MULTIPLICITIES OF GALOIS REPRESENTATIONS IN JACOBIANS OF SHIMURA CURVES

BY

KENNETH A. RIBET*

Mathematics Department, University of California, Berkeley CA 94720 USA

Let p and q be distinct primes. The new part of $J_o(pq)$ (defined, according to one's taste, as a quotient or subvariety of $J_o(pq)$) is known to be isogenous to the Jacobian J of the Shimura curve derived from the rational quaternion algebra of discriminant pq. We show that J and the new subvariety of $J_o(pq)$ differ in one significant respect. Namely, certain kernels which are 2-dimensional for the latter variety may be either 2- or 4-dimensional for the former. We give a simple criterion to decide whether the dimension is 2 or 4, and exhibit a procedure for constructing examples where the dimension is 4. We illustrate this procedure by constructing a 4-dimensional kernel with $pq = 11 \cdot 193$.

To Professor I.I. Piatetski-Shapiro

Introduction

Let p and q be distinct primes. Consider the modular curve $X_o(pq)$ over $\mathbf{Q}$. This curve is endowed with a Hecke correspondence T_ℓ for each prime number ℓ. (The operators T_p and T_q are often denoted U_p and U_q, respectively.) The correspondence T_ℓ induces an endomorphism of $J_o(pq) = \mathrm{Pic}^o(X_o(pq))$ which is again denoted T_ℓ. Let $\mathbf{T} = \mathbf{T}_{pq}$ be the (commutative) subring of $\mathrm{End}(J_o(pq))$ which is generated by the family of endomorphisms T_ℓ.

*Partially supported by the National Science Foundation

Suppose that m is a maximal ideal of $\mathbf{T}$, and let $k = \mathbf{T}/\mathsf{m}$ be its residue field. Let

$$\rho_{\mathsf{m}} : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathbf{GL}(2, k)$$

be the usual two-dimensional semisimple representation of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ attached to m ([3], Th. 6.7 or [12], §5). This representation is characterized, up to isomorphism, by the fact that it is unramified at each prime number r different from p, q, and the characteristic of k, together with the condition that the matrix $\rho_{\mathsf{m}}(\mathsf{Frob}_r)$ have trace T_r mod m and determinant r mod m, for each such r. (Here Frob_r is a Frobenius element for the prime r in $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$.)

Let $J_o(pq)[\mathsf{m}]$ be the kernel of m on $J_o(pq)(\overline{\mathbf{Q}})$, i.e., the intersection of the kernels of all elements of m on $J_o(pq)(\overline{\mathbf{Q}})$. The following result is a special case of Theorem 5.2(b) of [12].

THEOREM **1** *Assume that* m *is prime to* $2pq$ *and that the representation* ρ_{m} *is irreducible. Then* $J_o(pq)[\mathsf{m}]$ *is two-dimensional over* k*, and the* k*-linear action of* $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ *on* $J_o(pq)[\mathsf{m}]$ *defines a representation equivalent to* ρ_{m}*.*

Let J_{new} be the *new subvariety* of $J_o(pq)$. This abelian variety may be defined as the connected component of the kernel of the natural "trace" map

$$J_o(pq) \longrightarrow J_o(p) \times J_o(p) \times J_o(q) \times J_o(q)$$

([7], §2(b)) or, alternatively, as the dual of the new *quotient* of $J_o(pq)$ as in [16]. The variety J_{new} is a $\mathbf{T}$-stable subvariety of $J_o(pq)$; the image $\overline{\mathbf{T}}$ of $\mathbf{T}$ in $\mathrm{End}(J_{\mathrm{new}})$ is the *new quotient* of $\mathbf{T}$. We say that m is *new* if it arises from a maximal ideal of $\overline{\mathbf{T}}$ by pullback, relative to the quotient map $\mathbf{T} \to \overline{\mathbf{T}}$. Equivalently, m is new if and only if the kernel $J_{\mathrm{new}}[\mathsf{m}]$ of m on J_{new} is non-zero. Using the irreducibility of $J_o(pq)[\mathsf{m}]$, we deduce

THEOREM **2** *Suppose that* m *satisfies the hypothesis to Theorem 1, and that* m *is new. Then the representation* $J_{\mathrm{new}}[\mathsf{m}]$ *is equivalent to* ρ_{m}*.*

Now let $\mathcal{O}$ be a maximal order in a rational quaternion algebra of discriminant pq. (Up to isomorphism, there is only one such order.) Let C be the Shimura curve associated with the moduli problem of classifying abelian surfaces with an action of $\mathcal{O}$. Let $J = \mathrm{Pic}^o(C)$ be the Jacobian of C. As recalled in [12], §4, the curve C carries a family of Hecke correspondences T_ℓ, which again lead to commuting endomorphisms $T_\ell \in \mathrm{End}(J)$. The ring $\overline{\mathbf{T}}$ acts faithfully on J in such a way that each Hecke operator $T_\ell \in \overline{\mathbf{T}}$ acts on J as the corresponding endomorphism T_ℓ ([12], Cor. 4.2). Using this action, we define the kernel $J[\mathsf{m}]$ of m on $J(\overline{\mathbf{Q}})$ for each new maximal ideal m of $\mathbf{T}$. The group $J[\mathsf{m}]$ is non-zero because the action of $\overline{\mathbf{T}}$ on J is faithful.

View $J[\mathsf{m}]$ as a $k[\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})]$-module. If ρ_{m} is irreducible, a standard argument of Mazur ([6], II, Prop. 14.2) shows that the semisimplification of $J[\mathsf{m}]$ is a direct sum of copies of the simple $k[\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})]$-module corresponding to ρ_{m}. Call ν the number of summands. The k-dimension of $J[\mathsf{m}]$ is then 2ν. Our aim is to calculate the integer ν, which we call the *multiplicity* of ρ_{m} in $J[\mathsf{m}]$.

