \in G(\mathbf{A}).$$

In particular, if  $W$  is the complexification of a rational representation  $W_{\mathbf{Q}}$ , then  $UtU$  actually acts on  $\mathcal{A}_W(U, \mathbf{Q})$ . Moreover, the Hecke operator  $UtU$  comes from a correspondence on  $X(U)$ , in a way that is familiar from the case of modular curves. Namely, let  $U' = U \cap tUt^{-1}$ . Then we define two maps  $p_1, p_2: G(\mathbf{Q}) \backslash G(\mathbf{A})/U' \rightarrow G(\mathbf{Q}) \backslash G(\mathbf{A})/U$  by

$$(2.14) \quad p_1(g) = g, \quad p_2(g) = gt.$$

The map  $g \mapsto (p_1(g), p_2(g))$  induces a map  $X(U') \rightarrow X(U) \times X(U)$ , which is the desired correspondence. Namely,

$$(2.15) \quad f|UtU = p_{1*} p_2^* f,$$

where  $p_2^*$  is the pullback along  $p_2$ , and  $p_{1*}$  is the trace (pushforward) along  $p_1$ . Equation (2.15) makes sense from both perspectives of regarding an automorphic form as a function on  $G(\mathbf{Q}) \backslash G(\mathbf{A})/U$  or as a section of an orbifold line bundle on  $X(U)$ .

### 3 Automorphic Forms on Definite Quaternion Algebras

We now specialize the setup of Section 2 to the case where  $G$  is the inner form of the group  $\text{PGL}(2, \mathbf{Q})$  associated to a definite quaternion algebra  $B$  over  $\mathbf{Q}$ . In other words, for any  $\mathbf{Q}$ -algebra  $A$ ,

$$(3.1) \quad G(A) = (B \otimes_{\mathbf{Q}} A)^\times / A^\times.$$

We shall also have use for the group  $\tilde{G}$  which is the corresponding inner form of  $\text{GL}(2, \mathbf{Q})$ ; *i.e.*,  $\tilde{G}(A) = (B \otimes A)^\times$ . The varieties associated to rings of automorphic

forms on  $G$  are certain curves of genus zero that were first introduced in [G1], which is a convenient source for many of the facts that we state below.

We first specify the  $W_\lambda$ ,  $\overline{\mathcal{O}}_\lambda$ , and  $Y_\lambda$  (in the notation of Section 2) that will be relevant in our case. Since  $B$  is definite,  $G(\mathbf{R}) \cong \mathbf{H}^\times / \mathbf{R}^\times$ , where  $\mathbf{H}$  is the set of Hamilton quaternions. Thus  $G(\mathbf{R}) \cong \mathrm{SU}(2) / \{\pm 1\} \cong \mathrm{SO}(3)$ . For  $n \geq 0$ , write  $W_n = \mathrm{Sym}^n \mathbf{C}^2$ , where  $W_1 = \mathbf{C}^2$  is the standard representation of  $\mathrm{SU}(2)$ . Thus the irreducible representations of  $G(\mathbf{R})$  are the  $W_{2n}$ . We shall take  $W_\lambda$  to be  $W_2$ , which is the three-dimensional adjoint representation of  $G(\mathbf{R})$ ; hence  $W_{n\lambda} = W_{2n}$ . Note that these representations are all self-dual; we shall therefore not distinguish  $W_{2n}$  from  $W_{2n}^*$ . We easily obtain the following proposition.

**Proposition 3.1**

1. The representation  $W_\lambda = W_2$  comes from the rational representation  $W_{\mathbf{Q}}$  of  $G(\mathbf{Q}) = B^\times / \mathbf{Q}^\times$  acting by conjugation on the space  $\{x \in B \mid \mathrm{tr} x = 0\}$ . Here,  $\mathrm{tr} = \mathrm{tr}_{B/\mathbf{Q}}$  is the reduced trace in the quaternion algebra.
2. We can give a rational model for  $\overline{\mathcal{O}}_\lambda$  as follows: for any  $\mathbf{Q}$ -algebra  $A$ ,

$$(3.2) \quad \overline{\mathcal{O}}_\lambda(A) = \{x \in B \otimes_{\mathbf{Q}} A \mid \mathrm{tr} x = 0, N x = 0\},$$

where  $\mathrm{tr}$  and  $N$  are the reduced trace and norm from  $B \otimes_{\mathbf{Q}} A$  to  $A$ . Similarly,

$$(3.3) \quad Y_\lambda(A) = (\overline{\mathcal{O}}_\lambda(A) - 0) / A^\times.$$

3. The corresponding projective variety  $Y_\lambda$  is a Severi-Brauer variety, in that  $Y_\lambda(\mathbf{C}) \cong \mathbf{P}^1(\mathbf{C})$ , but  $Y_\lambda$  has no rational, or even real, points.

**Proof**

1. This is well-known. For instance,  $B$  splits over  $\mathbf{C}$ , so  $W_\lambda$  is the adjoint representation of  $\mathrm{PGL}(2, \mathbf{C})$  on the set of complex matrices of the form  $\begin{pmatrix} a & b \\ c & -a \end{pmatrix}$ .
2. This is also standard. Over  $\mathbf{C}$ , a highest weight vector is  $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ , and its orbit is the set of  $\begin{pmatrix} a & b \\ c & -a \end{pmatrix}$  with  $-a^2 - bc = 0$ .
3. Using (3.2),  $Y_\lambda(\mathbf{R})$  is easily seen to be empty, because  $B$  is definite, whence  $B \otimes_{\mathbf{Q}} \mathbf{R} \cong \mathbf{H}$ , whose norm form is anisotropic. As for  $Y_\lambda(\mathbf{C})$ , note that it is the curve in the projective plane given by  $-a^2 - bc = 0$ , which is just the duple embedding of  $\mathbf{P}^1$  into  $\mathbf{P}^2$ , sending  $[s : t]$  to  $[a : b : c] = [st : s^2 : -t^2]$ . ■

As in Section 2, we can also construct  $Y(\mathbf{C}) = Y_\lambda(\mathbf{C}) = \mathbf{P}^1(\mathbf{C})$  as the quotient  $G(\mathbf{R})/T(\mathbf{R})$ . Viewing  $G(\mathbf{R})$  as  $\mathrm{SU}(2)/\{\pm 1\}$ , we can take  $T(\mathbf{R})$  to be the image of the subgroup of diagonal matrices in  $\mathrm{SU}(2)$ . We note an immediate corollary to the proof of Proposition 3.1.

**Corollary 3.2** *If  $K$  is any field over which  $B$  splits (for example, if  $K$  is an imaginary quadratic field contained in  $B$ ), then  $Y_\lambda(K) \cong \mathbf{P}^1(K)$ .*

We now proceed to apply the formalism of Section 2. Take a “level”  $U \in G(\mathbf{A}_f)$ , and define  $g_1, \dots, g_k$  and  $\Gamma_1, \dots, \Gamma_k$  as in Lemma 2.3. We thus obtain a ring of automorphic forms  $R = \bigoplus_{n \geq 0} \mathcal{A}(W_{2n}, U)$ . We then obtain a curve  $X(U) = \mathbf{Proj} R$ , which is defined over  $\mathbf{Q}$ . We also obtain the following isomorphism, also defined over  $\mathbf{Q}$ :

$$(3.4) \quad X(U) \cong \bigsqcup_{i=1}^k \Gamma_i \backslash Y.$$

In [G1], Gross originally defined  $X(U)$  by (3.2), (3.3), and (3.4), but without introducing a ring of automorphic forms.

Note that  $X(U)(\mathbf{C})$  is the disjoint union of quotients of  $\mathbf{P}^1(\mathbf{C})$  by finite groups; each such quotient is again isomorphic to  $\mathbf{P}^1(\mathbf{C})$ , by Lüroth’s theorem. Some orbifold problems appear due to our having taken quotients by finite groups. Namely, the line bundle  $\mathcal{L}_\lambda$  in Remark 2.11 is  $\mathcal{O}(2)$  on  $\mathbf{P}^1(\mathbf{C})$ , but passing to the quotient by  $\Gamma_i$  introduces certain “corrections” at the fixed points of the action of  $\Gamma_i$ . (This is similar to the situation with elliptic points on modular curves; see Proposition 2.16 of [S]). At any rate, for sufficiently high level (*i.e.*, small  $U$ ), the groups  $\Gamma_i$  are all trivial. Thus, the complexity of  $X(U)$  is more combinatorial than geometric. The combinatorics mainly involve the number  $k$  of connected components of  $X(U)$ , and their interaction with the Hecke correspondences. We shall now rephrase this combinatorial complexity in terms of more classical language, involving orders and Brandt matrices in the quaternion algebra  $B$ . Much of the following is adapted from [G1] and [P].

