Math. Ann. 253, 43–62 (1980)

Mathematische Annalen

Twists of Modular Forms and Endomorphisms of Abelian Varieties

Kenneth A. Ribet*

Department of Mathematics, University of California, Berkeley, CA 94720, USA

1. Introduction

Let A and B be Abelian varieties over a number field k, and let l be a prime. Let V_A and V_B be the $\mathbf{Q}_l$-adic Tate modules of A and B. Tate's conjecture [19] for homomorphisms $A \to B$ asserts that the natural injection

(1.1) $\mathrm{Hom}_K(A, B) \otimes \mathbf{Q}_l \hookrightarrow \mathrm{Hom}_{\mathrm{Gal}(\bar{k}/K)}(V_A, V_B)$

is an isomorphism for each finite extension K of k in a fixed algebraic closure $\bar{k}$ of k. The main purpose of this paper is to verify Tate's conjecture in the special case where $k = \mathbf{Q}$ (but K is an arbitrary number field) and A and B are the Jacobians $J_1(N)$, $J_1(M)$ of modular curves $X_1(N)$ and $X_1(M)$.

In doing this, it is easy to compute the right-hand side of (1.1), or at least its dimension, since V_A and V_B are just (products of) l-adic representations attached to modular forms. The problem is to "justify" this dimension by exhibiting many homomorphisms $A \to B$. This is essentially what we do, except that we first reduce to the case where A and B are each equal to the factor A_f of $J_1(N)$ attached to a weight 2 newform f on $\Gamma_1(N)$.

Then the question becomes that of exhibiting an endomorphism of A_f each time that f has an "extra twist," meaning essentially that f is a twist of one of its own conjugates. We show that this can be done by taking up some ideas of Shimura [16, Sect. 4] concerning the "geometrical meaning" of twists. In the case where f does not have complex multiplication, the full endomorphism algebra of A_f is described as the "crossed product algebra" attached to a certain cocycle whose values are Jacobi sums.

Our interest in this subject was rekindled by a recent conversation with Tunnell concerning his work relating divisors on $X_1(N) \times X_1(M)$ with the L-function of this surface [20]. Also related to this paper is the recent work of Atkin-Li on twisting [1], to which little direct reference is made in the text below. Further, after this paper was submitted for publication, Professor Ihara informed

* Partially supported by the National Science Foundation under grant MCS 77-03719, and by École Polytechnique (1979–1980)

0025-5831/80/0253/0043/$04.00

the author that F. Momose had obtained results similar to those below, by techniques which are essentially identical to ours. Momose studies the group of twists of a newform of arbitrary weight ($\geqq 2$) and the implications of twisting for the l-adic representation attached to such a form. His work will be appearing soon.

2. Eigenforms and Abelian Varieties

In this section, we review some results of Shimura concerning Jacobians of modular curves, adopting the perspective of [16]. For ease of exposition, we introduce the convention, to be in force throughout the remainder of this paper, that all modular forms considered are to be *cusp forms* and of *weight 2.*

Let Γ be a subgroup of $\mathbf{SL}_2\mathbf{Z}$, intermediate between $\Gamma_1(N)$ and $\Gamma_0(N)$. For definiteness, let us in fact take

$$\Gamma = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N) \,\middle|\, a \equiv d \equiv 1 \bmod m \right\},$$

where m is a (positive) divisor of N. Let $S(\Gamma)$ be the space of forms on Γ, and for $n \geqq 1$, let T_n be the n-th Hecke operator on $S(\Gamma)$. Let $X(\Gamma)/\mathbf{Q}$ be the modular curve associated to Γ, and let $J(\Gamma)$ be its Jacobian. In Shimura's theory, the T_n arise from certain correspondences on $X(\Gamma)/\mathbf{Q}$, which are then viewed as endomorphisms of $J(\Gamma)$ by regarding $J(\Gamma)$ as the Albanese variety of $X(\Gamma)$. We denote the endomorphisms by $\xi_n, n \geqq 1$. We write $\Omega_{J(\Gamma)}$ for the space of invariant differentials on $J(\Gamma)$, which may be alternately viewed as the space of regular differentials on $X(\Gamma)$. These are $\mathbf{Q}$-vector spaces whose dimension is the genus of $X(\Gamma)$. We write $\Omega_{J(\Gamma)/\mathbf{C}}$ for the corresponding space over $\mathbf{C}$, i.e., $\Omega_{J(\Gamma)} \bigotimes_{\mathbf{Q}} \mathbf{C}$. We have, canonically

(2.1) $\Omega_{J(\Gamma)/\mathbf{C}} \simeq S(\Gamma)$.

For η an endomorphism of $J(\Gamma)$, we write η^* for the (pullback) map it induces on $\Omega_{J(\Gamma)/\mathbf{C}}$; this pullback is already defined on the vector space $\Omega_{J(\Gamma)}$ if $\eta \in \mathrm{End}_{\mathbf{Q}} J(\Gamma)$. Via (2.1), we have

$$\xi_n^* = T_n.$$

We consider the special case where m^2 divides N, so that "slashing" by the matrix $\begin{pmatrix} 1 & u/m \\ 0 & 1 \end{pmatrix}$ for $u \in \mathbf{Z}$ induces a map

$$a_u : S(\Gamma) \to S(\Gamma).$$

According to [16, Sect. 4], there is a (unique) endomorphism α_u of $J(\Gamma)$ such that

$$\alpha_u^* = a_u.$$

This endomorphism is not defined over $\mathbf{Q}$, but rather over the field of m-th roots of 1.

Returning to the general case where m^2 need not divide N, we let $f = \sum a_n q^n$

be a normalized eigenform in $S(\Gamma)$. Thus we suppose that

$$f|T_n = a_n f$$

for *all* $n \geqq 1$. [We remark that the definition of the T_n depends on Γ, or at least on N, so that f need not be an eigenform in $S(\Gamma')$ when $\Gamma' \subsetneqq \Gamma$.] The coefficient field $E_f = \mathbf{Q}(\ldots a_n \ldots)$ is a number field, i.e. a finite extension of $\mathbf{Q}$. If f is fixed, we denote it simply by E. Shimura associates to f an Abelian variety $A = A_f$ of dimension $[E:\mathbf{Q}]$ given as a quotient of $J(\Gamma)$:

$$v: J(\Gamma) \to A.$$

The variety A and the map v are defined over $\mathbf{Q}$, and the kernel of v is connected (i.e., is an Abelian variety). Further, we have an embedding θ of E into $(\mathrm{End}_{\mathbf{Q}} A) \otimes \mathbf{Q}$, the $\mathbf{Q}$-algebra of endomorphisms of $A/\mathbf{Q}$. For $n \geqq 1$, $\theta(a_n)$ is given by a commutative diagram

$$\begin{array}{ccc} J(\Gamma) & \xrightarrow{\xi_n} & J(\Gamma) \\ \downarrow v & & \downarrow v \\ A & \xrightarrow{\theta(a_n)} & A \end{array}$$

The space $\Omega_{A/\mathbf{C}}$ of invariant differentials on A over $\mathbf{C}$ may be identified (via v^*) with the subspace of $S(\Gamma)$ generated by the conjugates σf of f ($\sigma \in \mathrm{Aut}\,\mathbf{C}$).

Despite a remark made above, the form f may be viewed as an eigenform in $S(\Gamma')$ for *many* subgroups Γ' of Γ: it suffices that the level N' of Γ' be divisible by the *same* primes as N. (See [18, Chap. 3] and especially Theorems (3.43) and (3.53).) Using Γ and one such Γ', and f, we construct two Abelian varieties A and A'.

Proposition (2.2). *The varieties A and A' are isogenous over* $\mathbf{Q}$.

Proof. The inclusion $\Gamma \subset \Gamma'$ leads to a surjection $X(\Gamma') \to X(\Gamma)$ and then a surjection $J(\Gamma') \to J(\Gamma)$ (Albanese functoriality), defined over $\mathbf{Q}$. Composing this latter quotient map with the quotient $v: J(\Gamma) \to A$ defining A, we obtain a map $\varphi: J(\Gamma') \to A$ defined over $\mathbf{Q}$. We clearly have $\varphi^*(\Omega_A) = v'^*(\Omega_{A'})$, as we can easily verify after tensoring with $\mathbf{C}$. It follows that there is a unique isomorphism λ of Abelian varieties up to isogeny such that $\lambda \circ v' = \varphi$. (Actually, λ is a literal map $A' \to A$ because the kernel of v' is connected.) By the uniqueness, λ is defined over $\mathbf{Q}$ since φ and v' are defined over $\mathbf{Q}$.

