Invent. math. 100, 431–476 (1990)

Inventiones mathematicae

On modular representations of $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ arising from modular forms

K.A. Ribet
Department of Mathematics, University of California, Berkeley, CA 94720, USA

1. Introduction

The Main Theorem

Consider a continuous irreducible representation

$$\rho\colon G \to \mathbf{GL}(2, \mathbf{F}),$$

where G is the Galois group $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ and $\mathbf{F}$ is a finite field of characteristic $l \geqq 3$. Suppose that ρ is modular of level N, i.e., that it arises from a weight-2 newform of level dividing N and trivial "Nebentypus character." Then ρ is an odd representation: the matrix $\rho(c)$ (where c is a complex conjugation in G) has eigenvalues $+1$, -1. Since $+1$ and -1 are distinct in $\mathbf{F}$, ρ is absolutely irreducible and has a model over every subfield of $\mathbf{F}$ containing the set trace(ρ). We assume that $\mathbf{F}$ has been chosen so that it is generated by this set.

Assume that ρ is a prime which exactly divides N (we write $p \| N$), and restrict ρ to a decomposition group of G for the prime p. View the restriction as a representation ρ_p of $\mathrm{Gal}(\bar{\mathbf{Q}}_p/\mathbf{Q}_p)$. We say that ρ is *finite* at p ([34] or [35], §2.8) if there is a finite flat $\mathbf{F}$-vector space scheme H over $\mathbf{Z}_p$ for which the action of $\mathrm{Gal}(\bar{\mathbf{Q}}_p/\mathbf{Q}_p)$ on the $\mathbf{F}$-vector space $H(\bar{\mathbf{Q}}_p)$ gives ρ_p. (If $l \neq p$, ρ is finite at p if and only if ρ_p is unramified.)

It is clear that ρ is finite at p whenever ρ is already modular of level N/p. In §1 of [34] (cf. [35]), Serre conjectured the converse, i.e., that if ρ is finite, then ρ is modular of level N/p. Soon thereafter, Mazur [20] proved this conjecture in the case

$$p \not\equiv 1 \pmod{l}$$

(Theorem 6.1 below). Here, combining Mazur's techniques with a geometric relation between classical modular curves and Shimura curves (Theorem 4.1), we prove Serre's conjecture whenever N is not divisible by l. (Our arguments now apply to the case where l divides N but l^2 does not divide N because of the main theorem of [21]. See Theorem 5.3 below for a statement of this result.) Our new

result and Mazur's earlier result may be stated together as follows (see Theorem 8.2):

Theorem 1.1 (Main Theorem). *Assume that ρ is finite at p (with $p \| N$). Then ρ, a priori modular of level N, is modular of level N/p whenever one or both of the following conditions hold:*

1. $p \not\equiv 1 \pmod{l}$
2. *N is prime to l.*

The following application of the Main Theorem is based on an idea of G. Frey [10].

Corollary 1.2. *Assume that all elliptic curves over $\mathbf{Q}$ are modular. Then Fermat's Last Theorem is true.*

Proof (modeled on [35], §4). Assume that (a, b, c) is a triple of non-zero relatively prime integers which satisfies the Fermat equation

$$a^l + b^l + c^l = 0$$

with $l \geqq 5$. Permuting (a, b, c), we may suppose that b is even and that we have $a \equiv 3 \pmod{4}$. Following Frey [10], define E to be the elliptic curve over $\mathbf{Q}$ with Weierstrass equation

$$y^2 = x(x - a^l)(x + b^l) .$$

One sees easily that E is semistable and has bad reduction precisely at those primes p which divide the product abc ([35], §4.1). Let N be the conductor of E, i.e., the product of these primes. (Note that N is divisible by 2.) Because of our assumption about elliptic curves over $\mathbf{Q}$, there is a weight-2 modular form f on $\Gamma_0(N)$, with integral q-expansion coefficients, whose Mellin transform is the L-function of E over $\mathbf{Q}$. In particular, the mod l representation ρ of $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ attached to f is realized by the vector space

$$V = E[l]$$

of l-division points on E. (The action of $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ on V is irreducible because of [35], §4.1, Proposition 6.) This representation is finite at every prime $p \neq 2$ which divides N in view of [35], (4.1.9) and (4.1.12).

The Main Theorem now shows that ρ is modular of level 2. Indeed, suppose that N is divisible by l. Then ρ is finite at $p = l$, and since $l \not\equiv 1 \pmod{l}$, ρ is modular of level N/l. Taking $N_0 = N/l$ in this case, and $N_0 = N$ if N is not divisible by l, we find in all cases that ρ is modular of some level N_0 which divides N and which is prime to l. The Main Theorem applied inductively to ρ now eliminates all odd primes from its level. We are left with the final conclusion that ρ is modular of level 2, as claimed. Since it is known that there are no non-zero cusp forms of weight 2 on $\Gamma_0(2)$, we have a contradiction. □

Summary

The first sections of the paper contain preliminary material. In §2, we recall material due to Raynaud [24] concerning Néron models of Jacobians. This work has already been summarized by Grothendieck [11], Mazur-Rapoport ([18], Appendix), and other authors. In the next two §§, we recall the work of Deligne-Rapoport [4] and Cerednik-Drinfeld ([3], [7]) on the bad reduction of classical modular curves and Shimura curves, respectively. We then combine their results with the results of §2 to obtain information about the Néron models of the Jacobians of these curves.

Especially, we derive a geometric result (Theorem 4.1) which mirrors a special case of the well known correspondence, due to Eichler [9], Shimizu [36], and Jacquet-Langlands [12], between modular forms on $\mathbf{GL}(2)$ and modular forms on the multiplicative group of a quaternion algebra. More precisely, we take two distinct prime numbers p and q, together with a positive integer M prime to pq, and deduce a Shimura curve C from an Eichler order of level M in the quaternion algebra over $\mathbf{Q}$ with discriminant pq. The curve C supports Hecke correspondences T_n which are analogues of the standard correspondences T_n on the classical modular curves. These correspondences induce endomorphisms T_n on a certain free abelian group Z: the character group of the connected component of the origin in the fiber over $\mathbf{F}_p$ of the Néron model of the Jacobian of C. Our Theorem 4.1 connects up the $\mathbf{Z}[\ldots T_n \ldots]$-module Z with an analogous module derived from $J_0(pqM)_{\mathbf{F}_q}$.