We first restrict ourselves to a particular kind of  $U$ . Let  $\mathcal{O} \subset B$  be an order;  $\mathcal{O}$  need not be maximal. Then define a level  $\tilde{U}$  in  $\tilde{G}$  by  $\tilde{U} = \prod_p \tilde{U}_p \subset \tilde{G}(\mathbf{A}_f)$ , where  $\tilde{U}_p = \mathcal{O}_p^\times \subset \tilde{G}(\mathbf{Q}_p)$ . Here for convenience we have written  $\mathcal{O}_p$  to mean  $\mathcal{O} \otimes_{\mathbf{Z}} \mathbf{Z}_p$ . Note that  $\tilde{U}$  contains  $\hat{\mathbf{Z}}^\times = \prod_p \mathbf{Z}_p^\times \subset \mathbf{A}_f^\times$ , and in fact  $\tilde{U} = \hat{\mathcal{O}}^\times$ , where  $\hat{\mathcal{O}} = \mathcal{O} \otimes_{\mathbf{Z}} \hat{\mathbf{Z}} = \prod_p \mathcal{O}_p$ . We shall similarly write  $B_p = B \otimes_{\mathbf{Z}} \mathbf{Z}_p$ , and  $\hat{B} = B \otimes_{\mathbf{Z}} \hat{\mathbf{Z}} = B \otimes_{\mathbf{Q}} \mathbf{A}_f$ . Then  $\tilde{G}(\mathbf{Q}_p) = B_p^\times$ , and  $\tilde{G}(\mathbf{A}_f) = \hat{B}^\times$ .

**Definition 3.3** For  $\mathcal{O}$  and  $\tilde{U}$  as above, we define  $U$  to be the projection of  $\tilde{U}$  to  $G(\mathbf{A}_f)$ ; thus  $U = \hat{\mathcal{O}}^\times / \hat{\mathbf{Z}}^\times$ .

We also recall (in stages) the definition of a proper  $\mathcal{O}$ -ideal.

**Definition 3.4**

1. Let  $L \subset B$  be a lattice; *i.e.*,  $L \cong \mathbf{Z}^4$ . Given  $\hat{x} \in \hat{B}^\times$ , define  $\hat{x}L \subset B$  to be the unique lattice such that  $(\hat{x}L)_p = \hat{x}_p L_p \subset B_p$  for all  $p$ . Here  $\hat{x}_p$  is the projection of  $\hat{x}$  to  $B_p^\times$ . Similarly define  $L\hat{x}$ . Typically,  $L$  will be a left or right ideal for  $\mathcal{O}$ .
2. A proper  $\mathcal{O}$ -ideal  $I \subset B$  will be a lattice of the form  $I = \hat{x}\mathcal{O}$ , where  $\hat{x} \in \hat{B}^\times$ . Thus  $I$  is a (possibly fractional) right  $\mathcal{O}$ -ideal, such that  $\mathcal{O} = \{x \in B \mid Ix \subset I\}$ .
3. The left order of a proper  $\mathcal{O}$ -ideal  $I$  is  $\mathcal{O}' = \{x \in B \mid xI \subset I\}$ . Thus if  $I = \hat{x}\mathcal{O}$ , then  $\mathcal{O}' = \hat{x}\mathcal{O}\hat{x}^{-1}$  in the sense of part 1 of this definition.

4. Two proper  $\mathcal{O}$ -ideals  $I$  and  $J$  are said to be equivalent iff there exists  $x \in B^\times$  with  $J = xI$ . The left ideals of  $I$  and  $J$  are then conjugate by an element of  $B^\times$ .
5. Note that the equivalence classes of proper  $\mathcal{O}$ -ideals are parametrized by the double cosets of  $B^\times \backslash \hat{B}^\times / \hat{\mathcal{O}}^\times$ . Namely, the double coset  $B^\times \hat{x} \hat{\mathcal{O}}^\times$  corresponds to the equivalence class of the ideal  $\hat{x}\mathcal{O}$ .

Henceforth an ideal in  $B$  will always mean a proper (possibly fractional) right  $\mathcal{O}$ -ideal, unless otherwise mentioned.

**Lemma 3.5** *Let  $\mathcal{O}$ ,  $U$ , and  $\tilde{U}$  be as above. Then the set of equivalence classes of  $\mathcal{O}$ -ideals is canonically in bijection with  $G(\mathbf{Q})_f \backslash G(\mathbf{A}_f)/U$ .*

**Proof** Use the facts that  $\mathbf{A}_f^\times = (\mathbf{Q}^\times)_f \hat{\mathbf{Z}}^\times$ , and that  $\tilde{U}$  contains  $\hat{\mathbf{Z}}^\times$ . Then  $G(\mathbf{Q})_f \backslash G(\mathbf{A}_f)/U$  can be identified with  $\tilde{G}(\mathbf{Q})_f \backslash \tilde{G}(\mathbf{A}_f)/\tilde{U}$ , which is just the double coset space  $B^\times \backslash \hat{B}^\times / \hat{\mathcal{O}}^\times$ . ■

**Lemma 3.6** *In the situation of Lemma 3.5, choose representatives  $\hat{x}_1, \dots, \hat{x}_k \in \hat{B}^\times$  for the double cosets in  $B^\times \backslash \hat{B}^\times / \hat{\mathcal{O}}^\times$ . Thus the ideals  $I_i = \hat{x}_i \mathcal{O}$ , for  $1 \leq i \leq k$ , are a set of representatives for the classes of ideals in  $B$ . Define  $\tilde{\Gamma}_i = B^\times \cap \hat{x}_i \tilde{U} \hat{x}_i^{-1} \subset \tilde{G}(\mathbf{Q})$ , analogously to Lemma 2.3. Then:*

1. The finite group  $\tilde{\Gamma}_i$  is the group of units in the left order of  $I_i$ . Explicitly,  $\tilde{\Gamma}_i = \{x \in B^\times \mid xI_i = I_i\}$ .
2. Let  $g_i$  be the projection of  $\hat{x}_i$  to  $G(\mathbf{A}_f)$ . Then the corresponding  $\Gamma_i$ , in the notation of Lemma 2.3, is the projection of  $\tilde{\Gamma}_i$  to  $G(\mathbf{Q})$ . Thus  $\Gamma_i = \tilde{\Gamma}_i / \{\pm 1\}$ .

**Proof** Easy. ■

We now turn to Hecke operators. For almost all  $p$ ,  $B$  and  $\mathcal{O}$  are unramified at  $p$ ; this means that there exists an isomorphism  $B_p \cong M(2, \mathbf{Q}_p)$ , so that  $\mathcal{O}_p$  corresponds to  $M(2, \mathbf{Z}_p)$ . Let  $t_p \in \mathcal{O}_p$  correspond to the matrix  $\begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix} \in M(2, \mathbf{Z}_p)$ . We can view  $t_p$  as an element of  $\tilde{G}(\mathbf{Q}_p) \subset \tilde{G}(\mathbf{A}_f)$ , or by projection as an element of  $G(\mathbf{Q}_p) \subset G(\mathbf{A}_f)$ .

**Definition 3.7** Let  $B$  and  $\mathcal{O}$  be unramified at  $p$ , as above.

1. Define the Hecke operator  $T_p$  by the double coset  $Ut_pU$ . As the following proposition shows, this definition is independent of the choice of isomorphism  $B_p \cong M(2, \mathbf{Q}_p)$ .
2. Let  $T_p$  be as above, and choose  $g_1, \dots, g_k$  as in Lemma 3.6. Identify  $f \in \mathcal{A}(W_{2n}, U)$  with the tuple  $(f(g_i))_{i=1}^k \in \bigoplus_{i=1}^k W_{2n}^{\Gamma_i}$ . View such a tuple as a column “vector” whose  $i$ -th component is an element of  $W_{2n}^{\Gamma_i}$ . Write the action of  $T_p$  on  $\mathcal{A}(W_{2n}, U)$  as a matrix  $B_{p,n} = (b_{ij})_{i,j=1}^k$ , where  $b_{ij} \in \text{Hom}_{\mathbf{C}}(W_{2n}^{\Gamma_j}, W_{2n}^{\Gamma_i})$ . One calls  $B_{p,n}$  a Brandt matrix.

**Proposition 3.8** *The entries  $b_{ij}$  of  $B_{p,n}$  are given as follows: let  $I_1, \dots, I_k$  be, as in Lemma 3.6, representatives of the ideal classes of  $\mathcal{O}$ , compatible with our previous choice of  $g_1, \dots, g_k$ . To calculate  $b_{ij}$ , enumerate the subideals  $L_\nu \subset I_i$  satisfying the following conditions:*

1.  $I_i/L_\nu \cong (\mathbf{Z}/p\mathbf{Z})^2$ ,
2.  $L_\nu$  is in the same class as  $I_j$ ; so  $L_\nu = \gamma_\nu I_j$  for some  $\gamma_\nu \in B^\times$ .