We now discuss the special role played by those eigenforms f which are in fact *newforms* in the sense of ([6, 8], etc.). We consider only the groups $\Gamma_1(N)$, and write $S(N)$ for $S(\Gamma_1(N))$. As is well known, for each divisor M of N and each divisor d of N/M, the formula $\sum a_n q^n \mapsto \sum a_n q^{dn}$ defines a map

$$t_{M,d}: S(M) \to S(N).$$

If $S(M)^{\mathrm{new}}$ is the subspace of $S(M)$ generated by the newforms of level M, then

$$S(N) \simeq \bigoplus_M \bigoplus_d t_{M,d}(S(M)^{\mathrm{new}}).$$

This decomposition is echoed by a decomposition up to isogeny of $J_1(N)$, cf. [7, Sect. 2]. For each M, we consider the product $\prod_f A_f$ running over the set of (normalized) newforms of level M, taken up to conjugacy. (For $\sigma \in \operatorname{Aut}\mathbf{C}$, the form $\sigma f = \sum \sigma a_n q^n$ is a newform of level M if $f = \sum a_n q^n$ is such a newform. The Abelian varieties A_f and $A_{\sigma f}$ are the same.) This product is clearly a quotient of $J_1(M)$; i.e., the product of the structural maps $J_1(M) \to A_f$ is surjective. Following [7, Sect. 2], we let $J_1(M)^{\text{new}}$ be the associated "optimal quotient" of $J_1(M)$, i.e., that quotient which is isogenous to $\prod A_f$ and so that the kernel of $J_1(M) \to J_1(M)^{\text{new}}$ is connected. One knows that there is a homomorphism (over $\mathbf{Q}$)

$$\tau_{M,d} : J_1(N) \to J_1(M)^{\text{new}}$$

such that $\tau_{M,d}^* = t_{M,d}$. (Namely, $\tau_{M,d}$ is an appropriate "degeneracy operator," cf. [7, p. 138], followed by the quotient map $J_1(M) \to J_1(M)^{\text{new}}$.) The map

$$\tau : J_1(N) \to \prod_M \prod_d J(M)^{\text{new}}$$

made by assembling the various $\tau_{M,d}$ is an isogeny. As a corollary, we note explicitly the following fact.

Proposition (2.3). *The Abelian variety $J_1(N)$ is isogenous over $\mathbf{Q}$ to a product of Abelian varieties of the form A_f, where f is a newform of some level M dividing N.*

As an application, we give the relation between A_f and A_g when g is obtained from f by stripping away those coefficients of f which are not prime to some integer Q.

Proposition (2.4). *Let $f = \sum a_n q^n$ be a newform on $\Gamma_1(M)$ and let $Q \geqq 1$. Let g be the form $\sum_{(n,Q)=1} a_n q^n$, considered as an eigenform on $\Gamma_1(N)$ for a multiple N of M. Then A_f and A_g are isogenous over $\mathbf{Q}$.*

Proof. For each divisor d of N/M, we compose the map

$$\tau_{M,d} : J_1(N) \to J_1(M)^{\text{new}}$$

with the quotient $J_1(M)^{\text{new}} \to A_f$, thus obtaining a map

$$\varphi_d : J_1(N) \to A_f .$$

The space $\varphi_d^*(\Omega_{A_f/\mathbf{C}})$ is the subspace of $S(N)$ generated by $f(q^d)$ and its conjugates. The φ_d taken together define a map

$$\varphi : J_1(N) \to A_f \times \ldots \times A_f$$

which is *surjective*, the surjectivity being a consequence of the fact that τ is an isogeny. In terms of modular forms, $\varphi^*(\Omega_{A_f \times \ldots \times A_f/\mathbf{C}})$ is the *direct sum* of the spaces $\varphi_d^*(\Omega_{A_f/\mathbf{C}})$. As has already been suggested, for each d dividing N/M, the space $\varphi_d^*(\Omega_{A_f/\mathbf{C}})$ has as basis the distinct conjugates $\sigma f(q^d)$ of $f(q^d)$. Taking a different point of view, for each $\sigma \in \operatorname{Aut}\mathbf{C}$, we let V_σ be the subspace of $V = \varphi^*(\Omega_{A_f \times \ldots \times A_f/\mathbf{C}})$ generated by the $\sigma f(q^d)$ with d running over the divisors d of N/M. Then V is the direct sum of its (distinct) subspaces V_σ, and for each σ we have

$$V_\sigma = \{h \in S(N) \mid h | T_p = \sigma(a_p) h \quad \text{for all} \quad p \nmid N\} .$$

In particular, $\sigma g \in V_\sigma$. Therefore, if

$$v: J_1(N) \to A_g$$

is the structural map defining A_g, we have

$$v^*(\Omega_{A_g/C}) \subseteq V.$$

This implies that there is a unique map λ of Abelian varieties up to isogeny, defined over **Q**,

$$\lambda: A_f \times \ldots \times A_f \to A_g,$$

such that $\lambda \circ \varphi = v$.

View λ as a tuple of maps (λ_d), $\lambda_d: A_f \to A_g$. We claim that λ_1 is an isogeny.

For this, we first remark that f and g have the same coefficient field, since E_f is generated by almost all of the coefficients a_p of f. Thus A_f and A_g have the same dimension. So to show that λ_1^* is an isomorphism and hence prove the claim, it will be enough to show that λ_1^* is surjective. This map, however, is just the inclusion

$$v^*: \Omega_{A_g/\mathbf{C}} \hookrightarrow V$$

followed by the projection of V onto its direct factor $\varphi_1^*(\Omega_{A_f})$. For the surjectivity, we must show that, when σg is written as a linear combination

$$\sum c_d \cdot \sigma f(q^d),$$

the coefficient c_1 of σf is non-zero. This, however, is evidently the case, since the initial coefficient σa_1 of σg is non-zero.

3. Twisting and "Inner Twisting"

Let f be a newform of level N, and let χ be a (primitive) Dirichlet character of conductor r. As is well known, there is a unique newform $g = \sum_{n \geqq 1} b_n g^n$ characterized by the relation:

$$b_p = a_p \chi(p) \quad \text{for almost all } p$$

(i.e., for all but finitely many primes p). We have $b_n = \chi(n) a_n$ for all n prime to r, but not necessarily for all n. If M is the level of g, then $N \cdot r$ and $M \cdot r$ have the same prime factors. If **A** is the Adele ring of **Q** and π_f (resp. π_g) is the automorphic representation of **GL**(2, **A**) associated to f (resp. g), then the relation between f and g may be summarized by the formula

$$\pi_g = \pi_f \otimes \chi.$$

If ε_f and ε_g are respectively the ("Nebentypus") characters of f and g, then

$$\varepsilon_g = \varepsilon_f \cdot \chi^2.$$

We are mostly interested in the case where g turns out to be a conjugate σf of f. (As mentioned above, if $\sigma \in \operatorname{Aut}\mathbf{C}$, then the form

$$\sigma f = \sum \sigma a_n q^n$$

is again a newform, with character $\sigma\varepsilon_f$.) We shall assume from now on in this section that f is *not* a form which has *complex multiplication* in the sense that there is a Dirichlet character $\varphi \neq 1$ such that

$$a_p = \varphi(p) a_p$$

for almost all p.

Let Γ be the set of embeddings

$$\gamma : E \to \mathbf{C}$$

having the following property:

There exists a Dirichlet character χ such that $\gamma(a_p) = \chi(p) a_p$ for almost all p.

Since f is assumed not to have complex multiplication, the character χ is unique, given γ, when it exists; we thus may denote it by χ_γ. We clearly have

$$\varepsilon \chi^2 = \gamma(\varepsilon),$$

if $\varepsilon = \varepsilon_f$ is the character of f. Also, since γf and f have the same level N, the conductor of χ is divisible only by primes dividing N.

We now record some elementary facts concerning Γ.