We achieve this goal whenever m satisfies the hypotheses to Theorem 2, i.e., whenever m is new and prime to $2pq$ and the representation ρ_{m} is irreducible. To explain our result, we remark that the representation ρ must be ramified at at least one of the primes p, q. Indeed, were ρ_{m} unramified (or "finite") at both p and q, the main theorem of [12] would show that ρ_{m} is modular of level 1. In particular, ρ_{m} would be realized as a module of division points on the abelian variety $J_o(1)$, which is zero. This, clearly, would be a contradiction. Permuting p and q if necessary, we therefore may assume that ρ_{m} is ramified at p. Let us do so. Also, we fix a Frobenius element Frob_q for q in $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$.

The following Theorem will be proved in §2:

Theorem **3** *Assume that* m *satisfies the hypotheses of Theorem 2. Then the multiplicity of* ρ_{m} *in* $J[\mathsf{m}]$ *is 1 unless* ρ_{m} *is unramified at* q *and the Frobenius element* Frob_q *acts in* ρ_{m} *as* ± 1. *In this latter case, the multiplicity is 2.*

By the main theorem of [12], the hypothesis that ρ_{m} is unramified at q implies that ρ_{m} is modular of level p in the sense that it arises from a maximal ideal of the Hecke algebra $\mathbf{T}_p$ associated to $J_o(p)$. The maximal ideal m is then *old* as well as new: it is an "ideal of fusion" between old and new at level pq.

Conversely, we can make examples of m for which ρ_{m} occurs with multiplicity 2 via the following construction, in which p is considered as fixed, but q is allowed to vary. Start with a representation ρ of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ which is modular of level p. To fix ideas, assume that ρ is irreducible and that it is a representation over a finite field of characteristic prime to $2p$. Using the Cebotarev density theorem, find a prime q for which Frob_q acts in ρ as ± 1. Then there is a new maximal ideal $\mathsf{m} \subset \mathbf{T}_{pq}$ for which ρ_{m} and ρ are isomorphic. Indeed, the trace and determinant of Frob_q are respectively ± 2 and 1. Since the determinant of Frob_q is q, we have $q \equiv 1 \bmod \mathsf{m}$. Therefore, the key congruence

$$\operatorname{tr} \rho(\mathsf{Frob}_q) \equiv \pm(q+1) \pmod{\mathsf{m}}$$

is satisfied. According to Theorem 1 of [15], ρ arises from a maximal ideal m of $\mathbf{T}_{pq}$ which is "q-new." Such a maximal ideal is genuinely new (and not just q-new) unless the corresponding representation ρ_{m} of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ is finite at p. In our situation, $\rho_{\mathsf{m}} \approx \rho$ cannot be finite at p, since it would otherwise be modular of level 1 as in the discussion above.

For a concrete example, take $p = 11$, and let

$$\rho : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathbf{GL}(2, \mathbf{F}_3)$$

be the representation of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ given by the group of 3-division points on the elliptic curve $J_o(11)$. The image of ρ is all of $\mathbf{GL}(2, \mathbf{F}_3)$ (see [18]). The Galois extension K of $\mathbf{Q}$ which is cut out by ρ contains the field $\mathbf{Q}(\Delta^{1/3}, \mu_3)$, where $\Delta = -11^5$ is the discriminant of $J_o(11)$ ([17], p. 305). We seek a criterion to determine whether a not a prime number $q \neq 3, 11$ satisfies the condition $\rho(\mathsf{Frob}_q) = \pm 1$. This condition implies that $\det(\rho(\mathsf{Frob}_q)) = 1$, which means the congruence $q \equiv 1 \pmod 3$ is satisfied. Similarly, the trace of $\rho(\mathsf{Frob}_q)$ must be $\pm 2 \pmod 3$, which translates to the condition that the coefficient c_q of q in the expansion of $X \cdot \prod_{n \geq 1}(1 - X^n)^2(1 - X^{11n})^2$ must be non-zero mod 3. (See [18], where the c_q are tabulated for $q \leq 2000$.)

Assume that these necessary conditions are satisfied. Then $\rho(\mathsf{Frob}_q)$ is either ± 1, as desired, or else is of the form $\pm \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$ with $x \neq 0$ in $\mathbf{F}_3$. Consider the image of $\rho(\mathsf{Frob}_q)$ in the Galois group $\mathrm{Gal}(\mathbf{Q}(\Delta^{1/3}, \mu_3)/\mathbf{Q})$, which is isomorphic to the symmetric group $\mathbf{S}_3$. This image is trivial or of order 3 according as $\rho(\mathsf{Frob}_q) = \pm 1$ or $\rho(\mathsf{Frob}_q) = \pm \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$ (with $x \neq 0$). Concretely, this means that $\rho(\mathsf{Frob}_q) = \pm 1$ if 11 is a cube mod q. Calculation shows that the prime $q = 193$ satisfies this condition, as well as the necessary congruences $q \equiv 1$ and $c_q \equiv \pm 2 \pmod 3$. (We have $c_{193} = 4$.) Therefore, there is a new maximal ideal m in $\mathbf{T}_{11\cdot 193}$, of residue characteristic 3, such that the multiplicity of ρ_{m} in $J[\mathsf{m}]$ is 2.

Our motivation in proving Theorem 3 is to "contrast and compare" the two abelian varieties J_{new} and J. According to a theorem of [10] (now easier to prove using [4], Satz 4), J_{new} and J are isogenous over $\mathbf{Q}$. There has been some speculation that a natural $\mathbf{T}$-equivariant isogeny (in one direction or the other) should link these two abelian varieties. Theorems 2 and 3 seem to show that the support of the kernel of such an isogeny must, in general, contain maximal ideals m for which ρ_{m} is irreducible. This suggests that any construction of such an isogeny must be relatively elaborate.

Our proof of Theorem 3 is based on a number of the ideas of [12]. In particular, it relies on the exact sequence (see [12], Th. 4.1) relating the mod p bad reduction of J with the mod q bad reductions of $J_o(q)$ and $J_o(pq)$.