Then, for  $w \in W_{2n}^j$ ,

$$(3.5) \quad b_{ij}(w) = \sum_{\text{all } \nu \text{ as above}} \gamma_\nu w.$$

Note that  $\gamma_\nu w$  is well-defined, and that  $\sum_\nu \gamma_\nu w \in W_{2n}^i$ , because left multiplication by a unit of  $\mathcal{O}_i$  permutes the  $L_\nu$ 's. More prosaically,  $\{\gamma_\nu\}$  are a set of representatives of the orbits of  $\mathcal{O}_j^\times$ , acting by right multiplication on the set

$$(3.6) \quad \{\gamma \in I_i I_j^{-1} \mid N(\gamma) = p N(I_i)/N(I_j)\}.$$

**Proof** This is standard; compare with Definition 2.13 of [P]. Essentially, define  $f \in \mathcal{A}(W_{2n}, U)$  by  $f(g_j) = w$  and  $f(g_{j'}) = 0$  for  $j' \neq j$ ; then  $b_{ij}(w) = (T_p f)(g_i)$ . To compute this last quantity, think of  $f$  as a function on  $\tilde{G}(\mathbf{Q}) \backslash \tilde{G}(\mathbf{A})/\tilde{U}$ , invariant under the center  $\mathbf{A}^\times$ . The operator  $T_p$  then acts via the double coset  $\tilde{U} t_p \tilde{U} = \bigsqcup_\nu t_\nu \tilde{U}$ , and we must evaluate

$$(3.7) \quad b_{ij}(w) = (T_p f)(\hat{x}_i) = \sum_\nu f(\hat{x}_i t_\nu).$$

The point is that the collection of ideals  $L_\nu$ , where  $L_\nu = \hat{x}_i t_\nu \mathcal{O}$ , ranges over all subideals of  $I_i = \hat{x}_i \mathcal{O}$ , with  $I_i/L_\nu \cong (\mathbf{Z}/p\mathbf{Z})^2$ . Only the ideals  $L_\nu$  which are in the same class as  $I_j$  contribute nonzero terms to the sum in (3.7). ■

As is well known, the Hecke operators  $T_p$  (which we are only considering for those  $p$  where  $B$  and  $\mathcal{O}$  are unramified) can be simultaneously diagonalized on  $\mathcal{A}(W_{2n}, U)$ . Furthermore, the Jacquet-Langlands correspondence (which originated in the setting of definite quaternion algebras with Eichler and Shimizu) implies that if  $f \in \mathcal{A}(W_{2n}, U)$  is a simultaneous eigenform of all  $T_p$ 's, then there exists a classical modular form  $\tilde{f}$  (of weight  $2n + 2$ ) on  $\text{GL}(2)$ , with the same Hecke eigenvalues as  $f$ . One can then pass to the Galois representation attached to  $\tilde{f}$  to obtain the following well-known theorem.

**Theorem 3.9** *Given  $f \in \mathcal{A}(W_{2n}, U)$  that is a simultaneous eigenform of all  $T_p$ 's, with  $T_p f = \lambda_p f$ , and given a prime  $\ell$ , there exists a representation  $\rho_{f,\ell}: \text{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \rightarrow \text{GL}(2, \overline{\mathbf{Q}}_\ell)$ , with the property that for almost every  $p$ ,  $\rho_{f,\ell}(\text{Frob } p)$  has characteristic polynomial  $x^2 - p^n \lambda_p x + p^{2n+1}$ . Here  $\text{Frob } p$  is a Frobenius element at  $p$ . The factor of  $p^n$  is due to our choice of normalization for the Hecke operators.*

This theorem suggests the following question: is there some way to produce the representation  $\rho_{f,\ell}$  directly from  $f$ , without using the Jacquet-Langlands correspondence to first pass to a form  $\tilde{f}$  on  $\mathrm{GL}(2)$ ? This author is not aware of any such way. However, the curve  $X(U)$  has certain features, analogous to some of those features of a “classical” modular curve that play an essential role in the passage from a “classical” modular form  $\rho_{f,\ell}$  to a Galois representation. The rest of this paper is a discussion of these features of  $X(U)$  that are analogous to features of a modular curve.

The first feature is that a modular curve is in fact defined over a number field (frequently over  $\mathbf{Q}$ ), and hence one can get Galois representations on appropriate étale cohomology groups ( $H^1$ ) of modular curves. This feature carries over partially to  $X(U)$ . As we have seen,  $X(U)$  is indeed defined over  $\mathbf{Q}$ , but its interesting arithmetic information is almost entirely encoded in its connected components, *i.e.*, by  $H^0$ . However,  $H^0(X(U))$  does not have an interesting Galois action. The  $\mathbf{Q}$ -rational structure on  $X(U)$  may in some sense be the wrong one.

The second feature of a modular curve is that it is in fact a moduli space (for elliptic curves with extra structure, as is well-known), whence one can understand the reduction modulo  $p$  of a modular curve  $X'$  by reducing the corresponding moduli problem modulo  $p$ . This yields information about the Galois action of a Frobenius element  $\mathrm{Frob} p$  on a suitable  $H^1(X')$ , and in fact the Eichler-Shimura congruence relates the  $p$ -th Hecke operator on  $X'$  to  $\mathrm{Frob} p$ . In the case of  $X(U)$ , we shall interpret the complex points of  $X(U)$  as parametrizing certain complex tori that are generally not abelian varieties. Thus  $X(U)$  is not a moduli space in the usual sense, and it is not clear what the reduction of  $X(U)$  modulo  $p$  should be. Nonetheless, some of the complex points of  $X(U)$  are analogous to “CM-points” and do indeed correspond to abelian varieties. For these points, we shall indeed prove an analog of the Eichler-Shimura congruence.

#### 4 Complex Tori with Quaternionic Endomorphisms

As promised at the end of Section 3, we now interpret the complex points of  $X(U)$  as a kind of moduli space that does not parametrize algebraic objects. We keep the notation and assumptions of Section 3.

**Definition 4.1** A two-dimensional complex torus with a proper  $\mathcal{O}$ -action is a complex torus  $A \cong \mathbf{C}^2/L$  such that  $\mathcal{O}$  acts on  $A$  on the right by holomorphic endomorphisms, in such a way that  $L$  is isomorphic to a proper  $\mathcal{O}$ -ideal. Explicitly, this means that the action of  $\mathcal{O}$  on  $A$  is given by an (injective) homomorphism  $i: \mathcal{O} \rightarrow M(2, \mathbf{C})$ , such that:

1. For  $\gamma \in \mathcal{O}$ ,  $L \cdot i(\gamma) \subset L$ . (Here we view elements of  $\mathbf{C}^2$  as row vectors.) The homomorphism  $i$  gives us the action of  $\mathcal{O}$  on  $A$ .
2. The structure of right  $\mathcal{O}$ -module that is induced on  $L$  makes  $L$  isomorphic to a proper right  $\mathcal{O}$ -ideal.

In anticipation of the following proposition, fix an element  $J_0 \in B_{\mathbf{R}} \cong \mathbf{H}$  such that  $J_0^2 = -1$ . Left multiplication by  $J_0$  is thus a complex structure on  $B_{\mathbf{R}}$ , and right

multiplication by an element of  $B_{\mathbf{R}}$  is linear with respect to this complex structure. Our choice of  $J_0$  also defines a choice of maximal torus  $\tilde{T}(\mathbf{R}) \subset \tilde{G}(\mathbf{R})$ , namely the centralizer of the regular semisimple element  $J_0$ . Let  $T(\mathbf{R})$  be the projection of  $\tilde{T}(\mathbf{R})$  to  $G(\mathbf{R})$ ; it is a (one-dimensional) maximal torus of  $G(\mathbf{R})$ .

**Proposition 4.2** *The complex points of  $X(U)$  parametrize the isomorphism classes of two-dimensional complex tori with a proper  $\mathcal{O}$ -action on the right.*

**Proof** Let  $x \in X(U) \cong G(\mathbf{Q}) \backslash G(\mathbf{A})/UT(\mathbf{R}) \cong \tilde{G}(\mathbf{Q}) \backslash \tilde{G}(\mathbf{A})/\tilde{U}\tilde{T}(\mathbf{R})$ . (Here the second isomorphism follows from the fact that  $\mathbf{A}^\times = \mathbf{Q}^\times \hat{\mathbf{Z}}^\times \mathbf{R}^\times$ .) This last double coset space is  $B^\times \backslash (\hat{B}^\times \times B_{\mathbf{R}}^\times)/\hat{\mathcal{O}}^\times \tilde{T}(\mathbf{R})$ ; thus, pick a representative for  $x$  and write, by abuse of notation,  $x = \hat{x}x_{\mathbf{R}}$  with  $\hat{x} \in \hat{B}^\times$  and  $x_{\mathbf{R}} \in B_{\mathbf{R}}^\times$ . If we like, we may assume that  $\hat{x}$  is one of the representatives of  $B^\times \backslash \hat{B}^\times/\hat{\mathcal{O}}^\times$  chosen in Lemma 3.6, so  $x = \hat{x}_i$  for some  $i$ .

The point  $x$  then corresponds to the complex torus  $A_x = B_{\mathbf{R}}/\hat{x}\mathcal{O}$ , where the complex structure on  $B_{\mathbf{R}}$  is given by left multiplication by  $J_x = x_{\mathbf{R}}J_0x_{\mathbf{R}}^{-1}$ . Note that if  $\hat{x} = \hat{x}_i$ , then the lattice  $\hat{x}\mathcal{O}$  is the ideal  $I_i$ . The action of  $\mathcal{O}$  on  $A_x$  arises from right multiplication on  $B_{\mathbf{R}}$  (which preserves  $\hat{x}\mathcal{O}$ ), and this action commutes with the action of  $J_x$ , whence this action is holomorphic. We now show that the isomorphism class of  $A_x$  depends only on the class of  $x$  in the double coset space. On the one hand, right multiplying  $x$  by an element of  $\hat{\mathcal{O}}^\times \tilde{T}(\mathbf{R})$  does not change  $A_x$  at all. On the other hand, left multiplying  $x$  by an element  $\gamma \in B^\times$  gives rise to an isomorphism of complex tori with endomorphisms by  $\mathcal{O}$ :

$$(4.1) \quad A_{\gamma x} = B_{\mathbf{R}}/\gamma\hat{x}\mathcal{O} \xrightarrow{\gamma \cdot} B_{\mathbf{R}}/\hat{x}\mathcal{O} = A_x,$$

where the complex structure on  $A_{\gamma x}$  is given by  $J_{\gamma x} = \gamma J_x \gamma^{-1}$ , and the map indicated by  $\gamma \cdot$  is left multiplication by  $\gamma$  on  $B_{\mathbf{R}}$ .