The switch between p and q in our result enriches the analogy between the Jacobian $J = \mathrm{Pic}^0(C)$ and the "pq-new quotient" of $J_0(pqM)$ obtained by dividing $J_0(pqM)$ by its subvariety isogenous to a product of copies of $J_0(qM)$ and $J_0(pM)$. In fact, J and this quotient are well known to be isogenous over $\mathbf{Q}$ (cf. [26]), and much study of J has been motivated by a desire to find a "natural" isogeny between the two. Such an isogeny would induce a map between Z and the analogue of Z for $J_0(pqM)_{\mathbf{F}_p}$, rather than for $J_0(pqM)_{\mathbf{F}_q}$. Our theorem gives us the luxury of permuting the two primes p and q in situations where the connection between J and $J_0(pqM)$ is strong enough to allow us to pass from one to the other.

The §5, purely technical, discusses some relations between maximal ideals of Hecke algebras and representations of Gal($\bar{\mathbf{Q}}/\mathbf{Q}$). The last sections contain arguments leading to the Main Theorem. We begin, in §6, with Mazur's result [20], which corresponds to the case of the Main Theorem in which the congruence $p \not\equiv 1 \pmod{l}$ does not hold. The proof of Mazur's result is independent of §4; i.e., Shimura curves play no role.

Since the congruence $p \not\equiv 1 \pmod{l}$ certainly does not hold if $p = l$, we are now able to assume that p and l are distinct. We do this beginning in §7. Furthermore, we suppose in §7 that ρ, which arises by definition from a newform of level dividing Mp (where $M = N/p$), in fact arises from such a newform whose level is divisible by p. (If ρ comes from a newform of level prime to p, then there is nothing to prove.) We then prove that there are infinitely many primes q, $q \equiv -1 \pmod{l}$, such that ρ comes from a newform whose level divides pqM and is divisible by pq. We show, in fact, that q satisfies this condition if q is prime to lN and the image

under ρ of a Frobenius element for q in G has eigenvalues $+1, -1$. The existence of infinitely many q of this type is then guaranteed by the Cebotarev Density Theorem, since the image in $\rho(G)$ of a complex conjugation in G has eigenvalues $+1, -1$. Although our result in this § is similar to that of [28], we prove our result using (4.1) and make no appeal to [28].

In §8, we prove, under the hypotheses of the Main Theorem, that ρ, now modular of level Mpq, is modular of level Mq. This is sufficient for our purposes, because Mazur's result of §6 then applies to show that ρ is modular of level M, as desired. Our argument involves the Jacobian J discussed above. It uses heavily the results of §4, as well as (6.4).

This article evolved from lectures given at the MSRI, first during a seminar on modular forms and Galois representations, and then during a workshop on the Galois group of **Q**. The audience's comments significantly clarified some of the arguments in my earliest notes. For example, Lemma 6.2 was introduced into the text as the result of discussions with J-M. Fontaine and W. Messing.

A preliminary version of this article was carefully studied by Guy Henniart and Joseph Oesterlé. Their detailed comments have been extremely useful.

The author wishes to thank Bruce Jordan and Ron Livné for many key discussions concerning Shimura curves and their Jacobians, and especially for their generosity in sharing the ideas of [14]. He owes special thanks to Barry Mazur for a series of generous suggestions, made over several years.

The research described in this article was supported by grants from the National Science Foundation and the Vaughn Foundation. It was performed, in part, at the Max Planck Institute in Bonn, the MSRI in Berkeley, and the IHES in Bures-sur-Yvette. The author thanks these institutions, and their directors, for their hospitality.

Contents

2. The Picard-Lefschetz formula

Let p be a prime. Consider a curve C over a p-adic field K of characteristic 0, with residue field k of characteristic p. Denote by P the Jacobian $\mathrm{Pic}^0(C)$ of C. We recall in a special case some relations between the special fiber of the Néron model of P and the special fibers of suitable models of C. These relations are based on work of [24]. They are discussed in [11], §12 and in the appendix to [18].

Suppose first that $\mathscr{C}$ is the regular minimal model of C over the integer ring of K. Suppose that the greatest common divisor of the multiplicities of the irreducible components of $\mathscr{C}_k$ is 1. Let P_k be the special fiber of the Néron model of P and let $P^0 = (P_k)^0$ be the connected component of 0 in this special fiber.

As explained in [11], §12, the results of [24] imply that there is a canonical isomorphism

$$P^0 \approx \mathrm{Pic}^0(\mathscr{C}_k) ,$$

cf. [11], (12.1.12). Assume, moreover, that all singular points of the curve $\mathscr{C}_k$ are ordinary double points (i.e., have local equation $xy = 0$). Then P^0 is a semiabelian scheme over k, i.e., an extension of an abelian variety A by a torus. More precisely, write the normalization of $\mathscr{C}_k$ as a disjoint union of non-singular curves D_j. The normalization map $\cup D_j \to \mathscr{C}_k$ induces a surjection

$$\mathrm{Pic}^0(\mathscr{C}_k) \to \prod_j \mathrm{Pic}^0(D_j) = A ,$$

whose kernel T is a torus which may be described explicitly in view of [EGA IV], 21.8.5.

The description, which is well known, is most compactly expressed in terms of the "dual graph" $\mathscr{G}$ attached to $\mathscr{C}_k$. This is the unoriented graph with the following definition:

- The set of vertices of $\mathscr{G}$ is the set $\mathscr{T}$ of irreducible components of $\mathscr{C}_k$.
- The set of edges of $\mathscr{G}$ is the set $\mathscr{I}$ of singular points of $\mathscr{C}_k$.
- The edge corresponding to a singular point $i \in \mathscr{I}$ connects the two vertices corresponding to the two components of $\mathscr{C}_k$ which meet at i.

Proposition 2.1 (cf. [11], (12.3.7)). *There is a canonical isomorphism*

$$T \approx H^1(\mathscr{G}, \mathbf{Z}) \otimes \mathbf{G}_m .$$

Equivalently, we have

$$X \approx H_1(\mathscr{G}, \mathbf{Z}) ,$$

where $X = X(T)$ is the character group of T.

To calculate $H_1(\mathscr{G}, \mathbf{Z})$, we first consider the bouquet $\bar{\mathscr{G}}$ of circles obtained by collapsing to a single point all vertices of $\mathscr{G}$. The map $\mathscr{G} \to \bar{\mathscr{G}}$ induces an inclusion

$$X = H_1(\mathscr{G}, \mathbf{Z}) \to H_1(\bar{\mathscr{G}}, \mathbf{Z}) .$$

For each $i \in \mathscr{I}$, choose an orientation of the corresponding edge of $\mathscr{G}$, i.e., an

ordering $\{j_1(i), j_2(i)\}$ of the two components which pass through i. The resulting orientation of the edges of $\bar{\mathscr{G}}$ determines an isomorphism

$$H_1(\bar{\mathscr{G}}, \mathbf{Z}) \approx \mathbf{Z}^{\mathscr{I}} .$$

from which we deduce a non-canonical inclusion

$$X \subset \mathbf{Z}^{\mathscr{I}} . \tag{1}$$

To identify X with a specific subgroup of $\mathbf{Z}^{\mathscr{I}}$, we let D be the group of degree-0 formal integral linear combinations of elements of $\mathscr{T}$, i.e., the kernel of the degree map

$$\mathbf{Z}^{\mathscr{T}} \to \mathbf{Z} .$$

Proposition 2.2. *The group X corresponds to the kernel of the homomorphism*

$$\alpha: \mathbf{Z}^{\mathscr{I}} \to D$$

defined by

$$\alpha(i) = j_1(i) - j_2(i) .$$

For the proof, see [11], §12.4.