The author wishes to thank Nigel Boston, Ling San, and Jean-François Mestre for helpful conversations and correspondence during the preparation of this paper.

1 Multiplicity one for character groups

In this §, q is a prime number and M is a positive integer prime to q. Set $N = qM$. Let $\mathcal{J}$ be the Néron model of $J_o(N)_{/\mathbf{Q}_q}$, and write $J_o(N)_{/\mathbf{F}_q}$ for the special fiber of $\mathcal{J}$. As is well known, the connected component of 0 in $J_o(N)_{/\mathbf{F}_q}$, call it $J_o(N)^o_{/\mathbf{F}_q}$, sits in an exact sequence

$$0 \to T \to J_o(N)^o_{/\mathbf{F}_q} \xrightarrow{\pi} J_o(M)_{/\mathbf{F}_q} \times J_o(M)_{/\mathbf{F}_q} \to 0, \tag{1}$$

where T is a torus over $\mathbf{F}_q$. (This follows from results of Raynaud [8] and Deligne-Rapoport [2], as explained in the appendix to [6].) The character group

$$L = \mathrm{Hom}_{\overline{\mathbf{F}}_q}(T, \mathbf{G_m})$$

of T may be described explicitly as the group of degree-0 divisors on the supersingular points on $X_o(M)_{/\overline{\mathbf{F}}_q}$ ([6], Appendix).

Recall [7] that the two degeneracy maps $\delta_1, \delta_q : X_o(N) \rightrightarrows X_o(M)$ induce by functoriality a pair of maps $J_o(M) \rightrightarrows J_o(N)$. By composing their direct product with the sum map $J_o(N)^2 \to J_o(N)$, we obtain the standard degeneracy map $\alpha : J_o(M)^2 \to J_o(N)$, cf. [7, 11, 15, 16]. Passing to characteristic q, we find a map

$$\alpha_{/\mathbf{F}_q} : J_o(M)^2_{/\mathbf{F}_q} \to J_o(N)^o_{/\mathbf{F}_q}.$$

The composition of π with $\alpha_{/\mathbf{F}_q}$ is then an endomorphism of $J_o(M)^2_{/\mathbf{F}_q}$, which we may represent as a 2×2 matrix of endomorphisms of $J_o(M)_{/\mathbf{F}_q}$.

LEMMA **1** *The matrix $\pi \circ \alpha_{/\mathbf{F}_q}$ is the matrix $\begin{pmatrix} \mathrm{id} & \mathrm{Ver} \\ \mathrm{Ver} & \mathrm{id} \end{pmatrix}$, where* id *is the identity endomorphism of $J_o(M)$ and* Ver *is the Verschiebung endomorphism of $J_o(M)$, i.e., the transpose of the Frobenius endomorphism of $J_o(M)$.*

Proof. The map $\alpha_{/\mathbf{F}_q}$ is obtained by functoriality from two degeneracy maps $X_o(N) \rightrightarrows X_o(M)$, whereas the map π is deduced by functoriality from two maps in the other direction, which are peculiar to characteristic q ([2], V, §1). The four possible compositions are determined in [2], *loc. cit.* Two of them are the identity map of $X_o(M)_{/\mathbf{F}_q}$, while the other two are the Frobenius of $X_o(M)_{/\mathbf{F}_q}$. Passing to Jacobians (via the functor Pic^o), we obtain the indicated formula. ■

Let $\mathbf{T} = \mathbf{T}_N$ be the subring of $\mathrm{End}(J_o(N))$ generated by the Hecke operators T_ℓ for prime numbers ℓ. The ring $\mathbf{T}$ acts by functoriality on T and on L. These actions factor through faithful actions of the "q-new quotient" of $\mathbf{T}$, which is denoted $\mathbf{T}_1$ in [12], §3. (See [12], Theorem 3.10.) We say that a maximal ideal m of $\mathbf{T}$ is q-new if it arises by pullback from this quotient.

Similarly, the q-old quotient $\mathbf{T}_o$ of $\mathbf{T}$ may be defined in any of several equivalent ways. In ([12], §3), $\mathbf{T}_o$ is defined as the image of $\mathbf{T}$ in $\mathrm{End}(S_o)$, where S_o is the direct sum of two copies of the space of weight-2 cusp forms on $\Gamma_o(M)$. (This direct sum is naturally a $\mathbf{T}$-module because $\mathbf{T}$ preserves the direct sum after it has been identified with a subspace of the space of weight-2 cusp forms on $\Gamma_o(N)$, as in the work of Atkin-Lehner [1].) An equivalent geometric definition is the following one. There is a unique operation of $\mathbf{T}$ which is compatible with α and the operation of $\mathbf{T}$ on $J_o(N)$. The ring $\mathbf{T}$ acts on $J_o(M)^2$ through its quotient $\mathbf{T}_o$, which acts faithfully. Finally, consider the functorial action of $\mathbf{T}$ on $J_o(N)^o_{/\mathbf{F}_q}$. Then, in the exact sequence (1), there is a unique operation of $\mathbf{T}$ on $J_o(M)^2$ which is compatible with π and the action of $\mathbf{T}$ on $J_o(N)^o_{/\mathbf{F}_q}$. In this latter operation, $\mathbf{T}$ again acts through $\mathbf{T}_o$, which acts faithfully ([12], Th. 3.11). In analogy with the terminology introduced for $\mathbf{T}_1$, we say that a maximal ideal m of $\mathbf{T}$ is q-old if it arises by pullback from $\mathbf{T}_o$.