Conversely, every complex torus with a proper  $\mathcal{O}$ -action arises in this way, for a unique double coset  $B^\times x \hat{\mathcal{O}}^\times \tilde{T}(\mathbf{R})$ . ■

**Remark 4.3** We have chosen to parametrize complex structures on  $B_{\mathbf{R}}$  as conjugates of  $J_0$  by elements of  $\tilde{G}(\mathbf{R})/\tilde{T}(\mathbf{R})$ . As usual, one can eliminate the choice of  $J_0$  and  $T(\mathbf{R})$  by viewing a complex structure as a homomorphism from  $\mathbf{C}$  to  $B_{\mathbf{R}}$ . This identifies  $\mathbf{P}^1(\mathbf{C})$  with  $\text{Hom}(\mathbf{C}, B_{\mathbf{R}})$ , instead of with  $G(\mathbf{R})/T(\mathbf{R})$ . This latter identification is more canonical and will be taken up again in Proposition 4.12.

**Remark 4.4** As seen in Section 3, the connected components of  $X(U)$  correspond to the different ideal classes  $I_1, \dots, I_k$  of  $\mathcal{O}$ . In terms of the moduli space interpretation of Proposition 4.2, each connected component parametrizes tori  $\mathbf{C}^2/L$ , where  $L$  is isomorphic to a particular  $I_i$ . Furthermore, the connected component corresponding to  $I_i$  is isomorphic to  $\tilde{\Gamma}_i \backslash \mathbf{P}^1(\mathbf{C})$ , with  $\tilde{\Gamma}_i$  as in Lemma 3.6. Points on this connected component correspond to different complex structures on  $B_{\mathbf{R}}/I_i$ , by a correspondence virtually identical to that in Proposition 4.2. Namely, an element of  $\mathbf{P}^1(\mathbf{C})$  gives a complex structure on  $B_{\mathbf{R}}$ , and hence on  $B_{\mathbf{R}}/I_i$ . If two such complex structures differ by the action of an element  $\gamma \in \tilde{\Gamma}_i = \mathcal{O}_i^\times$ , this gives rise to an

isomorphism between the two different complex structures on  $B_{\mathbf{R}}/I_i$ , analogously to (4.1).

**Remark 4.5** An analog of the construction in Proposition 4.2 works even if  $B$  is an indefinite quaternion algebra. In that case one obtains the standard construction and moduli interpretation of Shimura curves. An interesting case is when  $B = M(2, \mathbf{Q})$  is split, and  $\mathcal{O} = \left\{ \begin{pmatrix} a & b \\ Nc & d \end{pmatrix} \mid a, b, c, d \in \mathbf{Z} \right\}$ . This yields the modular curve  $X_0(N)$  as a parameter space for complex tori with an action of  $\mathcal{O}$ . It turns out that such tori have the form  $E \times E'$ , where  $E$  and  $E'$  are elliptic curves with a cyclic  $N$ -isogeny between them, thereby recovering the usual moduli interpretation of  $X_0(N)$ . In the case of Shimura curves, the complex tori that they parametrize all end up being abelian varieties, in contrast to the situation with the curves  $X(U)$ ; see Proposition 4.9 below.

We now describe the “moduli” interpretation of the Hecke operator  $T_p$  on  $X(U)$ . As before, we assume that  $B$  and  $\mathcal{O}$  are unramified at  $p$ . It is most convenient to view  $T_p$  as a correspondence, or, in other words, as a multiple-valued function: given  $x \in X(U)$ ,  $T_p x$  will be a formal sum of  $(p + 1)$  points on  $X(U)$ . (The number  $p + 1$  is the degree of the correspondence  $T_p$ , namely the number  $r$  in (2.13), or the degree of the map  $p_1$  in (2.14).)

**Proposition 4.6** *Let  $x \in X(U)$  correspond to  $A = A_x$ , which we view as  $\mathbf{C}^2/L$ . Then  $T_p x$  is the formal sum of the points  $x_\nu$ , corresponding to tori  $\mathbf{C}^2/L_\nu$ , where  $L_\nu$  ranges over all  $\mathcal{O}$ -submodules of  $L$  such that  $L/L_\nu \cong (\mathbf{Z}/p\mathbf{Z})^2$ . In other words, the  $x_\nu$  correspond to complex tori  $A_\nu$  with an  $\mathcal{O}$ -equivariant isogeny  $A_\nu \rightarrow A$ , whose kernel is isomorphic to  $(\mathbf{Z}/p\mathbf{Z})^2$ .*

**Proof** Take a representative  $x = \hat{x}x_{\mathbf{R}}$  as above, thus identifying  $L$  with  $\hat{x}\mathcal{O}$ . The double coset defining  $T_p$  is  $\tilde{U}t_p\tilde{U} = \bigsqcup_{\nu} t_\nu\tilde{U}$ , and the desired points  $A_\nu$  are represented by  $x_\nu = \hat{x}t_\nu x_{\mathbf{R}}$ . Thus  $A_\nu = B_{\mathbf{R}}/L_\nu$  where  $L_\nu = \hat{x}t_\nu\mathcal{O}$  (the complex structure on  $B_{\mathbf{R}}$  is given by  $x_{\mathbf{R}}$ , and is the same as for  $A$ ). But we have seen in the proof of Proposition 3.8 that the  $L_\nu$  range over the subideals of  $L$  such that  $L/L_\nu \cong (\mathbf{Z}/p\mathbf{Z})^2$ . ■

**Remark 4.7** Such subideals  $L_\nu$  satisfy  $pL \subset L_\nu \subset L$ . View  $L_\nu/pL$  as an  $\mathcal{O}$ -submodule of  $L/pL$ ; one sees that  $L_\nu/pL$  is also isomorphic to  $(\mathbf{Z}/p\mathbf{Z})^2$ . Now  $L/pL$  is a right module over  $\mathcal{O}/p\mathcal{O}$ , and  $L$  is locally free of rank one over  $\mathcal{O}$ , so  $L/pL \cong \mathcal{O}/p\mathcal{O}$  as an  $\mathcal{O}/p\mathcal{O}$ -module (e.g., pass to the completion at  $p$ ). Moreover,  $\mathcal{O}/p\mathcal{O} \cong M(2, \mathbf{Z}/p\mathbf{Z})$ , since  $\mathcal{O}_p \cong M(2, \mathbf{Z}_p)$ . Thus, the  $L_\nu$  that we want to enumerate correspond to right ideals of  $M(2, \mathbf{Z}/p\mathbf{Z})$  that are two-dimensional over  $\mathbf{Z}/p\mathbf{Z}$ . These right ideals have the form  $L_{(a,b)} = \left\{ \begin{pmatrix} a & b \\ x & y \end{pmatrix} \mid x, y \in \mathbf{Z}/p\mathbf{Z} \right\}$ , and the map associating  $L_{(a,b)}$  to  $(a : b) \in \mathbf{P}^1(\mathbf{Z}/p\mathbf{Z})$  is a bijection.

We also remark that we can list the complex tori  $A_\nu$  as being obtained in the following way:

**Proposition 4.8** *Let  $A[p] = \{a \in A \mid pa = 0\}$  be the group of  $p$ -torsion points of  $A$ . Then  $\mathcal{O}/p\mathcal{O}$  acts on  $A[p]$ , and the situation is isomorphic to having  $M(2, \mathbf{Z}/p\mathbf{Z})$  act on*

$M(2, \mathbf{Z}/p\mathbf{Z})$  by right multiplication. Let  $\{C_\nu\}_\nu$  list the  $\mathcal{O}$ -submodules of  $A[p]$  such that  $C_\nu \cong (\mathbf{Z}/p\mathbf{Z})^2$ ; the  $C_\nu$  are enumerated essentially by the same  $L_{(a,b)}$  as in Remark 4.7. Then the  $A_\nu$  of Proposition 4.6 are the quotients  $A/C_\nu$ .

**Proof** Instead of taking  $A_\nu = B_{\mathbf{R}}/L_\nu$  as in Remark 4.7, we take the isomorphic complex torus  $A_\nu = B_{\mathbf{R}}/p^{-1}L_\nu$ , which is now a quotient of  $A$  by precisely a subgroup  $C_\nu$  of  $A[p]$  as above. ■

We now turn to the question of when a complex torus  $A$  with a proper  $\mathcal{O}$ -action is actually an abelian variety. A special case of a theorem by Shimura implies that only those  $A$  that have “complex multiplication” are abelian varieties.