Proposition (3.1). *Let σ and τ be embeddings of the coefficient field $E = \mathbf{Q}(\ldots a_n \ldots)$ of f into a field K. We have $\sigma = \tau\gamma$ for some $\gamma \in \Gamma$ if and only if there is a K^*-valued Dirichlet character φ such that*

$$\sigma a_p = \tau a_p \cdot \varphi(p)$$

for almost all p. Moreover, if $\sigma = \tau\gamma$, then $\varphi = \tau(\chi_\gamma)$.

Proof. Obvious.

Proposition (3.2). *For $\gamma \in \Gamma$, $\gamma(E) \subseteq E$.*

Proof. We have $\chi_\gamma^2 = \varepsilon^{\gamma - 1}$. (We use exponential notation at certain points below. Thus $\varepsilon^{\gamma - 1}$ denotes $\gamma\varepsilon \cdot \varepsilon^{-1}$.) Hence χ_γ takes values in the field $\mathbf{Q}(\varepsilon)$ generated by the values of ε. This implies

$$\gamma(a_p) = \chi_\gamma(p) \cdot a_p \in E,$$

as required, since E contains $\mathbf{Q}(\varepsilon)$.

We may thus regard Γ as a subset of the group $\operatorname{Aut}(E)$ of automorphisms of E over $\mathbf{Q}$.

Proposition (3.3). *The subset Γ of* $\operatorname{Aut}(E)$ *is in fact an Abelian subgroup. For $\gamma, \delta \in \Gamma$ we have the cocycle identity*

$$\chi_{\gamma\delta} = \chi_\gamma \cdot \gamma(\chi_\delta). \tag{3.4}$$

Proof. For $\gamma, \delta \in \Gamma$ we have for almost all p the equation

$$(\gamma\delta)(a_p) = \gamma(\chi_\delta(p) a_p) = \gamma(\chi_\delta(p)) \chi_\gamma(p) a_p,$$

which proves that Γ is a group and establishes (3.4). The fact that Γ is *Abelian*, which we will not use below, follows from the two equations

$$\chi_\gamma^2 = \varepsilon^{\gamma-1}, \quad \chi_\delta^2 = \varepsilon^{\delta-1}.$$

We now let $F = E^\Gamma$ be the *fixed field of* Γ. As Serre pointed out to the author, F is the field generated by the numbers

$$a_p^2 \varepsilon(p)^{-1}, \quad p \in S,$$

whenever S is a set of primes of density 1, contained in the set of primes not dividing N. This fact follows from an argument using l-adic representations, which we shall omit.

Proposition (3.5). *Suppose that φ is a Dirichlet character. Let $g = \sum b_n q^n$ be that newform which satisfies*

$$b_p = \varphi(p) a_p$$

for almost all p. Then the field F does not change if we replace f by g.

Proof. We regard F as the subfield of $\mathbf{C}$ cut out by the subgroup of Aut($\mathbf{C}$) consisting of those $\sigma \in \operatorname{Aut}\mathbf{C}$ such that:

There exists a Dirichlet character χ such that $\sigma a_p = \chi(p) a_p$ for almost all p.

If σ and χ satisfy this condition, then we have

$$\sigma b_p = (\chi \cdot \varphi^{\sigma-1})(p) \cdot b_p$$

for almost all p, so that the field F made for g is contained in the field F made for f. By symmetry, the two fields are equal.

Variant (3.6). We regard Dirichlet characters as functions on the maximal Abelian quotient $\operatorname{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})^{ab} \simeq \hat{\mathbf{Z}}^*$ of the Galois group of $\mathbf{Q}$. Let H be a closed subgroup of this group. It is natural to introduce the subgroup of Γ

$$\Gamma_H =: \{\gamma \in \Gamma \mid \chi_\gamma \text{ is trivial on } H\}$$

and its fixed field $F_H \supseteq F$. Especially, if H is the group $\{\pm 1\}$, the field F_H is invariant under twisting as in (3.5), since the character $\varphi^{\sigma-1}$ in the proof of (3.5) is even. The fields F_H occur in studying the l-adic representations attached to f, cf. (4.4).

Example (3.7). As is well known, E is either a CM field or a totally real field. Since f has no complex multiplication, these possibilities occur according as ε is non-trivial or trivial. Let $c: E \to E$ be the canonical "complex conjugation" of E. Then $c \in \Gamma$ and $\chi_c = \varepsilon^{-1}$, cf. [12, p. 21].

(3.8) Suppose that ε is real valued (i.e., of order 1 or 2). Then the characters χ_γ are again real valued, and Γ is an elementary 2-group. Examples where ε is trivial and where Γ has order 2 are given in [3, 5]. Examples where ε is quadratic and Γ has order 4 are the form $f^{(1)}$ of [15, Sect. 6] and the forms discussed in [15, Sect. 7]. There are presumably examples where Γ is arbitrarily large.

(3.9) *Suppose that f has trivial character* ($\varepsilon = 1$) *and N is square free. Then $\Gamma = \{1\}$; i.e., f has no "inner twists."*

More generally, we will prove

Theorem (3.9 bis). *Let f be a newform on $\Gamma_1(N)$ with N square free, possibly one with complex multiplication. Suppose that the Nebentypus character of f is trivial. Let χ be a non-trivial Dirichlet character, and let $g=\sum b_n q^n$ be that newform which satisfies*

$$b_p=\chi(p)a_p$$

for almost all p. Then the level of g is not square free.

Corollary (3.10). *If f is as in* (3.9 bis), *then in fact f does not have complex multiplication.*

Proof of (3.9 bis). Let $h=\sum c_n q^n$ be a newform of square free level M and character ε. Let π be the associated representation of $GL(2, \mathbf{A})$, and for each prime p, let π_p be the component at p of π. It is known that:

i) if $p \nmid M$, π_p is an unramified principal series representation of $\mathbf{GL}(2, \mathbf{Q}_p)$;

ii) if $p|M$ and if the character ε is ramified at p, then π_p is again a principal series representation $\pi(\mu_1, \mu_2)$ in which exactly one of the μ_i is unramified;

iii) if $p|M$ but if ε is trivial at p, then π_p is the twist by an unramified character of a "standard" special representation of $\mathbf{GL}(2, \mathbf{Q}_p)$ which does not depend on h.

(For this, cf. [2, pp. 118–119] and [4, Proposition 5.21].)

This applies in particular with π taken to be π_f or π_g, f and g being as in the statement of the theorem. For each p, we have

$$\pi_{g,p}=\pi_{f,p}\otimes\chi_p,$$

where χ_p is the component of χ at p. Given that $\pi_{f,p}$ is of types i) or iii) and that $\pi_{g,p}$ is of types i), ii) or iii), we are forced to conclude that χ_p is trivial. Since this is true for all p, χ is trivial, a contradication.

Remark. The above results are very close to those of Atkin and Li [1, Sects. 3 and 4]. See especially their (3.1) and (4.1).

(3.11) As a final example, we suppose that f is a newform whose coefficients a_n are rational. Let φ be a Dirichlet character and let g be the newform whose p-th coefficient is $\varphi(p)a_p$ for almost all p. The field of coefficients of g is the field generated by the values of φ, whereas, by (3.5), the field F made for g is just $\mathbf{Q}$. Hence, for trivial reasons, the group Γ for g may be quite large.

4. l-Adic Representations Attached to Eigenforms (of Weight 2)

Let f be a newform on $\Gamma_1(N)$ and let $\varepsilon:(\mathbf{Z}/N\mathbf{Z})^*\to\mathbf{C}^*$ be its (Nebentypus) character. As in [12], we regard ε as a character on $G=\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$, and we may view it as taking values in the coefficient field E of f. Let $A=A_f$ be the factor of $J_1(N)$ attached to f (Sect. 2).

Let l be a prime (fixed in what follows), and let $V=V_l(A)$ be the usual $\mathbf{Q}_l$-adic Tate module attached to A. Then V is simultaneously, and compatibly, a $\mathbf{Q}_l[G]$-module and a free $E\otimes\mathbf{Q}_l$-module of rank 2. The action of G on V is thus described by a map

$$\varrho: G\to \mathrm{Aut}_{E\otimes\mathbf{Q}}V\simeq \mathbf{GL}(2, E\otimes\mathbf{Q}_l),$$

which is known to be *the* l-adic representation attached to f, because of the Eichler-Shimura relation (see [15, Sect. 1] and [18, Chap. 7]). This means that ϱ is unramified at each prime p not dividing lN and that the image under ϱ of a Frobenius element $\varphi_p \in G$ for such a prime p has trace (resp. determinant) equal to a_p [resp. $\varepsilon(p)p$]. Here we calculate trace and determinant relative to $E \otimes \mathbf{Q}_l$, i.e., by viewing V as a free $E \otimes \mathbf{Q}_l$-module rather than a $\mathbf{Q}_l$-vector space. One has a great deal of information available about ϱ (cf. [12]), some of which we now recall.