Now let Φ be the group of connected components of P_k. Let Y be the analogue of X for the abelian variety dual to P, i.e., the character group arising from the reduction of the Albanese variety $\mathrm{Alb}(C)$. One may express Φ in terms of a standard bilinear pairing

$$u: X \times Y \to \mathbf{Z} ,$$

the monodromy pairing of [11], (11.5.2b). To do this, view the pairing as a homomorphism (again denoted u)

$$Y \to X^* ,$$

where $X^* = \mathrm{Hom}(X, \mathbf{Z})$. This map is injective, and there is a canonical isomorphism

$$\Phi \approx \mathrm{coker}(u)$$

[*loc. cit.*].

This isomorphism, valid more generally when P is not necessarily a Jacobian, is complemented by the Picard-Lefschetz formula ([11], §12) in the case under consideration. To state this formula, we orient the edges of $\mathscr{G}$ as above, and use this orientation to embed X in $\mathbf{Z}^{\mathscr{I}}$. Further, we use the Θ-polarization $P \approx \mathrm{Alb}(C)$ to obtain an isomorphism $X \approx Y$. Via this isomorphism, u becomes a bilinear pairing on X.

Theorem 2.3. *The pairing u is the restriction to X of the standard Euclidean pairing on $\mathbf{Z}^{\mathscr{I}}$. The group Φ is the cokernel of the map $X \to \mathrm{Hom}(X, \mathbf{Z})$ obtained from the inclusion of X in $\mathbf{Z}^{\mathscr{I}}$ and the Euclidean pairing on $\mathbf{Z}^{\mathscr{I}}$.*

Proof. The first statement is Théorème 12.5 of [11]. The second statement follows from the first statement, together with the isomorphism $\Phi \approx \mathrm{coker}(u)$, which is discussed above. □

Admissible curves

Next, as a variant, we relax the condition that $\mathscr{C}$ be regular, assuming instead that $\mathscr{C}$ is an *admissible curve* in the sense of Jordan-Livné [13], §3. This assumption implies that special fiber $\mathscr{C}_k$ of $\mathscr{C}$ has only ordinary double points as singularities; we define the sets $\mathscr{I}$ and $\mathscr{T}$ as above. Moreover, there is a collection of positive integers $e(i)$, $i \in \mathscr{I}$, such that the special fiber of a regular minimal model for C may be obtained from $\mathscr{C}_k$ by replacing each singular point $i \in \mathscr{I}$ with $e(i) > 1$ by a chain of $(e(i) - 1)$ copies of the projective line $\mathbf{P}^1$.

This construction produces a "blow-up" of $\mathscr{C}_k$ where the sets $\mathscr{I}$ and $\mathscr{T}$ are replaced by analogues $\tilde{\mathscr{I}}$ and $\tilde{\mathscr{T}}$. There is an evident surjective map

$$\tilde{\mathscr{I}} \to \mathscr{I}$$

gotten by contracting the $\mathbf{P}^1$'s. The associated map

$$\tau\colon \mathbf{Z}^{\mathscr{I}} \to \mathbf{Z}^{\tilde{\mathscr{I}}}$$

which takes each $i \in \mathscr{I}$ to the sum of its antecedents in $\tilde{\mathscr{I}}$ is then an injection with torsion free cokernel. On the other hand, the set $\mathscr{T}$ is a subset of $\tilde{\mathscr{T}}$, so that we have a natural injection

$$\mathbf{Z}^{\mathscr{T}} \to \mathbf{Z}^{\tilde{\mathscr{T}}}$$

Its restriction to the subgroup D of $\mathbf{Z}^{\mathscr{T}}$ gives an injection

$$\iota\colon D \to \tilde{D}\,,$$

where $\tilde{D}$ is the analogue of D for the blow-up.

The calculus introduced above computes the groups X and Φ for the Néron model of $\mathrm{Pic}^0(C)$. The computation starts with the sets $\tilde{\mathscr{I}}$ and $\tilde{\mathscr{T}}$ and an ordering of two components passing through each singular point of the blow-up. For example, this ordering defines a map $\tilde{\alpha}$ analogous to the map α seen above, whose kernel is the group X.

To relate X and Φ to the sets $\tilde{\mathscr{I}}$ and $\tilde{\mathscr{T}}$, we first order, as above, the two components of $\mathscr{C}_k$ which pass through each singular point i. We then find easily a (unique) analogous ordering for the blow up in such a way that the four maps α, $\tilde{\alpha}$, ι, and τ form a commutative square. The maps α and $\tilde{\alpha}$ are surjective, since the curve $\mathscr{C}_k$ is connected. Letting Y be the kernel of α, we discover a commutative diagram

$$\begin{array}{ccccccccc} 0 & \to & Y & \to & \mathbf{Z}^{\mathscr{I}} & \to & D & \to & 0 \\ & & \kappa\downarrow & & \tau\downarrow & & \iota\downarrow & & \\ 0 & \to & X & \to & \mathbf{Z}^{\tilde{\mathscr{I}}} & \to & \tilde{D} & \to & 0\,, \end{array} \tag{2}$$

where the map κ is induced by τ and ι. Since τ and ι are injective, so is κ. Counting ranks, we see that the cokernel of κ is a torsion abelian group. On the other hand, τ is such that its cokernel is torsion free. Since the Snake Lemma implies that the cokernel of κ injects into the cokernel of τ, κ is in fact an isomorphism. In other words, there is no difference between the groups X and Y, and we can continue to

calculate using the recipe discussed above. (This corresponds to the fact that the dual graph of $\mathscr{C}_k$ is replaced by a homotopic graph when $\mathscr{C}_k$ is replaced by its blow-up.)