**Proposition 4.9** *Let  $A = \mathbf{C}^2/L$  have a right action of  $\mathcal{O}$  by holomorphic endomorphisms. Then  $A$  is an abelian variety if and only if it is isogenous to  $E \times E$ , where  $E$  is an elliptic curve with complex multiplication by an imaginary quadratic field  $K$  that splits  $B$ . In other words,  $B \otimes_{\mathbf{Q}} K \cong M(2, K) \cong (\text{End } A) \otimes_{\mathbf{Z}} \mathbf{Q}$ . Viewing  $A$  as  $B_{\mathbf{R}}/L$  for an  $\mathcal{O}$ -ideal  $L$ , such an  $A$  is an abelian variety if and only if the complex structure  $J$  is left multiplication by an element of  $B_{\mathbf{R}}$  of the form  $J = \zeta/(\mathbf{N} \zeta)^{1/2}$ , where  $\zeta \in B^\times$  satisfies  $\text{tr } \zeta = 0$ . (The symbols  $\mathbf{N}$  and  $\text{tr}$  denote the reduced trace and norm from  $B$  to  $\mathbf{Q}$ .) In that case,  $K = \mathbf{Q}(\zeta)$ , and the complex structure on  $B_{\mathbf{R}}$  is inherited from the  $K$ -vector space structure on  $B$ , where  $K$  acts on  $B$  by left multiplication.*

**Proof** This is a special case of [S2, Proposition 15]. For the reader’s convenience, we sketch the proof. View  $A$  as  $B_{\mathbf{R}}/L$  with a complex structure  $J$ , where  $L$  is a lattice in  $B$  (hence  $L$  is commensurable with  $\mathcal{O}$ ). The complex torus  $A$  is an abelian variety iff we can find a skew-symmetric form  $E: B_{\mathbf{R}} \times B_{\mathbf{R}} \rightarrow \mathbf{R}$ , such that

1.  $E(\gamma, \delta) \in \mathbf{Z}$  if  $\gamma, \delta \in L$ ,
2.  $E(Jx, x)$  is a positive definite quadratic form,
3.  $E(Jx, Jy) = E(x, y)$  for  $x, y \in B_{\mathbf{R}}$ .

Now skew-symmetric forms on  $B_{\mathbf{R}}$  are of the form  $E(x, y) = \text{tr}(\eta \bar{x}y - \zeta x \bar{y})$ , where  $\eta, \zeta \in B_{\mathbf{R}}$  have trace 0, and  $\bar{x}$  is the conjugate of  $x \in B_{\mathbf{R}}$ . Condition 1 implies that  $\eta, \zeta \in B$  and are “sufficiently integral.” Condition 2 both forces  $\zeta \neq 0$ , and requires  $\text{tr}(-\zeta J)$  to be a sufficiently large positive number, so that the term  $\text{tr}(-\zeta Jx \bar{x})$  can overcome the contribution of the indefinite term  $\text{tr}(-\eta \bar{x}Jx)$ . Condition 3 forces  $J$  to commute with  $\zeta$ ; since  $\zeta \neq 0$ ,  $J$  must belong to  $\mathbf{R}(\zeta)$ , which is a copy of  $\mathbf{C}$  inside  $B_{\mathbf{R}}$ . Since  $\text{tr } J = \text{tr } \zeta = 0$  and  $\mathbf{N} J = 1$ , we conclude that  $J = \zeta/(\mathbf{N} \zeta)^{1/2}$ . Furthermore,  $K = \mathbf{Q}(\zeta)$  splits  $B$  because it is a maximal subfield of  $B$ . Letting  $K$  act on  $B$  by left multiplication, we see that  $B$  is isomorphic to  $K^2$  as a  $K$ -vector space. This isomorphism gives rise to an isomorphism  $B_{\mathbf{R}} \cong \mathbf{C}^2$ , compatible with the complex structure induced by  $J$ . Let  $\mathcal{O}_K$  be the ring of integers of  $K$ . The lattice  $L \subset B$  is commensurable with the lattice corresponding to  $\mathcal{O}_K \oplus \mathcal{O}_K \subset K^2 \cong B$ , and therefore our torus  $B_{\mathbf{R}}/L$  is isogenous to  $E \times E$ , where  $E$  is the CM elliptic curve  $\mathbf{C}/\mathcal{O}_K$ . ■

**Definition 4.10** We call a CM-point of  $X(U)$  any point  $x \in X(U)$  corresponding to an abelian variety as described in Proposition 4.9. We also call the  $K$  in that proposition the CM-field of  $x$ .

**Remark 4.11** A CM-point  $x \in X(U)$  also comes with a specific identification of  $K$  as a subfield of  $\mathbf{C}$ , i.e., with a CM-type of  $K$ . Namely, the choice of  $J \in B_{\mathbf{R}}$  gives an embedding of  $\mathbf{R}$ -algebras  $q: \mathbf{C} \rightarrow B_{\mathbf{R}}$ , with  $q(i) = J$ ; then  $K = B \cap q(\mathbf{C})$ , and  $q$  induces an embedding of  $K$  into  $\mathbf{C}$ .

**Proposition 4.12** *The CM-points of  $X(U)$  with CM-field  $K$  are precisely the points that are defined over  $K$ .*

**Proof** Here we must reexpress  $X(U)$  (and the complex tori it parametrizes) in a way that does not involve a choice of  $J_0$  or even of  $T(\mathbf{R})$ ; rather, we must capture the way in which  $X(U)$  is defined over  $\mathbf{Q}$ . We do this separately on each connected component of  $X(U)$ , following the method on page 131 of [G1]. The connected component corresponding to  $I_i$  is then  $\Gamma_i \backslash Y$  (see (3.4)). This component parametrizes complex structures  $J$  on  $B_{\mathbf{R}}$ , or rather on  $B_{\mathbf{R}}/I_i$ , up to replacing  $J$  by  $\gamma J \gamma^{-1}$  with  $\gamma \in \Gamma_i = \mathcal{O}_i^{\times} / \{\pm 1\}$ . This parametrization arises through a  $G(\mathbf{R})$ -equivariant bijection between the set of complex structures on  $B_{\mathbf{R}}$  and  $Y(\mathbf{C})$ , given as follows. As in Remarks 4.3 and 4.11, a complex structure on  $B_{\mathbf{R}}$  is given by a homomorphism of  $\mathbf{R}$ -algebras  $q: \mathbf{C} \rightarrow B_{\mathbf{R}}$ . There then exists a unique (complex) line  $\ell$  in the complex vector space  $B \otimes_{\mathbf{Q}} \mathbf{C}$ , such that

$$(4.2) \quad q(z)xq(z)^{-1} = (z/\bar{z})x, \quad \text{for } x \in \ell \text{ and } z \in \mathbf{C};$$

viewing the line  $\ell$  as a point in projective space,  $\ell$  is the point of the projective variety  $Y(\mathbf{C})$  that corresponds to our original  $q$ . (The fact that  $\ell \subset \overline{\mathcal{O}_\lambda(\mathbf{C})}$  is clear upon choosing an isomorphism  $B \otimes_{\mathbf{Q}} \mathbf{C} \cong M(2, \mathbf{C})$ , with respect to which  $q(z) = \begin{pmatrix} z & \\ & \bar{z} \end{pmatrix}$ ; then  $\ell$  is the span of  $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ , which has zero trace and norm, as required by (3.2).) Now to prove the proposition, note that by Proposition 4.9, a complex structure that gives CM by  $K$  (viewed as a subfield of  $\mathbf{C}$  by Remark 4.11) corresponds to a  $q$  that originates from a homomorphism  $q': K \rightarrow B$  of  $\mathbf{Q}$ -algebras. This is equivalent to saying that the line  $\ell$  comes from a ( $K$ -)line  $\ell' \subset B \otimes_{\mathbf{Q}} K$  satisfying (4.2) for  $x \in \ell'$  and  $z \in K$ . Hence  $\ell'$  corresponds to a point of  $Y(K)$ , which is what we wanted to show. ■

**Remark 4.13** The result in Proposition 4.12 stands in contrast to the usual situation with Shimura curves, where CM-points with CM-field  $K$  are in fact defined over an abelian extension of  $K$ . For Shimura curves, this reflects the fact that an abelian variety isogenous to  $E \times E$ , for a CM elliptic curve  $E$ , is defined over some abelian extension of  $K$ . In contrast, the analogous points of  $X(U)$  are defined over  $K$  itself; this seems to reflect the fact that the period matrix of the corresponding abelian variety is  $K$ -rational. In this sense, the rational structure on  $X(U)$  does not seem to have a direct relation with moduli questions, and so it is not clear how to relate this rational structure to the Galois representations  $\rho_{f,\ell}$  attached to automorphic forms on  $X(U)$

(via Theorem 3.9). One could try to describe a different Galois action on these CM-points, via conjugating the associated abelian varieties; see Proposition 4.15 below. This would still not carry enough information to reconstruct  $\rho_{f,\ell}$ ; I am indebted to B. Gross for this observation. Indeed, the Galois action on such CM abelian varieties will factor through  $\text{Gal}(L/\mathbf{Q})$ , where  $L$  is the maximal abelian extension of the compositum of all (imaginary) quadratic fields  $K$ ; as  $\text{Gal}(L/\mathbf{Q})$  is an inverse limit of solvable groups, it does not have any quotients isomorphic to  $\text{GL}(2, \mathbf{Z}_\ell)$ , and yet  $\rho_{f,\ell}$  usually has an image isomorphic to  $\text{GL}(2, \mathbf{Z}_\ell)$ .