Let $\bar{V}$ be the space $V \bigotimes_{\mathbf{Q}_l} \bar{\mathbf{Q}}_l$, and let $\bar{\varrho}$ be the corresponding representation of G. Thus $\bar{V}$ is free of rank 2 over $E \otimes \bar{\mathbf{Q}}_l$, an algebra which decomposes as a product of copies of $\bar{\mathbf{Q}}_l$, indexed by the enbeddings σ of E into $\bar{\mathbf{Q}}_l$. For each σ, define V_σ to be the tensor product

$$\bar{V} \bigotimes_{E \otimes \bar{\mathbf{Q}}_l} \bar{\mathbf{Q}}_l,$$

where $\bar{\mathbf{Q}}_l$ is viewed as an $E \otimes \bar{\mathbf{Q}}_l$ algebra via that $\bar{\mathbf{Q}}_l$-algebra homomorphism $E \otimes \bar{\mathbf{Q}}_l \to \bar{\mathbf{Q}}_l$ which extends σ. We have

$$\bar{V} = \prod_\sigma V_\sigma,$$

and this is just the decomposition of $\bar{V}$ imposed by the decomposition of $E \otimes \bar{\mathbf{Q}}_l$ as a product of copies of $\bar{\mathbf{Q}}_l$. We write ϱ_σ for the representation of G given by V_σ.

Proposition (4.1). *We have* $\operatorname{End}_G V = E \otimes \mathbf{Q}_l$.

Proof (*cf.* [11, *pp.* 788–789]). We introduce the decomposition $V = \prod V_\lambda$ induced by the decomposition of $E \otimes \mathbf{Q}_l$ as a product of l-adic fields E_λ. Each module V_λ is simple over $E_\lambda[G]$ [12, *p.* 29], and the action of G on V_λ is non-Abelian [12, p. 36]. Hence $\operatorname{End}_{G, E_\lambda} V_\lambda = E_\lambda$, so that $\operatorname{End}_{G, E \otimes \mathbf{Q}_l} V = E \otimes \mathbf{Q}_l$ and then

$$\operatorname{End}_{G, E \otimes \bar{\mathbf{Q}}_l} \bar{V} = E \otimes \bar{\mathbf{Q}}_l.$$

This latter equation signifies, in turn, that $\operatorname{End}_G V_\sigma = \bar{\mathbf{Q}}_l$ for each σ. Similarly, the V_σ are semi-simple as G-modules (i.e. as $\bar{\mathbf{Q}}_l[G]$-modules) because the V_λ are simple. Hence V_σ is in fact simple, putting the two statements together. Thus the statement to be proved, which we rewrite

$$\operatorname{End}_G \bar{V} = E \otimes \bar{\mathbf{Q}}_l,$$

signifies that the V_σ are pairwise non-isomorphic $\bar{\mathbf{Q}}_l$ [G]-modules. However, if V_σ and V_τ are G-isomorphic, we find (taking traces) that

$$\sigma a_p = \tau a_p$$

for almost all p, which implies that σ and τ are equal.

Corollary (4.2). *We have* $(\operatorname{End}_{\mathbf{Q}} A) \otimes \mathbf{Q} = E$. *In particular, A is a simple Abelian variety over* $\mathbf{Q}$.

Proof. The first statement follows because E is *a priori* given as a subalgebra of $(\operatorname{End}_{\mathbf{Q}} A) \otimes \mathbf{Q}$ and because of the embedding

$$(\operatorname{End}_{\mathbf{Q}} A) \otimes \mathbf{Q}_l \hookrightarrow \operatorname{End}_G V.$$

The second statement follows from the first because an Abelian variety is simple if and only if its endomorphism algebra is a (skew) field.

For more delicate questions, we distinguish the case where f has complex multiplication in the sense of [12]: there is a non-trivial Dirichlet character φ such that $\varphi(p)a_p = a_p$ for almost all p. The character φ is then necessarily the real character corresponding to an imaginary quadratic field k, and we say that f has complex multiplication by k. The "CM" case may be characterized as that where the modules V_λ become Abelian on some open subgroup of G [12, (4.4)], and as that where f is derived from a Hecke character ψ of k which satisfies

$$\psi((\alpha)) = \alpha$$

for all $\alpha \in k^*$ which are "multiplicatively" congruent to 1, modulo the conductor of ψ [12, (4.5)]. If f has complex multiplication, then A is isogenous over $\bar{\mathbf{Q}}$ to a power of an elliptic curve with complex multiplication by k [14]. On the other hand, if A has *some* factor of CM type, then f has complex multiplication [15, Proposition 1.6].

Remark (4.3). If f does *not* have complex multiplication, then [12, (4.4)] the action of each open subgroup H of G is non-Abelian on each module V_λ. It follows as in the proof of (4.1) that we have

$$\mathrm{End}_H V_\sigma = \bar{\mathbf{Q}}_l$$

for each embedding σ of E into $\bar{\mathbf{Q}}_l$. We will use this fact in making calculations involving $\mathrm{End}_H V$. (Here, and below, we use $\mathrm{End}_H \ldots$ as an abbreviation for $\mathrm{End}_{\bar{\mathbf{Q}}_l[H]} \ldots$.)

For the next result, we suppose that f is a form which does *not* have complex multiplication. We recall the subgroups Γ_H of Γ and their fixed fields F_H introduced in (3.6). For each closed subgroup H of G, we write simply Γ_H and F_H for the objects $\Gamma_{\bar{H}}$, $F_{\bar{H}}$ where $\bar{H}$ is the image of H in $\hat{\mathbf{Z}}^*$ under the map $G \to \mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})^{ab} \simeq \hat{\mathbf{Z}}^*$.

Theorem (4.4). *For each open subgroup H of G, we have isomorphisms*

$$(\mathrm{End}_H V) \bigotimes_{\mathbf{Q}_l} \bar{\mathbf{Q}}_l \simeq (\mathrm{End}_{F_H} E) \bigotimes_{\mathbf{Q}} \bar{\mathbf{Q}}_l .$$

Proof. To begin with, we have

$$(\mathrm{End}_H V) \bigotimes_{\mathbf{Q}_l} \bar{\mathbf{Q}}_l \simeq \mathrm{End}_{\bar{\mathbf{Q}}_l[H]} \bar{V} .$$

Now $\bar{V}$ breaks up into a sum of modules V_σ, each of which is simple as an H-module and satisfies moreover

$$\mathrm{End}_H V_\sigma = \bar{\mathbf{Q}}_l .$$

Thus to compute $\mathrm{End}_H \bar{V}$, we have only to determine when V_σ and V_τ are isomorphic as H-modules, for σ and τ two embeddings of E into $\bar{\mathbf{Q}}_l$. It is easy to see that this occurs if and only if there is a character of finite order

$$\varphi : G \to \bar{\mathbf{Q}}_l^* ,$$

trivial on H, such that V_σ and $V_\tau \otimes \varphi$ are isomorphic as G-modules. This condition easily translates into the equality: $\sigma a_p = (\tau a_p)\varphi(p)$ for almost all p. By (3.1) this occurs if and only if $\sigma = \tau\gamma$ for some $\gamma \in \Gamma_H$. Let Σ_l be the set of embeddings $\sigma: E \to \bar{\mathbf{Q}}_l$. Then we have

$$\operatorname{End}_H \bar{V} = \prod_{\sigma \in \Sigma_l/\Gamma_H} \operatorname{End}_H\Big(\prod_{\gamma \in \Gamma_H} V_{\sigma\gamma}\Big) \approx \mathbf{M}(a, \bar{\mathbf{Q}}_l)^b,$$

where

$$a = \# \Gamma_H = [E : F_H]$$
$$b = \# (\Sigma_l/\Gamma_H) = [F_H : \mathbf{Q}].$$

This proves the theorem since

$$(\operatorname{End}_{F_H} E) \otimes \bar{\mathbf{Q}}_l \simeq \mathbf{M}(a, F_H) \bigotimes_{\mathbf{Q}} \bar{\mathbf{Q}}_l \approx \mathbf{M}(a, \bar{\mathbf{Q}}_l)^b.$$

Continuing to assume that f has no complex multiplication, we derive from (4.4) a description of the l-adic Lie algebra attached to ϱ. More precisely, the image $\varrho(G)$ of ϱ is an l-adic Lie group and its Lie algebra $\mathfrak{g}$ is a subalgebra of $\mathfrak{gl}(V)$, an algebra which we may view as $\operatorname{End} V$, furnished with its usual Lie algebra multiplication.