At the same time, we find that Φ is the cokernel of the map γ: $Y \to \mathrm{Hom}(Y, \mathbf{Z})$ gotten from the restriction to Y of the Euclidean pairing on $\mathbf{Z}^{\mathscr{S}}$. Equivalently, this pairing is gotten by restricting to Y the pairing on $\mathbf{Z}^{\mathscr{S}}$ whose matrix is the diagonal matrix with entries $e(i)$. (In other words i and i' are paired to 0 or to $e(i)$ according as i and i' are distinct or equal.) In summary, the calculation of X and Φ proceeds essentially as if $\mathscr{C}$ were the minimal model of C. The sole complication is that the pairing one uses on $\mathbf{Z}^{\mathscr{S}}$ must take the positive integers $e(i)$ into account. (See also [11], 12.10.1.)

Theorem 2.4. *There is a natural homomorphism θ: $D \to \Phi$ whose cokernel is a quotient of the group* $\mathrm{Hom}(\mathbf{Z}^{\mathscr{S}}, \mathbf{Z})/\mathbf{Z}^{\mathscr{S}} \approx \oplus(\mathbf{Z}/e(i)\mathbf{Z})$, *the direct sum being extended over $\mathscr{S}$.*

Proof. Start with the description of Φ as the cokernel of γ. Write $\mathrm{Hom}(Y, \mathbf{Z})$ as the quotient

$$\mathrm{Hom}(\mathbf{Z}^{\mathscr{S}}, \mathbf{Z})/Y^{\perp},$$

where $Y^{\perp}$ is the group of linear forms on $\mathbf{Z}^{\mathscr{S}}$ which vanish on Y. We obtain an isomorphism

$$\Phi \approx \mathrm{Hom}(\mathbf{Z}^{\mathscr{S}}, \mathbf{Z})/(Y^{\perp} \oplus Y)$$

in which we identify Y with its image in $\mathrm{Hom}(\mathbf{Z}^{\mathscr{S}}, \mathbf{Z})$. It follows that Φ contains the subgroup

$$\Phi_0 = \mathbf{Z}^{\mathscr{S}}/(M \oplus Y),$$

where

$$M = Y^{\perp} \cap \mathbf{Z}^{\mathscr{S}}.$$

The group Φ/Φ_0 is a quotient of $\mathrm{Hom}(\mathbf{Z}^{\mathscr{S}}, \mathbf{Z})/\mathbf{Z}^{\mathscr{S}}$, which is simply the direct sum of the groups $\mathbf{Z}/e(i)\mathbf{Z}$ with $i \in \mathscr{S}$. Finally, we note that Φ_0 may be viewed as a quotient of $\mathbf{Z}^{\mathscr{S}}/Y$, a group which is isomorphic, via α, to D. We therefore obtain the desired result by letting θ be the projection of D onto Φ_0. □

Remark 2.5. Theorem 2.4 was motivated by Jordan-Livné [14], who prove a related result when C is a Shimura curve. It was used in earlier versions of this article for the purpose of analyzing the prime-to-6 parts of the component groups which appear below. However, in this write-up, no essential use is made of (2.4). The result of [14] appears below in a slightly different form as Theorem 4.3.

3. Quaternions and modular curves

In this paragraph, p and q are distinct prime numbers, and M is a positive integer prime to pq. We consider the mod q reduction of the modular curves $X_0(qM)$ and

$X_0(pqM)$. Let C be the modular curve $X_0(qM)$ over $\mathbf{Q}_q$. A model $\mathscr{C}$ of the type discussed in §2 has been studied (over $\mathbf{Z}_q$) by Deligne-Rapoport [4] and by Katz-Mazur [15]. The curve $\mathscr{C}_{\mathbf{F}_q}$ has two components, each a copy of the modular curve $X_0(M)_{\mathbf{F}_q}$ ([4], V, §1). More precisely, $\mathscr{C}_{\mathbf{F}_q}$ is obtained by attaching the two copies of $X_0(M)_{\mathbf{F}_q}$ at their supersingular points (those which arise from supersingular elliptic curves over $\bar{\mathbf{F}}_q$), a supersingular point x on the first copy being identified with its Frobenius transform $x^{(q)}$ on the second (*loc. cit.* 1.18). Therefore the set $\mathscr{T}$ has two elements. The set $\mathscr{I}$ is the set $\Sigma(M)$ of $\bar{\mathbf{F}}_q$-isomorphism classes of objects $\mathbf{E} = (E, B)$, where E is a supersingular elliptic curve over $\bar{\mathbf{F}}_q$ and B is a cyclic subgroup of E of order M. For each $i \in \mathscr{I}$, the elements $j_1(i), j_2(i)$ are the two distinct elements of $\mathscr{T}$. For convenience, we orient the $i \in \mathscr{I}$ so that $j_1(i)$ and $j_2(i)$ are each independent of i. The graph $\mathscr{G}$ in this case has precisely two vertices, and each edge connects the two distinct vertices. (No edge starts and leaves from the same vertex.) Therefore, (2.2) specializes to:

Proposition 3.1. *The character group X in the case $C = X_0(Mq)$ is the group of degree-0 divisors on the set $\Sigma(M)$ of supersingular points of $X_0(M)_{\bar{\mathbf{F}}_q}$.*

In this article, we refer to pairs $\mathbf{E} = (E, B)$ as "enhanced elliptic curves." We define in the evident way a homomorphism between two enhanced elliptic curves and, in particular, the endomorphism ring and automorphism group of an enhanced elliptic curve $\mathbf{E}$. For each $\mathbf{E}$, the $\mathbf{Q}$-algebra $H = (\mathrm{End}\ E) \otimes_{\mathbf{Z}} \mathbf{Q}$ is well known to be the unique quaternion algebra over $\mathbf{Q}$ (up to isomorphism) which is ramified precisely at q and the archimedian prime of $\mathbf{Q}$. The ring $\mathrm{End}(E)$ is a maximal order in H, while its subring $\mathrm{End}(\mathbf{E})$ is an Eichler order of level M in $\mathrm{End}(E)$. More precisely, let $\lambda\colon E \to E/B$ be the canonical quotient map. There is a natural inclusion of $\mathrm{End}(E/B)$ into H given by

$$\sigma \mapsto \lambda^{-1} \sigma \lambda .$$

The order $\mathrm{End}(\mathbf{E})$ of H is the intersection of the two maximal orders $\mathrm{End}(E)$ and $\mathrm{End}(E/B)$. It may be appropriate to describe $\mathrm{End}(\mathbf{E})$ as an *oriented* Eichler order; it is given explicitly as the intersection of an ordered pair of maximal orders of H. (An Eichler order R is, by definition, the intersection of two maximal orders, but these maximal orders need not be specified as an ordered pair. Further, R is, in general, the intersection of maximal orders in several ways.)