**Remark 4.14** We note that Corollary 3.2 implies that there are infinitely many CM-points with CM-field  $K$ , as they are parametrized by the points of several copies of quotients of  $\mathbf{P}^1(K)$  by finite groups.

We now turn to the last topic of this article, which is a generalization of the Eichler-Shimura congruence relation to the CM-points on  $X(U)$ . As mentioned in the introduction and at the end of Section 3, this congruence is one of the crucial steps in attaching Galois representations to classical modular forms, and to modular forms on indefinite quaternion algebras. The fact that an analog of this congruence also holds in our setting of definite quaternion algebras is evidence that one might yet be able to find a way to produce Galois representations directly from  $X(U)$ , despite the fact that Remark 4.13 seems discouraging. We first give a direct proof of a weaker version of the analog of the Eichler-Shimura congruence, using the theory of complex multiplication. Although we do not need this weaker version (Theorem 4.20) to prove the full analog (Theorem 4.22), we include it because it is reminiscent of Shimura's own proof of the Eichler-Shimura congruence in Theorem 7.9 of [S], which proceeds by showing that for a modular curve  $X'$ , there are infinitely many CM-points on the Hecke correspondence  $T_p \subset X' \times X'$  whose reduction modulo  $p$  lies on the graph of the Frobenius map. In contrast, our proof of the more general Theorem 4.22 is less direct, and invokes the Eichler-Shimura congruence for modular curves.

Our first step in proving Theorem 4.20 is to describe what the theory of complex multiplication says about CM-points on  $X(U)$ . This follows the formulation in Theorem 5.4 of [S]. Write  $K^{ab}$  for the maximal abelian extension of  $K$ , and write  $K_{\mathbf{A}}^{\times}$  for the set of ideles of  $K$ . A homomorphism  $q: K \rightarrow B$  gives rise to another homomorphism, also written  $q: K_{\mathbf{A}}^{\times} \rightarrow B_{\mathbf{A}}^{\times}$ ,  $B_{\mathbf{A}}^{\times}$  being the adelization of  $B^{\times}$ , i.e.,  $B_{\mathbf{A}}^{\times} = \tilde{G}(\mathbf{A})$ . We allow elements of  $B_{\mathbf{A}}^{\times}$  to act on lattices in  $B$  via the projection  $B_{\mathbf{A}}^{\times} = B_{\mathbf{R}}^{\times} \times \hat{B}^{\times} \rightarrow \hat{B}^{\times}$ , as in Definition 3.4.

**Proposition 4.15** Let  $A$  be a two-dimensional abelian variety with a right  $\mathcal{O}$ -action, as in Propositions 4.9 and 4.12, so  $A$  has CM by an imaginary quadratic field  $K$ , viewed as a subfield of  $\mathbf{C}$ . Fix an isomorphism  $\xi: B_{\mathbf{R}}/I \rightarrow A$  for an  $\mathcal{O}$ -ideal  $I$ , such that the complex structure on  $B_{\mathbf{R}}$  arises from a homomorphism  $q: K \rightarrow B$ . We also write  $\xi$  for the isomorphism  $\xi: B \rightarrow A_{\text{tor}}$ , where  $A_{\text{tor}}$  is the set of torsion points of  $A$ . Let  $\sigma$  be an automorphism of  $\mathbf{C}$  whose restriction to  $\text{Gal}(K^{ab}/K)$  is given by the idele  $s \in K_{\mathbf{A}}^{\times}$ . Then there is an isomorphism  $\xi': B_{\mathbf{R}}/q(s^{-1})I \rightarrow A^{\sigma}$ , such that the action of  $\sigma$  on the torsion

points makes the following diagram commute:

$$(4.3) \quad \begin{array}{ccc} B/I & \xrightarrow{\xi} & A_{\text{tor}} \\ q(s^{-1}) \cdot \downarrow & & \downarrow \sigma \\ B/q(s^{-1})I & \xrightarrow{\xi'} & A_{\text{tor}}^\sigma. \end{array}$$

Here  $q(s^{-1}) \in B_A^\times$ . Left multiplication by  $q(s^{-1})$  maps  $B/I$  to  $B/q(s^{-1})I$  via the decomposition  $B/I \cong \bigoplus_p B_p/I_p$ , as in Section 5.2 of [S].

**Remark 4.16** The fact that  $A^\sigma$  also has CM by  $K$  is clear. Indeed,  $A$  has CM if and only if the rational endomorphism algebra  $\text{End } A \otimes_{\mathbf{Z}} \mathbf{Q}$  is isomorphic to  $M(2, K)$ ; the structure of this endomorphism algebra is unaffected by  $\sigma$ .

**Remark 4.17** In this and in our subsequent discussion, we do not assume anything about the field of rationality of isomorphisms or isogenies between abelian varieties; for our purposes,  $\xi$  and  $\xi'$  are only defined over  $\mathbf{C}$ .

**Proof of Proposition 4.15** Take an isogeny  $E \times E \rightarrow A$ , where  $E$  is an elliptic curve with complex multiplication by  $K$ . Hence  $A$  is isomorphic to  $E \times E/C$ , where  $C$  is the finite kernel of this isogeny. We then obtain that  $A^\sigma$  is isomorphic to  $E^\sigma \times E^\sigma/C^\sigma$ , which we calculate by the usual theory of complex multiplication. This involves realizing  $E$  as  $\mathbf{C}/\mathfrak{a}$  for some lattice  $\mathfrak{a}$  in  $K$ ; thus  $A$  is isomorphic to  $\mathbf{C} \oplus \mathbf{C}/(\mathfrak{a} \oplus \mathfrak{a}, C)$ , where  $(\mathfrak{a} \oplus \mathfrak{a}, C)$  is the lattice generated by  $\mathfrak{a} \oplus \mathfrak{a}$  and a set of representatives for  $C$ , which we shall again write as  $C$ . Note that  $C \subset K \oplus K$ , since  $C$  is a torsion subgroup of  $E \times E$ . Now our original isogeny  $E \times E \rightarrow A$  arises from a map  $\mathbf{C} \oplus \mathbf{C} \rightarrow B_{\mathbf{R}}$ , which in turn arises by extension of scalars (from  $\mathbf{Q}$  to  $\mathbf{R}$ ) of an isomorphism  $K \oplus K \rightarrow B$ . This isomorphism takes the lattice  $(\mathfrak{a} \oplus \mathfrak{a}, C)$  to  $I$ ; given  $\alpha \in K$ , this isomorphism also carries multiplication by  $\alpha$  on  $K \oplus K$  over to left multiplication by  $q(\alpha)$  on  $B$ .

We now invoke Theorem 5.4 of [S]. Then  $E^\sigma$  is isomorphic to  $\mathbf{C}/s^{-1}\mathfrak{a}$ , and the action of  $\sigma$  on torsion points in  $E_{\text{tor}}$  is given by a diagram analogous to (4.3). Thus  $A^\sigma$  is isomorphic to the quotient of  $\mathbf{C} \oplus \mathbf{C}$  by the lattice  $(s^{-1}\mathfrak{a} \oplus s^{-1}\mathfrak{a}, [s^{-1}]C)$ . Here  $[s^{-1}]C$  is a set of representatives in  $K \oplus K$  for the result of multiplying  $C \in K \oplus K/\mathfrak{a} \oplus \mathfrak{a}$  by  $s^{-1}$  and obtaining a new set of points  $[s^{-1}]C \subset K \oplus K/s^{-1}\mathfrak{a} \oplus s^{-1}\mathfrak{a}$ , as in Section 5.2 of [S]. Working inside  $K \oplus K$ , one checks the equality of lattices  $(s^{-1}\mathfrak{a} \oplus s^{-1}\mathfrak{a}, [s^{-1}]C) = s^{-1}(\mathfrak{a} \oplus \mathfrak{a}, C)$  (this is straightforward but not quite as trivial as the notation suggests). In terms of our isomorphism between  $K \oplus K$  and  $B$ , the lattice  $(s^{-1}\mathfrak{a} \oplus s^{-1}\mathfrak{a}, [s^{-1}]C)$  then corresponds to  $q(s^{-1})I$ . We similarly obtain (4.3). ■

**Corollary 4.18** Let  $A \cong B_{\mathbf{R}}/I$  be as in Proposition 4.15. Then the field of moduli of  $A$ , equipped with its endomorphisms, is the ring class field over  $K$  corresponding to the order  $\mathcal{O}'_K = q^{-1}(\mathcal{O}')$ , where  $q: K \rightarrow B$  is the inclusion of Proposition 4.15, and  $\mathcal{O}'$  is the left order of  $I$ .