It is obvious from (4.4) that the algebras $\operatorname{End}_H V$ (as H varies) form subalgebras of a certain algebra $\mathscr{X}$ which is equal to $\operatorname{End}_H V$ whenever H is "sufficiently small" in the sense that it is contained in the kernels of all $\chi_\gamma (\gamma \in \Gamma)$. We then have $\operatorname{End}_{\mathfrak{g}} V = \mathscr{X}$, which implies that $\mathfrak{g}$ is contained in $\operatorname{End}_{\mathscr{X}} V$. A second constraint arises from the fact that the determinant of ϱ (taken, as usual, relative to $E \otimes \mathbf{Q}_l$) is the product of a character of finite order and the l-adic cyclotomic character, which is $\mathbf{Q}_l^*$-valued and of infinite order. We have then $\mathfrak{g} \subseteq \mathfrak{h}$, where we define

$$\mathfrak{h} = \{m \in \operatorname{End}_{\mathscr{X}} V \mid \operatorname{tr} m \in \mathbf{Q}_l\};$$

but, on the other hand, $\mathfrak{g}$ is *not* contained in

$$\{m \in \operatorname{End}_{\mathscr{X}} V \mid \operatorname{tr} m = 0\},$$

which is the semisimple part of $\mathfrak{h}$. Another fact is that $\mathfrak{g}$ is reductive, since the representation ϱ is semisimple.

Proposition (4.5). *We have* $\mathfrak{g} = \mathfrak{h}$.

Proof. We again work over $\mathbf{Q}_l$, and we set

$$\bar{\mathscr{X}} = \mathscr{X} \bigotimes_{\mathbf{Q}_l} \bar{\mathbf{Q}}_l, \quad \bar{\mathfrak{g}} = \mathfrak{g} \bigotimes_{\mathbf{Q}_l} \bar{\mathbf{Q}}_l, \quad \bar{\mathfrak{h}} = \mathfrak{h} \bigotimes_{\mathbf{Q}_l} \bar{\mathbf{Q}}_l.$$

We have $\bar{\mathfrak{g}} \subseteq \bar{\mathfrak{h}}$. For $\sigma \in \Sigma_l$, we look at the image $\bar{\mathfrak{g}}_\sigma$ of $\bar{\mathfrak{g}}$ in $\operatorname{End} V_\sigma = \mathfrak{gl}(V_\sigma)$. Since $\operatorname{End}_{\bar{\mathfrak{g}}} V_\sigma = \bar{\mathbf{Q}}_l$, and since $\bar{\mathfrak{g}}_\sigma$ is reductive but not contained in $\mathfrak{sl}(V_\sigma)$, we find easily that $\bar{\mathfrak{g}}$ (and hence $\bar{\mathfrak{h}}$) maps onto $\mathfrak{gl}(V_\sigma)$. If there is only one σ, i.e. if $E = \mathbf{Q}$, the proof is complete.

Supposing that this is not the case, we consider, for each pair $\sigma, \tau \in \Sigma_l$ with $\sigma \neq \tau$, the images $\bar{\mathfrak{g}}_{\sigma,\tau}$ and $\bar{\mathfrak{h}}_{\sigma,\tau}$ of $\bar{\mathfrak{g}}$ and $\bar{\mathfrak{h}}$ in $\mathfrak{gl}(V_\sigma \times V_\tau)$. We find that V_σ and V_τ are $\bar{\mathfrak{g}}$-

isomorphic if and only if $\sigma=\tau\gamma$ for some $\gamma\in\Gamma$, by using the information obtained in the proof of (4.4). If this is *not* the case, it follows by a standard analysis (cf. [13, p. 325]) that $\bar{\mathfrak{g}}_{\sigma\tau}$ (and hence $\bar{\mathfrak{h}}_{\sigma\tau}$) is equal to the image in $\mathfrak{gl}(V_\sigma\times V_\tau)$ of

$$\{m\in \operatorname{End}\bar{V}\,|\,\operatorname{tr} m\in\bar{\mathbf{Q}}_l\},$$

namely

$$\{(m_\sigma,m_\tau)\in \mathfrak{gl}(V_\sigma)\times\mathfrak{gl}(V_\tau)\,|\,\operatorname{tr} m_\sigma=\operatorname{tr} m_\tau\}.$$

If V_σ and V_τ are $\bar{\mathfrak{g}}$-isomorphic, they are also $\bar{\mathfrak{h}}$ isomorphic because of the double commutant theorem. (We have

$$\bar{\mathscr{X}}=\operatorname{End}_{\bar{\mathfrak{g}}}\bar{V}\supseteqq \operatorname{End}_{\bar{\mathfrak{h}}}\bar{V}\supseteqq \operatorname{End}_{\mathscr{A}}\bar{V},$$

where $\mathscr{A}=\operatorname{End}_{\bar{\mathscr{X}}}\bar{V}$, and the right hand group is again $\bar{\mathscr{X}}$.) We have then

$$\bar{\mathfrak{g}}_{\sigma\tau}=\bar{\mathfrak{h}}_{\sigma\tau}=\{(m_\sigma,m_\tau)\,|\,m_\sigma=i^{-1}m_\tau i\},$$

where

$$i:V_\sigma\xrightarrow{\sim}V_\tau$$

is an $\bar{\mathfrak{h}}$-isomorphism. (Note that i is well defined up to multiplication by scalars in $\bar{\mathbf{Q}}_l^*$.)

Thus, to summarize, we have $\bar{\mathfrak{g}}_{\sigma\tau}=\bar{\mathfrak{h}}_{\sigma\tau}$ for *all* pairs of distinct embeddings σ, τ in Σ_l. Using the fact that $\bar{\mathfrak{g}}$ and $\bar{\mathfrak{h}}$ each have Abelian parts of dimension 1, we may deduce the equality $\bar{\mathfrak{g}}=\bar{\mathfrak{h}}$, and thus the proposition, from the following result.

Lemma (4.6). *Let Σ be a finite set, and for each $\sigma\in\Sigma$ let $\mathfrak{s}_\sigma$ be a finite-dimensional simple Lie algebra, over a field of characteristic* 0. *Let* $\mathfrak{g}$ *and* $\mathfrak{h}$ *be subalgebra of* $\prod_\sigma \mathfrak{s}_\sigma$, *with* $\mathfrak{g}\subseteqq\mathfrak{h}$. *Suppose that*

1) $\mathfrak{h}$ *maps onto each factor* $\mathfrak{s}_\sigma$.
2) $\mathfrak{g}$ *and* $\mathfrak{h}$ *have equal images in* $\mathfrak{s}_\sigma\times\mathfrak{s}_\tau$, *for* $\sigma\neq\tau$.

The $\mathfrak{g}$ *and* $\mathfrak{h}$ *are equal.*

Proof. By the Lie algebra version of Goursat's lemma (cf. [11, Lemma (5.2.1)]), the image of $\mathfrak{h}$ in $\mathfrak{s}_\sigma\times\mathfrak{s}_\tau$ is either all of $\mathfrak{s}_\sigma\times\mathfrak{s}_\tau$, or else the graph of an isomorphism $\mathfrak{s}_\sigma\simeq\mathfrak{s}_\tau$. For $\sigma,\tau\in\Sigma$, we say that σ and τ are *equivalent* if the kernels of the two projections

$$\mathfrak{h}\to\mathfrak{s}_\sigma,\quad \mathfrak{h}\to\mathfrak{s}_\tau$$

are equal. Let $A\subset\Sigma$ be a set of representatives for the equivalence classes under this equivalence. Then, clearly, the map

$$\mathfrak{h}\to\prod_{\sigma\in A}\mathfrak{s}_\sigma$$

is an injection. It is surjective by [11, Lemma, p. 790], since $\mathfrak{h}$ maps onto each partial product $\mathfrak{s}_\sigma\times\mathfrak{s}_\tau$. Similarly, the composite

$$\mathfrak{g}\hookrightarrow\mathfrak{h}\to\prod_{\sigma\in A}\mathfrak{s}_\sigma$$

is surjective. Hence $\mathfrak{g}=\mathfrak{h}$ as required.