THEOREM 4 *Let* m *be a maximal ideal of* $\mathbf{T}$ *which is prime to* $2N$ *and such that the corresponding representation* ρ_{m} *of* $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ *is irreducible. Assume that* ρ_{m} *is unramified at* q*. Then* m *is* q*-old.*

Proof. To prove this theorem, we review the proof given for Theorem 8.2 of [12]. First of all, m is either q-old or q-new (but might be both), so we may assume that m is q-new. We do so. Pick an "auxiliary" prime number Q: this is a prime number which is prime to $2N$ and the characteristic of $\mathbf{T}/\mathsf{m}$, and which is such that a Frobenius element for Q in $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ maps under ρ_{m} to the image of a complex conjugation in $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. Following the proof of Theorem 8.2 of [12], we introduce the Hecke algebra $\mathbf{T}_{QN}$ associated with the space of weight-2 cusp forms on $\Gamma_o(NQ)$. We then pick a maximal ideal $\mathcal{M}$ of $\mathbf{T}_{NQ}$ which is *compatible* with m. To explain this notion, we view $\mathbf{T}_N$ and the Q-old quotient of $\mathbf{T}_{NQ}$ as subrings of the commutative ring $\mathcal{R}$ which they generate together in the ring of endomorphisms of the direct sum of two copies of the space of weight-2 cusp forms on $\Gamma_o(N)$. (In this ring, the operators T_ℓ coming from $\mathbf{T}_N$ and from $\mathbf{T}_{NQ}$ are equal for all primes ℓ, except for the case $\ell = Q$. The ring $\mathcal{R}$ is generated by the shared Hecke operators T_ℓ (with $\ell \neq Q$), together with the Hecke operator T_Q coming from $\mathbf{T}_N$ and the Q^{th} Hecke operator U_Q coming from $\mathbf{T}_{NQ}$.) The compatibility means that m and the projection of $\mathcal{M}$ in the Q-old quotient of $\mathbf{T}_{NQ}$ are contained in a common maximal ideal.

Looking carefully at the proof of Theorem 8.2 of [12], one sees that the following property of $\mathcal{M}$ is proved: the ideal $\mathcal{M}$ is "qQ-old" in the sense that it arises from the "Qq-old quotient" of $\mathbf{T}_{NQ}$, defined (for example) as a subring of $\mathrm{End}(J_o(M)^4)$. For the convenience of the reader, §3 provides more details concerning this point.

The indicated property of $\mathcal{M}$ becomes much simpler if we jettison (temporarily) the two different Hecke operators T_Q. Namely, consider the subring R of $\mathbf{T}$ which is generated by all the T_ℓ with the *exception* of T_Q. Let m_R be the intersection of m with R. What is proved about $\mathcal{M}$ gives, in particular, that m_R is q-old in the sense that it arises by pullback from the subring R_o

of $\mathbf{T}_o$ which is generated by the T_ℓ with $\ell \neq Q$. By the going-up theorem of Cohen-Seidenberg, this shows that there is some maximal ideal m' of $\mathbf{T}$ which is q-old and which contains m_R. To prove the theorem, it is enough to verify that m and m' coincide.

Let $\mathbf{F}$ be the residue field of m_R, so that $\mathbf{F}$ is a subfield of each of $\mathbf{T}/\mathsf{m}$ and $\mathbf{T}/\mathsf{m}'$. By the Chinese Remainder Theorem, to prove that $\mathsf{m} = \mathsf{m}'$ is to prove that the image of $\mathbf{T}$ in $\mathbf{T}/\mathsf{m} \times \mathbf{T}/\mathsf{m}'$ is a field. The image of R in $\mathbf{T}/\mathsf{m} \times \mathbf{T}/\mathsf{m}'$ is $\mathbf{F}$, embedded "diagonally" in the product. It thus suffices to show that the image of T_Q in the product lies inside the image of $\mathbf{F}$ in the product. However, by applying the Cebotarev Density Theorem to $\rho_{\mathsf{m}} \times \rho_{\mathsf{m}'}$, we see that there are infinitely many primes ℓ, $\ell \neq Q$, so that T_ℓ and T_Q have the same image in $\mathbf{T}/\mathsf{m} \times \mathbf{T}/\mathsf{m}'$. ■

In the following discussion, we assume that m is a maximal ideal of $\mathbf{T}$ which is prime to $2N$ and such that the representation ρ_{m} of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ is irreducible. According to [12], Theorem 5.2(b), the kernel $J_o(N)[\mathsf{m}]$ of m on $J_o(N)$ is multiplicity free in the sense that $J_o(N)[\mathsf{m}]$ is two-dimensional (and therefore isomorphic to ρ_{m} as a representation of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$). We shall calculate the dimension of $L/\mathsf{m}L$. By the characterization of $\mathbf{T}_1$ which was cited, $L/\mathsf{m}L$ is non-zero if and only if m is q-new. We say that $L/\mathsf{m}L$ is *multiplicity free* if it is of dimension ≤ 1 over the residue field $k = \mathbf{T}/\mathsf{m}$. With this definition, $L/\mathsf{m}L$ is automatically multiplicity free if m is not q-new.

Proposition 1 *Assume that m is q-new, prime to $2N$, and such that ρ_{m} is irreducible. Then $L/\mathsf{m}L$ is multiplicity free unless ρ_{m} is unramified at q and a Frobenius element Frob_q for q in $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ acts in ρ_{m} as ± 1. In this latter case, $L/\mathsf{m}L$ is of dimension 2 over k.*

Proof. Let D be the Galois group $\mathrm{Gal}(\overline{\mathbf{Q}}_q/\mathbf{Q}_q)$, thought of as a decomposition group for q in $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. We consider that Frob_q is a Frobenius element of D. Let ℓ be the characteristic of k. As discussed in §6 of [12], the work of Grothendieck in SGA7I [5] establishes a natural inclusion of $k[D]$-modules

$$\mathrm{Hom}(L/\mathsf{m}L, \mu_\ell) \hookrightarrow J_o(N)[\mathsf{m}]. \tag{2}$$

The left-hand module is unramified, with Frob_q acting as qT_q ([12], Proposition 3.8). Further, the Hecke operator T_q is the negative of the Atkin-Lehner involution w_q on the torus T ([12], Proposition 3.7). Therefore, Frob_q acts on $\mathrm{Hom}(L/\mathsf{m}L, \mu_\ell)$ as $+q$ or as $-q$.