The automorphism group of $\mathbf{E}$ is a subgroup of $(\mathrm{End}\ E)^*$, a finite group whose order divides 24. Since $\mathrm{Aut}(\mathbf{E})$ contains the subgroup $\{\pm 1\}$, it is of even order. From ([4], VI, Th. 6.9), we obtain

$$e(i) = \frac{\#(\mathrm{Aut}\ \mathbf{E})}{2} .$$

In particular, $e(i)$ is a divisor of 12. Using (2.4), we obtain:

Proposition 3.2. *The finite group Φ is an extension by the cyclic group $\theta(D)$ of a group of exponent dividing* 12.

[More information about Φ is given in (3.12)–(3.14).]

We next recall a description of the set $\mathscr{S} = \Sigma(M)$ in terms of the arithmetic of the quaternion algebra H. This description is due to Deuring [6] in the case of supersingular elliptic curves with no additional level structure (i.e., when $M = 1$). Since all supersingular elliptic curves over $\bar{\mathbf{F}}_q$ are isogenous, one can start with a fixed $\mathbf{E}_0$ and keep track of the isomorphism classes of enhanced elliptic curves gotten by isogenies from $\mathbf{E}_0$. This problem has been studied in detail in analogous (but more complicated) problems in the theory of Shimura varieties (see for example [2, 17, 22]).

For each enhanced $\mathbf{E} = (E, B)$ over $\bar{\mathbf{F}}_q$, let $T(\mathbf{E})$ be the "adelic Tate module" of E:

$$T(\mathbf{E}) = T_q(E) \times \prod_{l \neq q} T_l(E) ,$$

where $T_q(E)$ is the Dieudonné module associated to E. In order to maintain an analogy between $T_q(E)$ and the $T_l(E)$, we take $T_q(E)$ to be the contravariant Dieudonné module attached to $E(q)$, where $E(q)$ is the q-divisible group of E. Thus we have $T_q(E) = \mathsf{M}(E(q))^t$, where $\mathsf{M}(—)^t$ is the functor considered in [23], §3. (For its definition, see [23], 3.6.)

We consider $T(\mathbf{E})$ as "enhanced" by the distinguished cyclic subgroup B of $T(\mathbf{E})/MT(\mathbf{E})$. Fix $\mathbf{E}_0 = (E_0, B_0)$, and define

$$R = \mathrm{End}(\mathbf{E}_0), \qquad H = R \otimes_{\mathbf{Z}} \mathbf{Q} .$$

Let $R_{\mathbf{f}}$ and $H_{\mathbf{f}}$ be the adelizations of these rings, i.e., their tensor products with $\hat{\mathbf{Z}}$. Given an enhanced supersingular curve $\mathbf{E} = (E, B)$, select a non-zero $\lambda \in \mathrm{Hom}(E, E_0) \otimes_{\mathbf{Z}} \mathbf{Q}$. This homomorphism identifies $T(\mathbf{E})$ with a sublattice of $V(\mathbf{E}_0) = T(\mathbf{E}_0) \otimes_{\mathbf{Z}} \mathbf{Q}$. We may find a unique element

$$g \in H_{\mathbf{f}}^*/R_{\mathbf{f}}^*$$

such that one has the equality of enhanced lattices $gT(\mathbf{E}) = T(\mathbf{E}_0)$. (This means that $gT(\mathbf{E})$ and $T(\mathbf{E}_0)$ coincide as lattices of $V(\mathbf{E}_0)$ and that the induced isomorphism

$$g\colon T(\mathbf{E})/MT(\mathbf{E}) \approx T(\mathbf{E}_0)/MT(\mathbf{E}_0)$$

carries B to B_0.) Because of the ambiguity in the choice of λ, g is well defined only in

$$H^* \backslash H_{\mathbf{f}}^*/R_{\mathbf{f}}^* .$$

Proposition 3.3. *This construction provides a bijection $\phi_{\mathbf{E}_0}$ from the set $\Sigma(M)$ of supersingular points of $X_0(M)_{\bar{\mathbf{F}}_q}$ to the coset space $H^* \backslash H_{\mathbf{f}}^*/R_{\mathbf{f}}^*$.*

For a detailed proof of similar results in the context of Shimura varieties, see [22] or [2], §11.

Variant 3.4. *The set $\Sigma(M)$ is naturally isomorphic to the set of right ideal classes of the Eichler order R of level M in H.*

Indeed, the indicated set of ideal classes is readily identified with the coset space above ([41], p. 87).

Remarks 3.5. a. The reader may prefer to view the set of right ideal classes of R as the set of isomorphism classes of locally free rank-1 right R-modules. For each $\mathbf{E}$, the group $\mathrm{Hom}(\mathbf{E}_0, \mathbf{E})$ becomes such a module under composition with endomorphisms of $\mathbf{E}_0$. The map

$$\mathbf{E} \mapsto \mathrm{Hom}(\mathbf{E}_0, \mathbf{E})$$

then gives a direct association

$$(\text{isomorphism classes of enhanced elliptic curves}) \to (\text{ideal classes})$$

which mimics that of Serre [32].

Working with $\mathrm{Hom}(\mathbf{E}, \mathbf{E}_0)$ instead of $\mathrm{Hom}(\mathbf{E}_0, \mathbf{E})$, one gets a 1-1 correspondence between isomorphism classes of locally free rank-1 *left* R-modules and isomorphism classes of enhanced supersingular elliptic curves. We see this correspondence from the lattice point of view by writing

$$g^{-1} T(\mathbf{E}) = T(\mathbf{E}_0)$$

instead of $gT(\mathbf{E}) = T(\mathbf{E}_0)$ in the construction giving (3.3).

b. There is a natural involution of $\Sigma(M)$, the Frobenius automorphism $x \mapsto x^{(q)}$. From the viewpoint of (3.3), this map arises from right multiplication on $H_{\mathbf{f}}^*$ by an element of $H_{\mathbf{f}}^*$ which is 1 locally at all primes different from q and is a uniformizer at the prime q (cf. [22], Theorem 5). In the language of (3.4), the involution associates to the class of an R-ideal I the class of the unique ideal $I' \subset I$ of index q^2 in I.

Proposition 3.6 [cf. [42], Theorem 4.5]. *Let B and B' be maximal orders of a quaternion algebra of discriminant q such that $S = B \cap B'$ is an Eichler order of level M in B. Then there is an enhanced supersingular elliptic curve $\mathbf{E}$ over $\bar{\mathbf{F}}_q$ and an isomorphism*

$$\kappa\colon (S, B) \approx (\mathrm{End}(\mathbf{E}), \mathrm{End}(E)),$$

i.e., an isomorphism $B \approx \mathrm{End}(E)$ which carries S to $\mathrm{End}(\mathbf{E})$. Moreover, let $\mathbf{E}'$ be such an elliptic curve and let κ' be an isomorphism $(S, B) \approx (\mathrm{End}(\mathbf{E}'), \mathrm{End}(E'))$. Then the pair $(\mathbf{E}', \kappa')$ is isomorphic to either $(\mathbf{E}, \kappa)$ or to $(\mathbf{E}^{(q)}, \kappa^{(q)})$.