**Proof** Since we are also considering the endomorphisms of  $A$ , which are an order in  $M(2, K)$ , the field of moduli in question contains  $K$ . Thus the field of moduli is the class field corresponding to those  $s \in K_A^\times$  which satisfy the following two properties: first,  $q(s^{-1})I = \gamma I$  for some  $\gamma \in B$ ; second, conjugation by  $\gamma$  (as in (4.1)) preserves the complex structure on  $B_R$ . This means that conjugation by  $\gamma$  preserves the  $K$ -structure on  $B$  induced by  $q$ ; hence  $\gamma = q(\alpha)$  for some  $\alpha \in K$ . In other words,  $I$  is stable under left multiplication by  $q(s\alpha) \in B_A^\times$ ; hence our set of  $s$  is  $K^\times (\mathcal{O}'_K)^\times \subset K_A^\times$ , which is exactly the open subgroup corresponding to the ring class field of  $\mathcal{O}'_K$ . ■

**Remark 4.19** In particular, the field of moduli of  $A$  as above is the Hilbert class field of  $K$  if and only if  $\mathcal{O}'_K$  is the full ring of integers of  $K$ . In all cases,  $q$  as above gives what is called an optimal embedding of  $\mathcal{O}'_K$  into  $\mathcal{O}'$ .

We can now prove our weak form of the congruence of Eichler and Shimura, essentially only for half the primes (essentially, those that are split in  $K$ , or, equivalently, those where the abelian variety is ordinary).

**Theorem 4.20** *Let  $x \in X(U)(K)$  correspond to an abelian variety  $A$  with both a right  $\mathcal{O}$ -action and CM by  $K$ ; use the notation and assumptions of Proposition 4.15. For almost every prime  $p$  that is split in  $K$ , let  $\sigma$  be a Frobenius element above  $p$ . Then  $A^\sigma$  corresponds to one of the points  $x_\nu$  in the formal sum of points  $T_p x$  described in Proposition 4.6. In other words, if  $A^\sigma$  corresponds to the point  $x' \in X(U)(K)$ , then the pair  $(x, x')$  lies on the correspondence  $T_p$ , viewed as a correspondence on  $X(U) \times X(U)$ .*

**Proof** Write  $A = B_R/I$  for an  $\mathcal{O}$ -ideal  $I$ , and assume that  $\mathcal{O}$  is unramified at  $p$ , as in Definition 3.7, so that  $T_p$  makes sense. Let  $\mathcal{O}'_K$  be as in Corollary 4.18, and assume that  $p$  does not divide the conductor of  $\mathcal{O}'_K$ ; i.e., writing  $K'$  for the ring class field of  $\mathcal{O}'_K$ , we are requiring  $p$  to be unramified in  $K'$ . All in all, we have excluded finitely many  $p$  (note that the set of excluded  $p$  depends on  $\mathcal{O}'_K$ , which depends on  $x$ ). Now  $p$  is split in  $K$ , with  $p = \mathfrak{p}\bar{\mathfrak{p}}$ , so our Frobenius element  $\sigma$  is either  $\text{Frob } \mathfrak{p}$  or  $\text{Frob } \bar{\mathfrak{p}}$ , these two Frobenius elements being inverse to each other in  $\text{Gal}(K'/K)$ . We can then choose an element  $s \in K_A^\times$  representing  $\sigma$ , by taking  $s$  to be a uniformizer in one of the completions  $K_\mathfrak{p}^\times$  (if  $\sigma = \text{Frob } \mathfrak{p}$ ) or in  $K_{\bar{\mathfrak{p}}}^\times$  (if  $\sigma = \text{Frob } \bar{\mathfrak{p}}$ ), both viewed as subgroups of  $K_A^\times$ . In both cases,  $q(s^{-1})$  is an element of the  $p$ -adic completion  $\mathcal{O}'_K \otimes_{\mathbb{Z}} \mathbb{Z}_p \cong \mathbb{Z}_p \times \mathbb{Z}_p$ , and the norm of  $q(s^{-1})$  is  $p^{-1}$ . Thus  $q(s^{-1})I$  is an  $\mathcal{O}$ -ideal containing  $I$ , with  $q(s^{-1})I/I \cong (\mathbb{Z}/p\mathbb{Z})^2$ . (In coordinates, we can choose an isomorphism  $B_p \cong M(2, \mathbb{Q}_p)$  such that  $\mathcal{O}'_p$  corresponds to  $M(2, \mathbb{Z}_p)$ , and  $\mathcal{O}'_K \otimes_{\mathbb{Z}} \mathbb{Z}_p \subset \mathcal{O}'_p$  corresponds to  $\mathbb{Z}_p \times \mathbb{Z}_p$ , embedded diagonally into  $M(2, \mathbb{Z}_p)$ . The idele  $s$  then corresponds to either  $(p, 1)$  or  $(1, p)$  in  $K_p = K_\mathfrak{p} \times K_{\bar{\mathfrak{p}}} \cong \mathbb{Q}_p \times \mathbb{Q}_p$ .) We then invoke Proposition 4.8 and conclude the theorem. ■

**Remark 4.21** If  $(x, x')$  is any pair on the correspondence  $T_p$ , then  $x$  corresponds to an abelian variety with CM-field  $K$  if and only if  $x'$  does as well. This is clear from the fact that the complex tori corresponding to  $x$  and to  $x'$  are isogenous. Alternatively, one can show directly that  $x \in X(U)(K)$  if and only if  $x' \in X(U)(K)$ .

We now give the general proof of the analog of the Eichler-Shimura congruence, without needing to restrict ourselves to  $p$  split in  $K$ . We shall also obtain our results for all  $p$  where  $\mathcal{O}$  is unramified, so the finite set of “bad”  $p$  is independent of the CM-point  $x$ , and even of the CM-field  $K$ .

**Theorem 4.22** *Let  $x \in X(U)(K)$  be as in Theorem 4.20, corresponding to an abelian variety  $A$ . Take a prime  $p$  where  $\mathcal{O}$  is unramified, and write  $T_px$  as the formal sum of  $p + 1$  points  $T_px = \sum_{\nu=0}^p x_\nu$ ; call the corresponding abelian varieties  $A_0, \dots, A_p$ . Choose a prime  $\mathfrak{P}$  of  $\overline{\mathbf{Q}}$  above  $p$ , and write  $\overline{A}$  for the reduction of (a good model of)  $A$  modulo  $\mathfrak{P}$ ; similarly, write  $\overline{A}_\nu$  for the reduction of  $A_\nu$ . Then we can reorder the  $A_\nu$  so that we obtain isomorphisms (defined over the algebraic closure of  $\mathbf{Z}/p\mathbf{Z}$ ):*

$$(4.4) \quad \overline{A}^{\text{Frob } p} \cong \overline{A}_0, \quad \overline{A}^{(\text{Frob } p)^{-1}} \cong \overline{A}_\nu, \quad \text{for } 1 \leq \nu \leq p.$$

We shall use the following lemma:

**Lemma 4.23** *With  $A$  as above, there exists an elliptic curve  $E$  with CM by  $K$ , and an isogeny  $\varphi: E \times E \rightarrow A$ , such that*

1.  *$\ker \varphi$  has order prime to  $p$ , whence  $\varphi$  induces an isomorphism  $E[p] \times E[p] \cong A[p]$  on the torsion points of order  $p$ .*
2. *The resulting right action of  $\mathcal{O}/p\mathcal{O}$  on  $E[p] \times E[p]$  is compatible with an isomorphism  $\mathcal{O}/p\mathcal{O} \cong M(2, \mathbf{Z}/p\mathbf{Z})$ , with  $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M(2, \mathbf{Z}/p\mathbf{Z})$  sending  $(P, Q) \in E[p] \times E[p]$  to  $(aP + cQ, bP + dQ)$ .*

**Proof of Lemma 4.23** View  $A$  as  $B_{\mathbf{R}}/I$  for an  $\mathcal{O}$ -ideal  $I$ , with the complex structure coming from  $q: K \rightarrow B$ . As before, write  $\mathcal{O}'_K = q^{-1}\mathcal{O}' = \{\alpha \in K \mid q(\alpha)I \subset I\}$ . We shall show that we can take  $E = \mathbf{C}/\mathcal{O}'_K$ .