In our situation, the dimension of $\mathrm{Hom}(L/\mathsf{m}L, \mu_\ell)$ is at least 1, while the dimension of $J_o(N)[\mathsf{m}]$ is exactly 2, as remarked above. Hence, if $L/\mathsf{m}L$ is not multiplicity free, it has dimension 2, and $\mathrm{Hom}(L/\mathsf{m}L, \mu_\ell)$ coincides with $J_o(N)[\mathsf{m}]$. Since the latter module is a model for the representation ρ_m, this latter representation is unramified. (Here, we could say "unramified at q," but this qualification is somewhat superfluous since the coincidence of $\mathrm{Hom}(L/\mathsf{m}L, \mu_\ell)$ and $J_o(N)[\mathsf{m}]$ gives merely an equality of $k[D]$-modules.) It follows also that Frob_q acts in ρ_m as one of the two scalars $\pm q$. To see that $q \equiv 1 \pmod{\mathsf{m}}$, we note that the determinant of Frob_q in ρ_m is q, while the determinant of either scalar $\pm q$ is q^2. Therefore, if $L/\mathsf{m}L$ is not multiplicity free, then Frob_q acts as ± 1, as claimed.

Suppose, conversely, that ρ_m is unramified at q and that Frob_q acts in ρ_m as $+1$ or -1. By considering the determinant, we see again that $q \equiv 1 \pmod{\mathsf{m}}$. Also, m is q-old, by Theorem 4. This implies that the kernel $(J_o(M) \times J_o(M))[\mathsf{m}]$ of m on $J_o(M)^2$ is non-zero. On the other hand, the kernel of $\alpha : J_o(M)^2 \to J_o(N)$ has trivial intersection with $J_o(M)^2[\mathsf{m}]$, since the kernel of α is "Eisenstein," whereas ρ_m is irreducible. (See Theorem 1 of [13], Theorem 4.3 of [11], and Theorem 5.2(c) of [12].) By the irreducibility of $V = J_o(N)[\mathsf{m}]$, α identifies $J_o(M)^2[\mathsf{m}]$ with $J_o(N)[\mathsf{m}]$.

Since m is q-new, T_q mod m is ± 1 and the Atkin-Lehner involution w_q acts on $J_o(N)[\mathsf{m}]$ as ∓ 1 (with the opposite sign). By comparing the actions of Frob_q on $J_o(N)[\mathsf{m}]$ and its submodule $\mathrm{Hom}(L/\mathsf{m}L, \mu_\ell)$, we see that the sign "$\pm$" for the action of Frob_q on $J_o(N)[\mathsf{m}]$ is $+$ if $T_q \pmod{\mathsf{m}}$ is $+1$, and is $-$ if $T_q \pmod{\mathsf{m}}$ is -1. Finally, the degeneracy map α is equivariant with respect to the Atkin-Lehner involution w_q on $J_o(N)$ and the involution $(x, y) \mapsto (y, x)$ on $J_o(M)^2$. Putting all this together, we find that $J_o(M)^2[\mathsf{m}]$ lies inside the diagonal image of $J_o(M)$ in $J_o(M)^2$ if Frob_q acts on $J_o(N)[\mathsf{m}]$ as -1, and in the antidiagonal image of $J_o(M)$ in $J_o(M)^2$ if Frob_q acts on $J_o(N)[\mathsf{m}]$ as $+1$. (By the "antidiagonal image," we mean the graph of multiplication by -1.)

To fix ideas, we will suppose from now on that Frob_q acts as -1 on $J_o(N)[\mathsf{m}]$, so that $J_o(N)[\mathsf{m}]$ lies in the image of $J_o(M)$ in $J_o(N)$ under the composition of α with the diagonal embedding of $J_o(M)$ in $J_o(M)^2$. One, extremely minor, advantage of this choice is that the composition is a map $J_o(M) \to J_o(N)$ which has *trivial* kernel. In the antidiagonal situation, the analogous composition has (in general) a non-trivial kernel. However, the kernel is finite; and, as remarked above, it is "Eisenstein." This implies, as already noted, that the kernel does not intersect the groups which interest us.

Pulling back $J_o(N)[\mathsf{m}]$ to $J_o(M)$, we find a subgroup W of $J_o(M)[\ell]$ such that

$$J_o(N)[\mathsf{m}] = \{\, \alpha(x,x) \,|\, x \in W \,\}.$$

The Frobenius element Frob_q of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ acts on W as -1. Viewing W as a group of points on $J_o(M)_{/\mathbf{F}_q}$, we see that the Frobenius *endomorphism* of $J_o(M)_{/\mathbf{F}_q}$ acts on W as -1. Since $q \equiv 1 \pmod{\ell}$, the Verschiebung endomorphism of $J_o(M)_{/\mathbf{F}_q}$ acts, as well, as -1 on W. By Lemma 1, all points (x,x) with $x \in W$ lie in the kernel of $\pi \circ \alpha$. Thus $J_o(N)[\mathsf{m}]$ (viewed as a group of points of $J_o(N)_{/\mathbf{F}_q}$) lies in the kernel of $\pi_{/\mathbf{F}_q}$, which is the torus T. Therefore, we have $J_o(N)[\mathsf{m}] \subset \mathrm{Hom}(L/\mathsf{m}L, \mu_\ell)$. It follows that $L/\mathsf{m}L$ has dimension greater than 1. ■

2 Shimura Curves

The principal aim of this section is to prove Theorem 3. We return to the notations introduced in the Introduction. Thus p and q are distinct primes, J is the Jacobian of the Shimura curve introduced earlier, $\mathbf{T} = \mathbf{T}_{pq}$ is the Hecke algebra at level pq, and m is a maximal ideal of $\mathbf{T}$. We assume that m is new and prime to $2pq$, and that the representation ρ_{m} is irreducible. We suppose that p and q have been ordered so that ρ_{m} is ramified at p. Our goal is to investigate the dimension of $J[\mathsf{m}]$ over $k = \mathbf{T}/\mathsf{m}$.