[We say that $(\mathbf{E}, \kappa)$ and $(\mathbf{E}', \kappa')$ are isomorphic if there is an isomorphism $\mathbf{E} \approx \mathbf{E}'$ for which the induced isomorphism $\iota\colon \mathrm{End}(\mathbf{E}) \approx \mathrm{End}(\mathbf{E}')$ satisfies $\kappa' \iota = \kappa$.]

Proof. Fix an enhanced supersingular elliptic curve $\mathbf{E}_0$ as before. Let

$$R = \mathrm{End}(\mathbf{E}_0), \qquad A = \mathrm{End}(E_0), \qquad H = R \otimes \mathbf{Q}.$$

After choosing and fixing an isomorphism $B \otimes \mathbf{Q} \approx H$, we may (and do) assume that B, B' and S are orders in H.

We first consider all pairs $(\mathbf{E}, \kappa)$ consisting of an enhanced elliptic curve $\mathbf{E}$ and an injection $\kappa\colon \mathrm{End}(\mathbf{E}) \otimes \mathbf{Q} \to H$ (which need not necessarily map $\mathrm{End}(\mathbf{E})$ to S and $\mathrm{End}(\mathbf{E})$ to B). For each non-zero $\lambda \in \mathrm{Hom}(E, E_0) \otimes_{\mathbf{Z}} \mathbf{Q}$, we obtain such an injection κ_λ by mapping $e \in \mathrm{End}(\mathbf{E}) \otimes \mathbf{Q}$ to $\lambda e \lambda^{-1}$. By the Skolem-Noether Theorem, every κ is of the form κ_λ; moreover, $\lambda \in \mathrm{Hom}(E, E_0) \otimes_{\mathbf{Z}} \mathbf{Q}$ and

$\lambda' \in \mathrm{Hom}(E, E_0) \otimes_{\mathbf{Z}} \mathbf{Q}$ give isomorphic pairs $(\mathbf{E}, \kappa)$, $(\mathbf{E}', \kappa')$ if and only if there is an isomorphism $\iota\colon \mathbf{E} \to \mathbf{E}'$ such that λ and $\lambda'\iota$ differ by an element of $\mathbf{Q}^*$. (Cf. [42], Prop. 3.4.)

The construction

$$(\mathbf{E}, \lambda) \mapsto T(\mathbf{E}) \subset V(\mathbf{E}_0)$$

furnishes a 1-1 correspondence between the set of isomorphism classes of pairs $(\mathbf{E}, \lambda)$ and the set $H_{\mathbf{f}}^*/R_{\mathbf{f}}^*$ of "enhanced" lattices in $V(\mathbf{E}_0)$. Dividing by $\mathbf{Q}^*$, we obtain a 1-1 correspondence between $H_{\mathbf{f}}^*/(R_{\mathbf{f}}^*\mathbf{Q}^*)$ and the set of isomorphism classes of pairs $(\mathbf{E}, \kappa)$ with $\mathbf{E}$ an enhanced elliptic curve and κ an injection $\mathrm{End}(\mathbf{E}) \otimes \mathbf{Q} \to H$.

Take $g \in H_{\mathbf{f}}^*$ and consider the associated pair $(\mathbf{E}, \kappa)$. The image of $\mathrm{End}(\mathbf{E})$ (resp. $\mathrm{End}(E)$) in H is the order $H \cap (gR_{\mathbf{f}}g^{-1})$ (resp. $H \cap (gA_{\mathbf{f}}g^{-1})$). Thus κ maps $\mathrm{End}(\mathbf{E})$ to R and $\mathrm{End}(E)$ to A if and only if we have the equalities

$$gA_{\mathbf{f}}g^{-1} = B_{\mathbf{f}}, \qquad gR_{\mathbf{f}}g^{-1} = S_{\mathbf{f}}.$$

Examine these equalities locally at each prime l, i.e., for g now in H_l^*. When $l = q$, the condition on g is empty. Indeed, the quaternion algebra H_q over $\mathbf{Q}_q$ has a unique maximal order ([41], Lemme 1.5, p. 34), so that all $g \in H_q^*$ take A_q to B_q and R_q to S_q. Note that there are two classes in $H_q^*/(R_q^*\mathbf{Q}_q^*)$: the valuation on H_q^* makes H_q^*/R_q^* isomorphic to $\mathbf{Z}$, and division by $\mathbf{Q}_q^*$ corresponds to division of $\mathbf{Z}$ by $2\mathbf{Z}$.

When l is prime to qM, there is only one equality to be satisfied, since A coincides with R and B with S at the prime l. This equality can be satisfied, since all maximal orders in $\mathrm{M}(2, \mathbf{Q}_l)$ are conjugate ([41], Th. 2.3, p. 38). Moreover, the g for which the equality is satisfied form a single class in $H_l^*/(R_l^*\mathbf{Q}_l^*)$, since the normalizer of $\mathrm{M}(2, \mathbf{Z}_l)$ in $\mathbf{GL}(2, \mathbf{Q}_l)$ is $\mathbf{GL}(2, \mathbf{Z}_l)\mathbf{Q}_l^*$.

Finally, suppose that l divides M, and let $n > 0$ be the valuation of M at l. The two Eichler orders R_l and S_l are each intersections of a unique pair of maximal orders of $H_l \approx \mathrm{M}(2, \mathbf{Q}_l)$ ([41], 2.4, p. 39). The order S_l is the intersection of B_l and B_l', while R_l is the intersection of A_l and A_l', where A' is the endomorphism ring of the elliptic curve E' gotten from E by dividing E by the cyclic subgroup of order M which enhances it. An element g of H_l^* thus conjugates A_l to B_l and R_l to S_l if and only if it conjugates A_l to B_l and A_l' to B_l'.

We may regard A_l, B_l, A_l', and B_l' as vertices a, b, a', b' of the tree Δ associated to $\mathbf{SL}_2$ over $\mathbf{Q}_l$ ([33], Ch. II). To do this, we note that the vertices of Δ are the lattices in $\mathbf{Q}_l \oplus \mathbf{Q}_l$, taken modulo homothety. The map sending the lattice $L \subset \mathbf{Q}_l \oplus \mathbf{Q}_l$ to the maximal order $\mathrm{End}(L)$ of $\mathrm{M}(2, \mathbf{Q}_l)$ sets up a 1-1 correspondence between the vertices of Δ and the maximal orders in $\mathrm{M}(2, \mathbf{Q}_l)$, cf. [41], p. 41.