We claim that  $I/pI$  is isomorphic as an  $\mathcal{O}'_K/p\mathcal{O}'_K$ -module to  $\mathcal{O}'_K/p\mathcal{O}'_K \oplus \mathcal{O}'_K/p\mathcal{O}'_K$ , with the right action of  $\mathcal{O}/p\mathcal{O}$  corresponding to the right action of  $M(2, \mathbf{Z}/p\mathbf{Z})$ , analogously to (2) above. This is not hard, but takes some care. Choosing an isomorphism of  $\mathcal{O}/p\mathcal{O}$  with  $M(2, \mathbf{Z}/p\mathbf{Z})$ , we know that  $I/pI$  is isomorphic to  $M(2, \mathbf{Z}/p\mathbf{Z})$  as a right  $M(2, \mathbf{Z}/p\mathbf{Z})$ -module, and that  $\mathcal{O}'_K/p\mathcal{O}'_K$  acts on the left of  $I/pI$  by left multiplication via a homomorphism  $\iota: \mathcal{O}'_K/p\mathcal{O}'_K \rightarrow M(2, \mathbf{Z}/p\mathbf{Z})$ . (Caution:  $\iota$  is not quite the map induced from  $q$ . In essence, the  $p$ -adic completion  $I_p$  of  $I$  can be written as  $I_p = \gamma_p\mathcal{O}_p$ , where without loss of generality  $\gamma_p \in \mathcal{O}_p \cong M(2, \mathbf{Z}_p)$ . Then  $\iota$  is the conjugation of  $q$  by  $\gamma_p$ .) By our choice of  $\mathcal{O}'_K$ ,  $\mathcal{O}'_K/p\mathcal{O}'_K$  acts *faithfully* on  $I/pI$ , so  $\iota$  is an injection. Hence  $\iota$  gives  $V = (\mathbf{Z}/p\mathbf{Z})^2$  (viewed as column vectors) the structure of a faithful  $\mathcal{O}'_K/p\mathcal{O}'_K$ -module. We wish to show that  $V$  is isomorphic to  $\mathcal{O}'_K/p\mathcal{O}'_K$ , from which our claim will follow: indeed,  $I/pI \cong M(2, \mathbf{Z}/p\mathbf{Z})$  decomposes into a direct sum of two copies of  $V$  (the two columns of a matrix) under the left action of  $\mathcal{O}'_K/p\mathcal{O}'_K$ , and the right action of  $\mathcal{O}/p\mathcal{O}$  on  $V \oplus V$  is similar to (2) above. Now to see that that  $V \cong \mathcal{O}'_K/p\mathcal{O}'_K$ , note that  $\mathcal{O}'_K/p\mathcal{O}'_K$  is two-dimensional over  $\mathbf{Z}/p\mathbf{Z}$ , so  $\mathcal{O}'_K/p\mathcal{O}'_K \cong (\mathbf{Z}/p\mathbf{Z}[t])/(f(t))$ , where  $f(t)$  is a quadratic polynomial. The fact that  $\iota$  is injective means that  $f$  is the minimal polynomial of the linear transformation  $\iota(t)$

on  $V$ . Since  $V$  is also two-dimensional, we conclude that  $f$  is also the characteristic polynomial of  $\iota(t)$ . Thus  $V$  is a cyclic module for the linear transformation  $\iota(t)$ , with minimal polynomial  $f$ , whence  $V \cong (\mathbf{Z}/p\mathbf{Z})[t]/(f) \cong \mathcal{O}'_K/p\mathcal{O}'_K$ , as desired. (We remark that this proof seems more satisfying than a case-by-case proof that uses the fact that  $\mathcal{O}'_K/p\mathcal{O}'_K$  is isomorphic either to the ring  $\mathbf{Z}/p\mathbf{Z} \times \mathbf{Z}/p\mathbf{Z}$ , or to the finite field with  $p^2$  elements, or finally to  $(\mathbf{Z}/p\mathbf{Z})[t]/(t^2)$ —this last case occurring when  $p$  divides the conductor of  $\mathcal{O}'_K$ .)

We now conclude the proof of the lemma. We have produced an isomorphism  $\overline{\varphi}: \mathcal{O}'_K/p\mathcal{O}'_K \oplus \mathcal{O}'_K/p\mathcal{O}'_K \rightarrow I/pI$ , which satisfies an analog of property (2) above. Lift  $\overline{\varphi}$  to an injective homomorphism of  $\mathcal{O}'_K$ -modules  $\varphi_0: \mathcal{O}'_K \oplus \mathcal{O}'_K \rightarrow I$  (simply lift the images  $\overline{\varphi}(1, 0)$  and  $\overline{\varphi}(0, 1)$  to  $I$ ; the resulting homomorphism is injective because it extends to an isomorphism  $K \oplus K \rightarrow B$ , and to an isomorphism  $\mathbf{C} \oplus \mathbf{C} \rightarrow B_{\mathbf{R}}$ ). Since  $\overline{\varphi}$  is an isomorphism, the cokernel of  $\varphi_0$  has order prime to  $p$ . The homomorphism  $\varphi_0$  then induces a map  $\varphi: \mathbf{C}/\mathcal{O}'_K \times \mathbf{C}/\mathcal{O}'_K \rightarrow B_{\mathbf{R}}/I$ , which one easily checks has properties (1) and (2) above. ■

**Proof of Theorem 4.22** We use Lemma 4.23 to reduce our statement about  $A$  to the Eichler-Shimura congruence for  $E$  itself. Take  $\varphi: E \times E \rightarrow A$  as in that lemma. Following Proposition 4.8, we list the  $\mathcal{O}$ -stable subgroups  $C_\nu$  of  $A[p]$  with  $C_\nu \cong (\mathbf{Z}/p\mathbf{Z})^2$ . Passing from  $A[p]$  to the isomorphic group  $E[p] \times E[p]$ , we see that as  $\ell_\nu \subset E[p]$  varies among the  $p+1$  “lines” ( $\ell_\nu \cong \mathbf{Z}/p\mathbf{Z}$ ) in the “plane”  $E[p] \cong (\mathbf{Z}/p\mathbf{Z})^2$ ,  $C_\nu$  varies among the subgroups  $\ell_\nu \oplus \ell_\nu \subset E[p] \times E[p]$ . This last statement follows essentially from (2) of Lemma 4.23. Write  $C = \ker \varphi$ ; we thus see that the  $A_\nu$  are isomorphic to the quotients  $E \times E/(\ell_\nu \oplus \ell_\nu, C)$ , where  $(\ell_\nu \oplus \ell_\nu, C)$  is the subgroup of  $E[p] \times E[p]$  generated by  $\ell_\nu \oplus \ell_\nu$  and  $C$ . Now invoke the Eichler-Shimura congruence for  $E$  and for points of  $E$ , or rather for the modular curve  $X_1(N)$ : if  $P \in E[N]$  is a torsion point of order  $N$  prime to  $p$ , then for one choice of  $\nu$ , say for  $\nu = 0$ , we have the following isomorphism after reducing modulo  $\mathfrak{F}$ :

$$(4.5) \quad (\overline{(E/\ell_0)}, \overline{P_0}) \cong (\overline{E}^{\text{Frob } p}, \overline{P}^{\text{Frob } p}),$$

where  $P_0$  is the image of  $P$  in  $E/\ell_0$ . By the notation in (4.5), we mean that the isomorphism between  $\overline{(E/\ell_0)}$  and  $\overline{E}^{\text{Frob } p}$  carries the reduction  $\overline{P_0}$  of  $P_0$  to  $\overline{P}^{\text{Frob } p}$ , which is the result of applying  $\text{Frob } p$  to the reduction  $\overline{P}$  of  $P$ . The Eichler-Shimura congruence also implies that for the other  $\nu$ , we have isomorphisms

$$(4.6) \quad (\overline{(E/\ell_\nu)}, \overline{P_\nu}) \cong (\overline{E}^{(\text{Frob } p)^{-1}}, \overline{p \cdot P}^{(\text{Frob } p)^{-1}}), \quad \text{for } 1 \leq \nu \leq p.$$

Here  $P_\nu$  is again the image of  $P$  in  $E/\ell_\nu$ , and we have taken the  $p$ -th multiple of  $P$  on the elliptic curve before reducing modulo  $\mathfrak{F}$ . We note that analogs of (4.5) and (4.6) hold if we simultaneously take several torsion points  $P, Q, R, \dots \in E[N]$ .

Now  $\overline{A_0}$  is isomorphic to  $\overline{(E/\ell_0)} \times \overline{(E/\ell_0)}/\overline{C_0}$ , where  $C_0$  is the image of  $C$  in  $E/\ell_0 \times E/\ell_0$ . Writing a typical element of  $C$  as  $(P, Q) \in E \times E$ , and using (4.5), we conclude that  $\overline{A_0}$  is isomorphic to  $\overline{E}^{\text{Frob } p} \times \overline{E}^{\text{Frob } p}/\overline{C}^{\text{Frob } p}$ , which in turn is isomorphic to  $\overline{A}^{\text{Frob } p}$ . Of course, the fact that  $C$  has order prime to  $p$  is essential here. Similarly, we obtain the statement (4.4) about  $\overline{A_\nu}$  for  $1 \leq \nu \leq p$ , by using (4.6) and the fact that  $p \cdot C = C$ . ■

## References

- [BD] M. Bertolini and H. Darmon, *Heegner points,  $p$ -adic  $L$ -functions, and the Cerednik-Drinfeld uniformization*. Invent. Math. **131**(1998), 453–491.
- [BK] R. Brylinski and B. Kostant, *Differential Operators on Conical Lagrangian Manifolds*. In: Lie Theory and Geometry in Honor of Bertram Kostant, Progress in Math. **123**, Birkhäuser, 1994.
- [D] P. Deligne, *Formes modulaires et représentations de  $GL(2)$* . In: Modular Functions of One Variable II, Lecture Notes in Math. **349**, Springer, 1973.
- [G1] B. Gross, *Heights and the special values of  $L$ -series*. CMS Conf. Proc. **7**(1987), 115–187.
- [G2] ———, *Algebraic modular forms*. Preprint, 1997.
- [P] A. Pizer, *An algorithm for computing modular forms on  $\Gamma_0(N)$* . J. Algebra **64**(1980), 340–390.
- [S] G. Shimura, *Introduction to the Arithmetic Theory of Automorphic Functions*. Iwanami Shoten and Princeton University Press, 1971.
- [S2] ———, *On analytic families of polarized abelian varieties and automorphic functions*. Ann. of Math. **78**(1963), 149–192.

*Mathematics Department and Center for Advanced Mathematical Sciences  
American University of Beirut  
Bliss Street  
Beirut  
Lebanon  
email: kmakdisi@aub.edu.lb*