To achieve this goal, we will apply the discussion of §1 in the case where $M = p$, i.e., $N = pq$. We shall give $J_o(q)^2$ the unique $\mathbf{T}$-action which is compatible with the action of $\mathbf{T}$ on $J_o(pq)$ and the analogue $\beta : J_o(q)^2 \to J_o(pq)$ of the degeneracy map $\alpha : J_o(p)^2 \to J_o(pq)$. Then $\mathbf{T}$ acts on each of the abelian varieties J, $J_o(pq)$ and $J_o(q)^2$.

Use the notation $\mathcal{J}$, previously employed for the Néron model of $J_o(N)$, for the Néron model of J over $\mathbf{Q}_p$. Its special fiber $J_{/\mathbf{F}_p}$ is an extension of a finite group Ψ by its connected component $J^o_{/\mathbf{F}_p}$, which is a torus (cf. [12], §4). Write Y for the character group of this torus (computed over an algebraic closure $\overline{\mathbf{F}}_p$ of $\mathbf{F}_p$), so that the torus itself becomes $\mathrm{Hom}(Y, \mathbf{G_m})$. Let L be the character group which is introduced in that §, and let X be the analogue of L

for the abelian variety $J_o(q)^2$. Note that X and L are defined with reference to an algebraic closure of $\mathbf{F}_q$, while Y has just been defined with reference to an algebraic closure of $\mathbf{F}_p$. We suppose from now on that these algebraic closures have in fact been selected as algebraic closures of the residue fields $\mathbf{F}_{q^2}$ and $\mathbf{F}_{p^2}$ of the maximal order $\mathcal{O}$ which was used in the definition of J. The ring $\mathbf{T}$ acts by functoriality on L, Y and X.

THEOREM **5** *There is a natural* $\mathbf{T}$*-equivariant exact sequence*

$$0 \to Y \to L \xrightarrow{\beta^*} X \to 0. \tag{3}$$

This theorem is proved as Theorem 4.1 of [12], although the notations there are somewhat different. In [12], the group X is called "$X \oplus X$," the symbol X being reserved for the character group attached to $J_o(q)$. Further, Y is *defined* as the kernel of the map from L to X; the content of the theorem is that the character group attached to J may be identified with this kernel. Finally, the Hecke algebra appearing in [12], Th. 4.1 is of necessity the formal polynomial ring $\tilde{\mathbf{T}}$ on symbols representing Hecke operators, since it is only after proving this theorem that one knows that $\tilde{\mathbf{T}}$ operates on J through its quotient $\mathbf{T}$.

In [12], the map $Y \to L$ appears to depend on a certain number of choices. This is not very surprising in view of the fact that the very definition of Y depends on the choice of an algebraic closure of $\mathbf{F}_p$, while L is defined in terms of an algebraic closure of $\mathbf{F}_q$. On the other hand, all characters in Y and L are in fact defined over the quadratic subfields of $\overline{\mathbf{F}}_p$ and $\overline{\mathbf{F}}_q$, respectively. Thus, it is reasonable to hope that a canonical map $Y \to L$ can be defined with these quadratic subfields as initial data. The main content of [14] is to realize this hope. In particular, [14] shows that a canonical map $Y \to L$ can be given when $\mathbf{F}_{q^2}$ and $\mathbf{F}_{p^2}$ are chosen as the residue fields of $\mathcal{O}$. This is the choice that we have made.

PROPOSITION **2** *We have* $1 \leq \dim_k Y/\mathsf{m}Y \leq 2$. *The dimension is 2 if and only if* ρ_{m} *is unramified at* q *and* Frob_q *acts in* ρ_{m} *as* ± 1.

Proof. The localization X_{m} of X at m is 0. Indeed, suppose that X_{m} is non-zero. Then m is p-old in the sense that it arises by pullback from the p-old quotient of $\mathbf{T}$ (which can be defined as the image of $\mathbf{T}$ in the endomorphism ring of $J_o(q)^2$). This shows that ρ_{m} is modular of level q, which implies that ρ_{m} is unramified at p. However, according to our ordering of p and q, ρ_{m} is ramified at p.

The sequence (3) thus shows that L_{m} and Y_{m} are isomorphic. In particular, we have $L/\mathsf{m}L \approx Y/\mathsf{m}Y$. Our proposition thus follows from Proposition 1. ■

We next recall the interpretation of Ψ in terms of the monodromy pairing on Y [5]. As recalled in [12], §1, there is an interpretation of Ψ as the cokernel of an injection $\mu : Y' \to \mathrm{Hom}(Y, \mathbf{Z})$, where Y' is the analogue of the group Y for the abelian variety dual to J. Since $J = \mathrm{Pic}^o(C)$ is naturally isomorphic to the dual of J (i.e., to the Albanese variety of C), we have an isomorphism $Y \approx Y'$. This isomorphism is compatible with the functorial actions of $\mathbf{T}$ on Y and Y'. Indeed, to check this one must show that all Hecke operators T_r (with r prime) are fixed under the Rosati involution on $\mathrm{End}(J)$ coming from the usual principal polarization on the Jacobian J. This is a standard fact for the generators T_r of $\mathbf{T}$ with r prime different from p and q. For $r = p$ and $r = q$, we use the interpretation of T_r as $-w_r$, plus the fact that the involution w_r is its own transpose.

We thus have an exact sequence of $\mathbf{T}$-modules

$$0 \to Y \xrightarrow{\mu} \mathrm{Hom}(Y, \mathbf{Z}) \to \Psi \to 0. \tag{4}$$

To say that μ is $\mathbf{T}$-equivariant amounts to the statement that the bilinear pairing (,) associated with μ satisfies $(Ty_1, y_2) = (y_1, Ty_2)$ for $T \in \mathbf{T}$ and $y_1, y_2 \in Y$.

We recall that ℓ is the characteristic of $k = \mathbf{T}/\mathsf{m}$.