We now remove the assumption that f has no complex multiplication, and we introduce a second newform $f' = \sum a'_n q^n$. We let $E', A', V', \ldots$ be the objects for f' which correspond to $E, A, V \ldots$ for f.

Theorem (4.7). *The following statements are equivalent:*

1) *there exists an open subgroup H of G such that* $\mathrm{Hom}_H(V, V') \neq 0$.

2) *The Abelian varieties A and A' are each isogenous to powers of the same Abelian variety over $\bar{\mathbf{Q}}$.*

3) *Either f and f' have complex multiplication by the same quadratic field k, or else there are embeddings*

$$\sigma: E \to \mathbf{C}, \quad \sigma': E' \to \mathbf{C}$$

and a Dirichlet character χ such that

$$\sigma'(a'_p) = \sigma(a_p)\chi(p)$$

for almost all p.

Proof. 3)$\Rightarrow$2). If f and f' each have complex multiplication by k, then A and A' are each isogenous over $\bar{\mathbf{Q}}$ to powers of an elliptic curve with complex multiplication by k. Up to isogeny there is only one such curve, so we get (2). We next suppose that f and f$'$ do not each have complex multiplication by the same field k, but that we have $a'_p = \chi(p) a_p$ for almost all p. Then, in fact, neither f nor f' has complex multiplication, so that both A and A' have no Abelian subvarieties of CM type. From this we may easily deduce that E is its own commutant in $(\mathrm{End}\, A) \otimes \mathbf{Q}$ (and similarly for E') as in the proof of Theorem (2.3) of [10]. Hence the center of $(\mathrm{End}\, A) \otimes \mathbf{Q}$ is a field, so that, over $\bar{\mathbf{Q}}$, A is isogenous to a power of *some* Abelian variety. Similarly for A'. Thus, to prove 2), it suffices to show that A' is a quotient of a power of A, or vice versa.

This is precisely what would follow from Proposition 7 of Shimura [16] under the assumption that we have an equality

$$\sum \sigma' a'_n q^n = \sum \sigma a_n \chi(n) q^n .$$

(Note that $A = A_{\sigma f}$, $A' = A_{\sigma' f'}$.) A priori, however, we have an equality only for terms corresponding to those n which are prime to $r = \mathrm{cond}\, \chi$. Therefore, we let

$$g = \sum_{(n,r)=1} a'_n q^n ,$$

so that A_g *is* a quotient of a power of A, by Shimura's theorem. Since A_g and A' are isogenous (2.4), we get (2).

2)$\Rightarrow$1). Under the assumption 2), we have

$$\mathrm{Hom}_{\bar{\mathbf{Q}}}(A, A') \neq 0$$

so that

$$\mathrm{Hom}_K(A, A') \neq 0$$

for some number field K. Letting H be $\mathrm{Gal}(\bar{\mathbf{Q}}/K)$, we obtain 1).

1)⇒3). Assuming 1), we may choose embeddings $\sigma\in\Sigma_l$, $\tau\in\Sigma'_l$ such that

$$\mathrm{Hom}_H(V_\sigma, V'_\tau)\neq 0.$$

This means that some submodule of V_σ is isomorphic to some submodule of V_τ. (The modules in question are of course semisimple.) For a form with complex multiplication, the V_σ are Abelian (and reducible) on a subgroup of index 2 in G; for a form without complex multiplication, the V_σ are non-Abelian (and simple) on each open subgroup of G. Hence it is clear that either f and f' each have complex multiplication or else neither form has complex multiplication.

In the latter case, we have an isomorphism of H-modules

$$V_\sigma\approx V'_\tau,$$

so that there is a character $\varphi: G\to\bar{\mathbf{Q}}_l^*$, trivial on H, such that

$$V'_\tau\approx V_\sigma\otimes\varphi$$

as G-modules. This gives the equation

$$\tau(a'_p)=\sigma(a_p)\varphi(p)$$

for almost all p, which leads to 3).

In the former case, we have to prove that f and f' have complex multiplication by the *same* field. This reduces to the Tate conjecture for homomorphisms between elliptic curves with complex multiplication, since A and A' are each isogenous to powers of such curves. This case of the conjecture is well known (cf. the remarks in [13, p. 329]).

5. Endomorphisms of the Varieties A_f

Let $f=\sum a_n q^n$ be a newform on $\Gamma_1(N)$, and let A be the variety A_f. Our aim in this section is to calculate the endomorphism algebra $(\mathrm{End}\,A)\otimes\mathbf{Q}$ of A. Since A is a power of a CM elliptic curve when f has complex multiplication, we may consider this case to be understood. Therefore, we assume for the remainder of this section that f does not have complex multiplication. This enables us to speak of group Γ and its fixed field F (Sect. 3). We let E be, as usual, the coefficient field of f.

Theorem (5.1). *The endomorphism algebra of A is a central simple algebra over F which contains E as a maximal commutative subfield. Its degree over $\mathbf{Q}$ is $[E:\mathbf{Q}]\cdot[E:F]$.*

Remarks. 1) The second statement of (5.1) follows from the first because the degree over F of a central simple algebra over F having E as a maximal commutative subfield must be $[E:F]^2$.

2) Theorem (4.4) shows that the degree over $\mathbf{Q}$ of $(\mathrm{End}\,A)\otimes\mathbf{Q}$ is *at most* $[E:\mathbf{Q}]\cdot[E:F]$. Hence to prove (5.1), it suffices to show that $(\mathrm{End}\,A)\otimes\mathbf{Q}$ *contains* an algebra as described in (5.1).

The proof of (5.1) is the object of this section.

We first note that we may replace A in (5.1) by "the" Abelian variety A_h associated to

$$h = \sum_{(n,N)=1} a_n q^n,$$

in view of (2.4). In defining this Abelian variety, we in fact use a subgroup of $SL_2\mathbf{Z}$ which is *not* of the form $\Gamma_1(M)$. Namely, let m be the least common multiple of N and the conductors of the characters χ_γ for $\gamma \in \Gamma$. It is easy to see that h is an eigenform when considered as a modular form on the group

$$\left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(m^2) \middle| a \equiv d \equiv 1 \pmod{m} \right\}.$$

Using Shimura's construction described in Sect. 2, we attach to h an Abelian variety $B = A_h$ using this group. Then B is given as a quotient of the Jacobian J of the modular curve made with this group; as in Sect. 2, we let

$$v : J \to B$$

be the structural map.

We let S be the space of (weight 2 cusp) forms on this group and write T for the subspace $v^*(\Omega_{B/\mathbf{C}})$ of S. Then T is generated by h and its conjugates σh ($\sigma \in \mathrm{Aut}\,\mathbf{C}$). For $\sigma \in \mathrm{Aut}\,\mathbf{C}$, we let $\omega_\sigma \in \Omega_{B/\mathbf{C}}$ be the differential on B corresponding to σh in T. (Note that v^* is injective because v is surjective.) We view E as a ring of endomorphisms of $B \otimes \mathbf{Q}$, the Abelian variety B considered as a variety "up to isogeny." In particular, E acts by pullback on $\Omega_{B/\mathbf{C}}$, and we have for $e \in E$ the formula

(5.2) $\quad e^*(\omega_\sigma) = \sigma e \cdot \omega_\sigma,$

in which σe is the *complex number* obtained by applying σ to e. [To verify (5.2) we may assume that e is a coefficient a_n of E, and after we apply v^*, (5.2) becomes the identity

$$\sigma h | T_n = \sigma(a_n) \cdot \sigma h.]$$

Now let γ be an element of Γ, and let $\chi = \chi_\gamma$ be the corresponding character. Let r be the conductor of χ. For $u \in \mathbf{Z}$, let $\alpha_{u/r}$ be the endomorphism (denoted α_u in Sect. 2) whose action on S is given by slashing by the matrix $\begin{pmatrix} 1 & \frac{u}{r} \\ 0 & 1 \end{pmatrix}$. Let $\bar{\alpha}_{u/r}$ be the composite

$$v \circ \alpha_{u/r} : J \to B.$$

Let

$$\tilde{\eta}_\gamma : J \to B$$

be defined by the sum $\sum_{u \bmod r} \chi^{-1}(u) \circ \bar{\alpha}_{u/r}$, in which the $\chi^{-1}(u)$ are understood to be elements of E, so that $\tilde{\eta}_\gamma$ is a homomorphism of Abelian varieties up to isogeny. For the moment, we write simply $\tilde{\eta}$ for $\tilde{\eta}_\gamma$.