Since R and S are Eichler orders of level M, the vertices a and b are at distance n from each other, as are the vertices a' and b'. By the Elementary Divisor Theorem, we may choose a basis e_1, e_2 of $\mathbf{Q}_l \oplus \mathbf{Q}_l$ so that a is represented by the lattice $\mathbf{Z}_l e_1 \oplus \mathbf{Z}_l e_2$ and b by the lattice $\mathbf{Z}_l e_1 \oplus l^n \mathbf{Z}_l e_2$. Similarly, there is a basis f_1, f_2 of $\mathbf{Q}_l \oplus \mathbf{Q}_l$ so that a' is represented by the lattice $\mathbf{Z}_l f_1 \oplus \mathbf{Z}_l f_2$ and b' by the lattice $\mathbf{Z}_l f_1 \oplus l^n \mathbf{Z}_l f_2$. If $g \in \mathbf{GL}(2, \mathbf{Q}_l)$ maps e_1 to f_1 and e_2 to f_2, then g conjugates A_l to B_l

and A_l' to B_l'. On the other hand, if h also conjugates A_l to B_l and A_l' to B_l', we have

$$h^{-1}g \in N(A_l) \cap N(B_l) = (A_l^* \mathbf{Q}_l^*) \cap (B_l^* \mathbf{Q}_l^*) = (A_l^* \cap B_l^*)\mathbf{Q}_l^* = R_l^* \mathbf{Q}_l^* .$$

Hence the g conjugating A_l to B_l and A_l' to B_l' again make up a single class in $H_l^*/(R_l^* \mathbf{Q}_l^*)$.

From this local information, we deduce that the g in $H_{\mathbf{f}}^*$ which conjugate $A_{\mathbf{f}}$ to $B_{\mathbf{f}}$ and $R_{\mathbf{f}}$ to $S_{\mathbf{f}}$ form exactly two classes in $H_{\mathbf{f}}^*/(R_{\mathbf{f}}^* \mathbf{Q}^*)$. These classes are interchanged by left multiplication by any idele which is trivial outside the prime q and has odd valuation at q. It is a standard fact that this multiplication corresponds to the Frobenius map; cf. [22] and Remark 3.5b above. □

Action of Hecke operators on X

Each modular curve $X_0(N)$ is endowed with familiar Hecke correspondences for $n \geqq 1$ (see, for example, [39], Chapter 7). We write T_n for the n^{th} correspondence. In the notation of [39], one considers the double cosets $\Gamma_0(N)\alpha\Gamma_0(N)$ arising from those matrices $\alpha \in \Delta'$ which satisfy $\det(\alpha) = n$. To each such double coset is associated a correspondence $X_{SS}(\alpha)$. The Hecke correspondence T_n is defined as the sum of those correspondences $X_{SS}(\alpha)$ for which $\det(\alpha) = n$. (See [39], page 183.)

There is an equivalent "modular" definition of the T_n which involves mapping an elliptic curve with $\Gamma_0(N)$-structure to an appropriate formal sum of such objects. This interpretation is certainly well known; cf. (7.2.4) and Proposition 3.36 of [39]. The "modular" interpretation of the curve $X_0(N)$ and its correspondences T_n allows us to define these objects over the rational field $\mathbf{Q}$.

Each correspondence T_n of $X_0(N)$ induces an endomorphism of $J_0(N)$ in *two* ways. This circumstance arises because the association of a curve to its Jacobian is simultaneously a covariant or a contravariant functor, according as one takes the "Albanese" or the "Picard" point of view.

To elaborate on this idea in an abstract context, we first consider an irreducible curve X which is given as a subvariety of $U \times V$, where U and V are curves over a field k. (More generally, one should consider an integral linear combination of such subvarieties, as in §7.2 of [39].) Let $f\colon X \to U$ and $g\colon X \to V$ be the maps obtained from the inclusion of X in the product and the two canonical projections of $U \times V$ onto its factors. Let A_X, A_U, and A_V be the Jacobians of X, U and V, respectively. Assume that X is a correspondence, i.e., that f and g are non-constant maps.

The maps f and g induce homomorphisms $f_*\colon A_X \to A_U$ and $g_*\colon A_X \to A_V$ by Albanese functoriality, and homomorphisms $f^*\colon A_U \to A_X$ and $g^*\colon A_V \to A_X$ by Pic functoriality of the Jacobian. The compositions $g_* f^*$ and $f_* g^*$ are then homomorphisms $\xi\colon A_U \to A_V$ and $T\colon A_V \to A_U$, respectively. These are the elements of $\mathrm{Hom}(A_U, A_V)$ and $\mathrm{Hom}(A_V, A_U)$ which are associated to X. (In [39], §7.2, only the former element is considered.)

In the special case where X is the graph of a map of curves $\phi\colon U \to V$, it is clear that ξ and T are the maps of Jacobians which ϕ induces by Albanese functoriality and Pic functoriality, respectively. Viewing the notion of "correspondence" as a generalization of that of "map," we are led in the general case to refer to ξ and T as

the Albanese and Pic maps induced by X. We consider that ξ and T have equal standing as homomorphisms of Jacobians induced by a correspondence. On the other hand, it follows from the definitions of ξ and T that ξ and T are exchanged if we permute U and V and replace X by its transpose. In particular, if we choose to consider only maps induced by Albanese functoriality, we are forced to replace X by its transpose in order to obtain T.

We remark also that A_X, A_U, and A_V are each canonically auto-dual, so that the dual of a homomorphism $A_X \to A_U$ (for instance) may be regarded as a homomorphism $A_U \to A_X$. It is a well known property of Jacobians that f_* is the dual of f^* and vice versa; analogously, g_* is the dual of g^* and vice versa. It follows from this that ξ and T are each other's duals. In the special case where $U = V$, we may conclude that ξ and T are permuted by the Rosati involution of $\mathrm{End}(A_U)$ associated with the canonical (theta) polarization of the Jacobian A_U.

We now specialize to the case where U and V are both equal to the modular curve $X_0(N)$ and X is replaced by the correspondence $T(n)$. The endomorphism of $J_0(N)$ which T_n induces by Albanese functoriality is the endomorphism denoted ξ_n in [39], Chapter 7. Its dual is the endomorphism of $J_0(N)$ which T_n induces by Picard functoriality. It seems that there is little danger in using the symbol T_n to denote this latter map. According to our general discussion, we then have

$$T_n = \xi_n^*, \qquad T_n^* = \xi_n, \tag{3}$$

where the exponent * is the Rosati involution on $\mathrm{End}(J_0(N))$.