Proposition 3 *The k-dimensions of $Y/\mathsf{m}Y$ and $(Y/\ell Y)[\mathsf{m}]$ are equal.*

Proof. Consider the map "multiplication by ℓ" on the terms of the exact sequence (4). Using the Snake Lemma, we get a four-term sequence

$$0 \to \Psi[\ell] \to Y/\ell Y \to \mathrm{Hom}(Y/\ell Y, \mathbf{Z}/\ell\mathbf{Z}) \to \Psi/\ell\Psi \to 0. \tag{5}$$

Further, the localization of Ψ at m is 0. Indeed, the exact sequence of [12], Theorem 4.3 gives after localization a sequence

$$X_{\mathsf{m}} \to \Psi_{\mathsf{m}} \to E_{\mathsf{m}} \to 0, \tag{6}$$

where E is a quotient of the component group attached to the Néron model of $J_o(pq)$ at q. Since this component group is Eisenstein ([12], Th. 3.12), we have $E_{\mathsf{m}} = 0$. Also, $X_{\mathsf{m}} = 0$, as was already noted.

It follows that localization of (5) gives an isomorphism of the localizations at m of the two middle terms. Now take kernels of m (i.e., "$[\mathsf{m}]$") on both sides, and use the easily verified fact that these kernels may be identified with the kernels on the two middle terms *before* localization. This gives an isomorphism between $(Y/\ell Y)[\mathsf{m}]$ and $\mathrm{Hom}(Y/\mathsf{m}Y, \mathbf{Z}/\ell\mathbf{Z})$, which implies, in particular, the desired dimension equality. ■

Let ν again be the multiplicity of ρ_{m} in $J[\mathsf{m}]$, so that $\dim_k J[\mathsf{m}] = 2\nu$. In view of Proposition 2, the following result will complete the proof of Theorem 3.

PROPOSITION 4 *We have* $\nu = \dim_k Y/\mathsf{m}Y$*; i.e.,* $\dim_k J[\mathsf{m}] = 2\dim_k Y/\mathsf{m}Y$.

Proof. Because J is purely toric at p, there is an exact sequence of $\mathbf{T}$-modules

$$0 \to \mathrm{Hom}(Y/\ell Y, \mu_\ell) \to J(\overline{\mathbf{Q}}_p)[\ell] \to Y/\ell Y \to 0. \tag{7}$$

This sequence is noted in [9], (3.3.1), and can certainly be deduced easily from [5]. In particular, the inclusion of $\mathrm{Hom}(Y/\ell Y, \mu_\ell)$ in $J(\overline{\mathbf{Q}}_p)[\ell]$ is an analogue for J of the inclusion (2) for $J_o(N)$. The sequence (7) is compatible with the natural action of $\mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p)$ on all terms; in particular, the action of $\mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p)$ on $\mathrm{Hom}(Y/\ell Y, \mu_\ell)$ is unramified. Taking kernels of m yields

$$0 \to \mathrm{Hom}(Y/\mathsf{m}Y, \mu_\ell) \to J[\mathsf{m}] \to (Y/\ell Y)[\mathsf{m}]. \tag{8}$$

By Propositions 2 and 3, the dimensions of $\mathrm{Hom}(Y/\mathsf{m}Y, \mu_\ell)$ and $(Y/\ell Y)[\mathsf{m}]$ are equal, with the common value being 1 or 2. Clearly, if $\nu > 1$, then $\nu = 2$ and the common dimension is 2. Assume that $\nu = 1$, so that the dimension of $J[\mathsf{m}]$ is 2. If $Y/\mathsf{m}Y$ does *not* have dimension 1, then (8) shows that $\mathrm{Hom}(Y/\mathsf{m}Y, \mu_\ell)$ and $J[\mathsf{m}]$ are equal inside $\mathrm{Hom}(Y/\ell Y, \mu_\ell)$. In particular, this gives $J[\mathsf{m}] \subseteq \mathrm{Hom}(Y/\ell Y, \mu_\ell)$, which forces the action of $\mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p)$ to be unramified. Since p and q were ordered so that this action is *ramified*, we may conclude that $\dim Y/\mathsf{m}Y = 1$. ■

3 Appendix

The purpose of this Appendix is to justify the assertion about $\mathcal{M}$ which is made in the course of the proof of Theorem 4. The justification was postponed until now because it is relatively technical. Also, it uses material which is close in spirit to that of §2. For example, it makes use of a generalization of the exact sequence (3) to the case of the Jacobian of a Shimura curve made with level structure.

To be more precise, let M, q, and Q be the positive integers occurring during the course of the proof of Theorem 4. Then Q and q are distinct primes, and they are prime to M. Let $\mathcal{O}$ be a maximal order in a rational quaternion algebra of discriminant qQ, and let C now be the Shimura curve associated with the moduli problem of classifying abelian surfaces A which are furnished with an action of $\mathcal{O}$ and an $\mathcal{O}$-stable subgroup of A which is isomorphic to $(\mathbf{Z}/M\mathbf{Z})^2$ as an abelian group. The Hecke ring $\mathbf{T}_{MqQ}$ acts on $J = \mathrm{Pic}^o(C)$, and this action cuts out the "qQ-new quotient" of $\mathbf{T}_{MqQ}$ ([12], 4.2).

Now the maximal ideal $\mathcal{M}$ which was constructed in the proof of Theorem 4 is qQ-new by Theorem 7.3 of [12]. This implies that the kernel $J[\mathsf{m}]$ is non-zero. The residue field k of m coincides with the residue field of $\mathcal{M}$; therefore $J[\mathcal{M}]$ is naturally a $k[\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})]$-module. By the Eichler-Shimura relations for J, and the argument of Mazur which was repeatedly cited, the semisimplification of $J[\mathcal{M}]$ is a direct sum of copies of the representation V giving ρ_{m}. In particular, we may realize V as a submodule of $J[\mathcal{M}]$. Because V is by assumption unramified at q, we may identify V with a group of division points on the fiber $J_{/\mathbf{F}_q}$ at q for the Néron model for J.