Claim (5.3). We have $\tilde{\eta}^*(\Omega_{B/\mathbf{C}}) \subseteq T$.

Proof. It suffices to show that $\tilde{\eta}^*(\omega_\sigma)$ belongs to T for each σ. Using (5.2) and the definitions, we find

$$\tilde{\eta}^*(\omega_\sigma) = \sum_{u \bmod r} \chi^{-\sigma}(u) \cdot \sigma h \left| \begin{pmatrix} 1 & \frac{u}{r} \\ 0 & 1 \end{pmatrix} \right.,$$

where we have written $\chi^{-\sigma}$ for the character $\sigma\chi^{-1}$. For a primitive character of conductor c we define as usual

$$g(\varphi) = \sum_{u=1}^{c} \varphi(u) e^{2\pi i u/c}.$$

Then we find by a well known calculation,

$$\tilde{\eta}^*(\omega_\sigma) = g(\chi^{-\sigma}) \sum_{n=1}^{\infty} \sigma\chi(n) \sigma a_n q^n$$
$$= g(\chi^{-\sigma})[\sigma\gamma(h)] \in T.$$

By (5.3), the map $\tilde{\eta}: J \to B$ factors across the quotient $v: J \to B$, so that there is an *endomorphism* η_γ of $B \otimes \mathbf{Q}$ with the property that $\eta_\gamma \circ v = \tilde{\eta}$. Note that η_γ is uniquely determined by this property and as a consequence is defined over the field of r-th roots of unity, since the $\alpha_{u/r}$ are defined over this field. The computation performed in the proof of (5.3) gives the formula

(5.4) $\quad \eta_\gamma^*(\omega_\sigma) = g(\chi_\gamma^{-\sigma}) \omega_{\sigma\gamma}$

for all $\sigma: E \to \mathbf{C}$ and all $\gamma \in \Gamma$.

For γ, $\delta \in \Gamma$, let

$$c(\gamma, \delta) = \frac{g(\chi_\gamma^{-1}) g(\chi_\delta^{-\gamma})}{g(\chi_{\gamma\delta}^{-1})}.$$

Since the product of the two characters in the numerator is the character in the denominator (3.4), $c(\gamma, \delta)$ may be interpreted as a "Jacobi sum." [Note that $\chi_\delta^{-\gamma}$ means $\gamma(\chi_\delta^{-1})$.] One knows that $c(\gamma, \delta)$ is an element of E such that

$$\sigma c(\gamma, \delta) = \frac{g(\chi_\gamma^{-\sigma}) g(\chi_\delta^{-\sigma\gamma})}{g(\chi_{\gamma\delta}^{-\sigma})}$$

for all $\sigma: E \to \mathbf{C}$ [17, p. 797]. We view $c(\gamma, \delta)$ as an element of $(\operatorname{End} B \otimes \mathbf{Q})$, whereas the $\sigma c(\gamma, \delta)$ are to be interpreted as complex numbers. Here are some formulas involving the $c(\gamma, \delta)$ and elements of E:

(5.5) For $e \in E$ and $\gamma \in \Gamma$ we have $\eta_\gamma \cdot e = \gamma(e) \cdot \eta_\gamma$.

Proof. Both sides of the equation are elements of $(\operatorname{End} B) \otimes \mathbf{Q}$, and to check this equality it suffices to verify that they have the same action on the basis $\{\omega_\sigma\}$ of

$\Omega_{B/\mathbf{C}}$. We have

$$(\eta_\gamma e)^*(\omega_\sigma) = e^*(g(\chi_\gamma^{-\sigma})\omega_{\sigma\gamma}) = (\sigma\gamma)(e)g(\chi_\gamma^{-\sigma})\omega_{\sigma\gamma};$$

$$(\gamma(e)\eta_\gamma)^*(\omega_\sigma) = \sigma\gamma(e)\eta_\gamma^*(\omega_\sigma) = \sigma\gamma(e)g(\chi_\gamma^{-\sigma})\omega_{\sigma\gamma}.$$

(5.6) For $\gamma, \delta \in \Gamma$ we have

$$\eta_\gamma \cdot \eta_\delta = c(\gamma, \delta) \cdot \eta_{\gamma\delta}.$$

Proof. This follows by a similar computation. We have

$$(c(\gamma, \delta)\eta_{\gamma\delta})^*(\omega_\sigma) = \sigma c(\gamma, \delta)g(\chi_{\gamma\delta}^{-\sigma})\omega_{\sigma\gamma\delta} = g(\chi_\gamma^{-\sigma})g(\chi_\delta^{-\sigma\gamma})\omega_{\sigma\gamma\delta},$$

and similarly the operator $\eta_\gamma\eta_\delta$ has the identical effect on ω_σ.

(5.7) The map $c: \Gamma \times \Gamma \to E^*$ is a cocycle: for $\gamma_1, \gamma_2, \gamma_3 \in \Gamma$ we have

$$c(\gamma_1, \gamma_2) \cdot c(\gamma_1\gamma_2, \gamma_3) = [\gamma_1 \cdot c(\gamma_2, \gamma_3)] \cdot c(\gamma_1, \gamma_2\gamma_3).$$

Proof. This formula may be verified directly from the definition. Alternatively, by computing $\eta_{\gamma_1} \cdot \eta_{\gamma_2} \cdot \eta_{\gamma_3}$ in two different ways, one finds that the two sides become equal after right multiplication by $\eta_{\gamma_1\gamma_2\gamma_3} \in \mathrm{End}(B \otimes \mathbf{Q})$. This latter element is inversible (it acts invertibly on $\Omega_{B/\mathbf{C}}$), so the formula must hold.

The above formulas show that the algebra generated by E and the η_γ in $(\mathrm{End} B) \otimes \mathbf{Q}$ is a homomorphic image of a certain algebra $\mathscr{X}$ which is constructed beginning with the Galois extension E/F and the 2-cocycle c on its Galois group Γ. Namely, let $\mathscr{X}$ first be the E-vector space

$$\mathscr{X} = \bigoplus_{\gamma \in \Gamma} E \cdot X_\gamma,$$

where the X_γ are formal symbols. By imposing on the X_γ the rules

(5.5 bis) $X_\gamma \cdot e = \gamma(e) X_\gamma$ for $e \in E$ and $\gamma \in \Gamma$

(5.6 bis) $X_\gamma X_\delta = c(\gamma, \delta) X_{\gamma\delta}$,

we make $\mathscr{X}$ into an *associative algebra*. It is well known that $\mathscr{X}$ is a *central simple* algebra over F, the so-called "crossed product algebra" defined by the cocycle c [9, Theorem 29.6].

To complete the proof of (5.1), we have only to remark that the map

$$\mathscr{X} \to (\mathrm{End} B) \otimes \mathbf{Q} \approx (\mathrm{End} A) \otimes \mathbf{Q}$$

is *injective* because $\mathscr{X}$ has no two-sided ideals. It is then surjective, as already remarked above, by (4.4).

Remark (5.8). Let M be the Γ-module consisting of E^*-valued Dirichlet characters. It is easy to show that the construction of the 2-cocycle c beginning with the

M-valued 1-cocycle $b:\gamma\mapsto\chi_\gamma$ defines in fact a homomorphism

$$\delta:H^1(\Gamma,M)\to H^2(\Gamma,E^*).$$

It follows in particular that c has order dividing 2 in $H^2(\Gamma,E^*)$, since the square of b is the 1-coboundary $\gamma\mapsto\varepsilon^{\gamma-1}$. Now we may identify $H^2(\Gamma,E^*)$ with a subgroup of the Brauer group $\mathrm{Br}(F)$ of F, in such a way that the class of c in $H^2(\Gamma,E^*)$ is mapped to the class of $\mathscr{X}$ in $\mathrm{Br}(F)$. A consequence is the fact that $\mathscr{X}$ has order 1 or 2 in $\mathrm{Br}(F)$, meaning that $\mathscr{X}$ is either a matrix algebra over F, or else a matrix algebra over a quaternion division algebra with center F.

In general, it does not seem easy to distinguish between these two possibilities by "pure thought." However, one may show at least that $\mathscr{X}$ is a matrix algebra over F in the case where all characters χ_γ are even [i.e., satisfy $\chi_\gamma(-1)=1$], by making a local study suggested by the proof of ([12], Corollary 5.2). Further, $\mathscr{X}$ is again a matrix algebra if the abelian variety A_f has "potential multiplicative reduction" at some prime p of $\mathbf{Q}$, as we may see by ([11], Corollary (3.3.9)).

6. Applications

Theorem (6.1). *Let N and M be positive integers, let l be a prime number, and let k be a finite extension of* $\mathbf{Q}$ *in* $\bar{\mathbf{Q}}$. *Then the natural map*

$$\alpha_{K,l}:\mathrm{Hom}_K(J_1(N),J_1(M))\otimes\mathbf{Q}_l\hookrightarrow\mathrm{Hom}_{\mathrm{Gal}(\bar{\mathbf{Q}}/K)}(V_l(J_1(N)),V_l(J_1(M))),$$

a priori injective, is an isomorphism.

Proof. We know that $J_1(N)$ is isogenous to a product $\prod A_f$ of Abelian varieties attached to newforms (2.3), and that $J_1(M)$ is similarly isogenous to a product $\prod A_g$. Hence it suffices to treat the situation, analogous to that of the theorem, in which $J_1(N)$ and $J_1(M)$ have been replaced by varieties A_f and A_g respectively. The map α in question is certainly an isomorphism whenever the right-hand group is zero. Hence, by (4.7), we may confine our attention to the case where A_f and A_g are each isogenous to powers of the *same* Abelian variety over $\bar{\mathbf{Q}}$, and hence over some number field K_0. In verifying that $\alpha_{K,l}$ is an isomorphism, it is legitimate to consider only those K which are "sufficiently large" and, in particular, those containing K_0. Under this assumption, the question involving homomorphisms $A_f\to A_g$ reduces to the analogous question for *endomorphisms* of A_f.

Thus, to summarize, for (6.1) it is enough to show that the injection

$$\alpha_{K,l}:(\mathrm{End}_K A_f)\otimes\mathbf{Q}_l\to\mathrm{End}_{\mathrm{Gal}(\bar{\mathbf{Q}}/K)}(V_l(A_f))$$

is an isomorphism for all newforms f and all number fields K. In the case where f has complex multiplication, A_f is just a power of a CM elliptic curve, and this fact is well known, as we mentioned earlier. We now assume that f does *not* have complex multiplication. We consider (as we may) only those K such that $\mathrm{Gal}(\bar{\mathbf{Q}}/K)$ is contained in the kernel of all the characters $\chi_\gamma(\gamma\in\Gamma)$ and such that all endomorphisms of A_f are defined over K. The left-hand side then has ($\mathbf{Q}_l$-) dimension $[E:\mathbf{Q}]\cdot[E:F]$, by (5.1). The right-hand side has the same dimension, by (4.4). Hence $\alpha_{K,l}$, known to be injective, is an isomorphism as needed.

Now let N be a square-free integer, and let A be the product

$$\prod_{M|N} J_0(M)^{\mathrm{new}},$$

where $J_0(M)^{\mathrm{new}}$ is the "new part" of $J_0(M)$ defined as in Sect. 2. Thus

$$J_0(M)^{\mathrm{new}}=\prod A_f,$$

where f runs over the set of newforms on $\Gamma_0(M)$, modulo the action of Aut**C**. Therefore, A is a similar product, running over forms f of level *dividing* N. We have for each f,

$$E_f \subseteqq (\mathrm{End}\, A_f)\otimes \mathbf{Q},$$

so that

$$E=\prod E_f$$

is naturally a subalgebra of $(\mathrm{End}\,A)\otimes\mathbf{Q}$.

Theorem (6.2). *We have* $E=(\mathrm{End}\,A)\otimes\mathbf{Q}$.

[This was proved as Proposition (3.2) in [10] by a method which relied on the Deligne-Rapoport study of $J_0(N)$ at primes dividing N.]

Proof. For A_f and $A_{f'}$, two *different* factors of A, we have $\mathrm{Hom}(A_f, A_{f'})=0$. Indeed, were $\mathrm{Hom}(A_f, A_{f'})$ non-zero, there would be by (4.7) and (3.10) automorphisms σ and σ' of **C**, and a Dirichlet character χ, such that

$$\sigma'(a'_p)=\chi(p)\sigma(a_p)$$

for almost all p. [Here we have adopted the notation

$$f=\sum a_n q^n, \qquad f'=\sum a'_n q^n$$

of (4.7).] By (3.9 bis), the character χ would be trivial, so that f' would be a conjugate of f, implying that $A_{f'}=A_f$.

The prove the theorem, it is therefore enough to show that

$$(\mathrm{End}\,A_f)\otimes\mathbf{Q}=\mathbf{E}_f$$

for each f. Since f does not have complex multiplication (3.10), we may apply (5.1) to compute the degree over **Q** of $(\mathrm{End}\,A_f)\otimes\mathbf{Q}$. By (5.1) and (3.9), this degree is $[E_f:\mathbf{Q}]$.

References

1. Atkin, A.O.L., Li, W.-C.: Twists of newforms and pseudo-eigenvalues of W-operators. Invent. Math. **48**, 221–243 (1978)
2. Casselman, W.: On representations of GL_2 and the arithmetic of modular curves. In: Lecture Notes in Mathematics No. 349, pp. 107–141. Berlin, Heidelberg, New York: Springer 1973
3. Doi, K., Yamauchi, M.: On the Hecke operators for $\Gamma_0(N)$ and class fields over quadratic number fields. J. Math. Soc. Japan **25**, 629–643 (1973)
4. Gelbart, S.: Automorphic forms on Adele groups. Princeton: Princeton University Press 1975
5. Koike, M.: On certain Abelian varieties obtained from new forms of weight 2 on $\Gamma_0(3^4)$ and $\Gamma_0(3^5)$. Nagoya Math. J. **62**, 29–39 (1976)

6. Li, W.-C.: Newforms and functional equations. Math. Ann. **212**, 285–315 (1975)
7. Mazur, B.: Rational isogenies of prime degree. Invent. Math. **44**, 129–162 (1978)
8. Miyake, T.: On automorphic forms on GL_2 and Hecke operators. Ann. of Math. **94**, 174–189 (1971)
9. Reiner, I.: Maximal orders. New York: Academic Press 1975
10. Ribet, K.: Endomorphisms of semi-stable Abelian varieties over number fields. Ann. of Math. **101**, 555–562 (1975)
11. Ribet, K.: Galois action on division points of Abelian varieties with many real multiplications. Am. J. Math. **98**, 751–804 (1976)
12. Ribet, K.: Galois representations attached to eigenforms with nebentypus. Lecture Notes in Mathematics. No. 601, pp. 17–52, Berlin, Heidelberg, New York: Springer 1977
13. Serre, J.-P.: Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. Invent. Math. **15**, 259–331 (1972)
14. Shimura, G.: On elliptic curves with complex multiplication as factors of the Jacobians of modular function fields. Nagoya Math. J. **43**, 199–208 (1971)
15. Shimura, G.: Class fields over real quadratic fields and Hecke operators. Ann. of Math. **95**, 130–190 (1972)
16. Shimura, G.: On the factors of the Jacobian variety of a modular function field. J. Math. Soc. Japan **25**, 523–544 (1973)
17. Shimura, G.: The special values of the zeta functions associated with cusp forms. Comm. Pure Appl. Math. **29**, 783–804 (1976)
18. Shimura, G.: Introduction to the arithmetic theory of automorphic functions. Princeton: Princeton University Press 1971
19. Tate, J.: Algebraic cycles and poles of zeta functions. In: Arithmetical algebraic geometry. New York: Harper and Row 1966
20. Tunnell, J.: Cycles on the product of two Shimura curves and poles of zeta-functions (to appear)

Received February 21, 1980, in revised form April 11, 1980