This fiber is an extension of a component group Ψ by a torus $\mathrm{Hom}(Y, \mathbf{G_m})$. Let L be the character group of the toric part of $J_o(MqQ)_{/\mathbf{F}_Q}$, and let X be the character group of the toric part of $J_o(MQ)^2_{/\mathbf{F}_Q}$. Then the exact sequence (3) again may be constructed with these new definitions of Y, X, and L. Further, the group Ψ fits into an exact sequence which gives after localization at $\mathcal{M}$ the following analogue of (6):

$$X_{\mathcal{M}} \to \Psi_{\mathcal{M}} \to E_{\mathcal{M}} \to 0.$$

As in the proof of Proposition 3, the group $E_{\mathcal{M}}$ vanishes.

These considerations imply that $X_{\mathcal{M}}$ is non-zero. Indeed, suppose that $X_{\mathcal{M}}$ is 0. Then $\Psi[\mathcal{M}] = 0$, so that the kernel of $\mathcal{M}$ on the fiber $J_{/\mathbf{F}_q}$ coincides with $\mathrm{Hom}(Y/\mathcal{M}Y, \mathbf{G_m})$. This kernel is of k-dimension at least 2 because it contains the group V. Hence $\dim Y/\mathcal{M}Y \geq 2$. From (3) and the vanishing of $X_{\mathcal{M}}$, we then get $\dim L/\mathcal{M}L \geq 2$. As in the proof of Proposition 1, this inequality implies that Frob_Q acts in ρ_{m} as a scalar ± 1. However, we chose Q so that Frob_Q acts in ρ_{m} as a complex conjugation; in particular, it does not act as a scalar.

Knowing that $X_{\mathcal{M}}$ is non-zero gives us the information that $\mathcal{M}$ arises by pullback from the image of $\mathbf{T}_{MqQ}$ in $\mathrm{End}(J_o(MQ)^2)$. (We term this image the "q-old quotient" of $\mathbf{T}_{MqQ}$.) In particular, we may realize the $\mathbf{T}_{MqQ}[\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})]$-module V as a group of division points of $J_o(MQ)^2$. Since this group is unramified at Q, we may identify it with a group of division points on $J_o(MQ)^2_{/\mathbf{F}_Q}$. The group of division points in fact lives in the connected component of 0 in $J_o(MQ)^2_{/\mathbf{F}_Q}$, since the component group of $J_o(MQ)^2_{/\mathbf{F}_Q}$ is Eisenstein ([12], Theorem 3.12). It clearly cannot lie in the toric part $\mathrm{Hom}(X, \mathbf{G_m})$ of $J_o(MQ)^2_{/\mathbf{F}_Q}$, since Frob_Q does not act on V as a scalar. Hence it maps non-trivially to the abelian variety quotient $J_o(M)^4_{/\mathbf{F}_Q}$ of $J_o(MQ)^2_{/\mathbf{F}_Q}$. Therefore $\mathcal{M}$ arises by pullback from the quotient of $\mathbf{T}_{MqQ}$ which is cut out by $J_o(M)^4_{/\mathbf{F}_Q}$. As in [12], Theorem 3.11, this quotient is the same quotient which acts faithfully on $J_o(M)^4$, considered in the usual way as an abelian subvariety of $J_o(MqQ)$; in other words, it is the "qQ-old quotient" of $\mathbf{T}_{MqQ}$.

References

[1] Atkin, A.O.L. and Lehner, J.: Hecke operators on $\Gamma_o(m)$. Math. Ann. **185**, 134–160 (1970)

[2] Deligne, P., Rapoport, M.: Schémas de modules de courbes elliptiques. Lecture Notes in Math. **349**, 143–316 (1973)

[3] Deligne, P., Serre, J-P.: Formes modulaires de poids 1. Ann. Sci. École Norm. Sup. **7**, 507–530 (1974)

[4] Faltings, G.: Endlichkeitssätze für abelsche Varietäten über Zahlkörpern. Invent. Math **73**, 349–366 (1983). English translation in: Arithmetic Geometry, G. Cornell and J. H. Silverman, eds. New York: Springer-Verlag (1986)

[5] (SGA 7 I) Grothendieck, A.: Groupes de monodromie en géométrie algébrique. Lecture Notes in Mathematics **288**. Berlin-Heidelberg-New York: Springer 1972

[6] Mazur, B.: Modular curves and the Eisenstein ideal. Publ. Math. IHES **47**, 33–186 (1977)

[7] Mazur, B.: Rational isogenies of prime degree. Invent. Math. **44**, 129–162 (1978)

[8] Raynaud, M.: Spécialisation du foncteur de Picard. Publ. Math. IHES **38**, 27–76 (1970)

[9] Ribet, K.: Galois action on division points of abelian varieties with real multiplications. Am. J. Math. **98**, 751–804 (1976)

[10] Ribet, K.: Sur les variétés abéliennes à multiplications réelles. C.R. Acad. Sc. Paris *Série A* **291**, 121–123 (1980)

[11] Ribet, K.: Congruence relations between modular forms. Proc. International Congress of Mathematicians 1983, 503–514

[12] Ribet, K.: On modular representations of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ arising from modular forms. Invent. Math. To appear

[13] Ribet, K.: On the Component Groups and the Shimura Subgroup of $J_o(N)$. Sém. de Th. des Nombres de Bordeaux, Année 1987–88, Exposé 6

[14] Ribet, K.: Bimodules and abelian surfaces. Advanced Studies in Pure Mathematics **17**, 359–407 (1989)

[15] Ribet, K.: Raising the levels of modular representations. Progress in Mathematics. To appear.

[16] Ribet, K.: The old subvariety of $J_o(pq)$. To appear

[17] Serre, J-P.: Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. Invent. Math **15**, 259–331 (1972).

[18] Shimura, G.: A reciprocity law in non-solvable extensions. J. für die reine und angewandte Math. **221**, 209–220 (1966)