Furthermore, let $w = w_N$ be the standard Atkin-Lehner involution of $X_0(N)$, i.e., the involution denoted $X_{SS}(\tau)$ in [39], §7.5. Write again w for the corresponding involution of $J_0(N)$. (An involution on a curve induces the same endomorphism of its Jacobian under the Pic and Albanese functorialities.) Then one has

$$wT_nw = \xi_n, \qquad w\xi_nw = T_n. \tag{4}$$

These formulas follow from the identities given at the bottom of page 193 for the transpose of a modular correspondence, together with Prop. 3.54, of [39].

Consider the subalgebras $\Xi = \Xi_N$ and $\mathbf{T} = \mathbf{T}_N$ of $\mathrm{End}(J_0(N))$ generated by the ξ_n and by the T_n, respectively. The Rosati involution of $\mathrm{End}(J_0(N))$ (or, alternatively, conjugation by w) induces an isomorphism $\Xi \approx \mathbf{T}$. By viewing $J_0(N)$ as the Albanese variety of $X_0(N)$, we may identify the space of invariant differentials on $J_0(N)$ with the classical space $S_2(\Gamma_0(N))$ of weight-2 cusp forms for the group $\Gamma_0(N)$. Via this identification, each operator ξ_n induces the classical operator T_n^* on $S_2(\Gamma_0(N))$. (Cf. [39], page 183.) Moreover, the resulting representation of Ξ is faithful, since an endomorphism of an abelian variety over $\mathbf{C}$ is determined by its action on the cotangent space to the abelian variety at the origin. Therefore, Ξ and $\mathbf{T}$ may each be identified with the algebra generated by the classical operators T_n on the space $S_2(\Gamma_0(N))$. This algebra is a free finitely-generated $\mathbf{Z}$-module whose rank coincides with the dimension of the abelian variety $J_0(N)$, i.e., with the dimension of $S_2(\Gamma_0(N))$, cf. [39], Th. 3.45.

Once the endomorphisms T_n of $J_0(N)$ have been defined over $\mathbf{Q}$, they act automatically on the Néron model of $J_0(N)$ and in particular on the fiber of this Néron model at each prime dividing N. Consider now the special situation where

$N = qM$, q being prime to M as above. Let T denote the "toric part" (i.e., the largest torus) in the fiber at q of the Néron model. The T_n induce endomorphisms of T and therefore act by functoriality on the character group X of T. We propose to describe explicitly this action. To do this, we use the canonical isomorphism

$$X \approx H_1(\mathscr{G}, \mathbf{Z})$$

of (2.1). In view of the inclusion (1) of §2, it is natural to relate the actions of the T_n on X to the correspondences induced by the T_n on the set $\mathscr{S} = \Sigma(M)$ of isomorphism classes of enhanced supersingular elliptic curves over $\bar{\mathbf{F}}_q$. Note, however, that the map $X \to \mathbf{Z}^{\mathscr{S}}$ depends on our having oriented each edge $i \in \mathscr{S}$. Our discussion must take into account any inversions introduced by the T_n.

We first consider the case where n is prime to q. Then there are no inversions, as the T_n "preserve" each component of $X_0(N)_{\mathbf{F}_q}$. Moreover, the T_n operate on $\Sigma(M)$ in the evident way, i.e., via the same "modular rules" which define the T_n over $\mathbf{Q}$. For the sake of completeness, let us recall the rule for T_n when n is a prime number $r \neq q$; we give the expression for $T_r(\mathbf{E})$, where $\mathbf{E}$ is an elliptic curve E which is enhanced by a cyclic subgroup of order M.

We distinguish cases according as r is prime to M or a divisor of M. In the former case, we have the standard expression

$$T_r(\mathbf{E}) = \sum_C \mathbf{E}/C \ ,$$

where the sum is taken over all subgroups C of order r in E and where $\mathbf{E}/C$ is the elliptic curve E/C with the evident subgroup of order M. In the case where r divides M, the enhancement of E provides E, in particular, with a subgroup D of order r. We have

$$T_r(\mathbf{E}) = \sum_{C \neq D} \mathbf{E}/C \ .$$

We now compare the actions of T_q and the Atkin-Lehner involution $w = w_q$ on $X_0(N)$. Recall that w_q is defined in "modular" terms by regarding $X_0(N)$ as classifying triples (E, C_M, C_q), where the two latter elements are cyclic subgroups of the elliptic curve E having orders M and q, respectively. The involution w_q maps such a triple (E, C_M, C_q) to the triple

$$(E/C_q, (C_M \oplus C_q)/C_q, E[q]/C_q) \ .$$

We again denote by w_q the involutions induced by w_q on $J_0(N)$, the Néron model of $J_0(N)$, the fiber of this model in characteristic q, etc. Especially, w_q acts on the torus T and on its character group X. The following result is a variant of a formula found by Atkin-Lehner (cf. [1], Th. 3); the identity we give exploits the fact that T pertains to cusp forms of level $N = qM$ which are "q-new," cf. (3.10).

Proposition 3.7. *The identity $w_q = -T_q$ holds on the torus T.*

Proof. Consider the two "degeneracy" maps α, β: $X_0(N) \to X_0(M)$ (cf. [19]), defined over $\mathbf{Q}$ from a modular point of view by

$$\alpha: (E, C_M, C_q) \mapsto (E, C_M), \qquad \beta: (E, C_M, C_q) \mapsto (E/C_q, (C_M \oplus C_q)/C_q) \ .$$

A calculation gives the identity $w_q + T_q = \alpha^* \beta_*$ of endomorphisms of $J_0(N)$, where * and $_*$ refer to Pic and Albanese functoriality, respectively. In particular, $w_q + T_q$ factors through the map $\beta_*: J_0(N) \to J_0(M)$. Considering fibers at q of Néron models, we find that the restriction to T of $w_q + T_q$ factors through a map $T \to J_0(M)_{\mathbf{F}_q}$. All such maps are 0, since T is a torus and $J_0(M)$ is an abelian variety. □

Proposition 3.8. (i) *The involution w_q permutes the two components of $X_0(N)_{\mathbf{F}_q}$. It acts on the set $\mathscr{S}$ of singular points of $X_0(N)_{\mathbf{F}_q}$ as the Frobenius morphism $x \mapsto x^{(q)}$.* (ii) *The action of T_q on the character group X is the restriction to X of the map on $\mathbf{Z}^{\Sigma(M)}$ induced by the Frobenius automorphism of $\Sigma(M)$. This restriction is the Frobenius automorphism of X.*

Proof. For (i), see [4], Chapter V, §1. The first statement of (ii) follows from (3.7) and (i), as w_q combines the Frobenius automorphism of $\Sigma(M)$ with an inversion of the two vertices of the graph $\mathscr{G}$. The second statement of (ii) then results from the fact that the two components of $X_0(qM)_{\mathbf{F}_q}$ are rational. (Cf. [18], Appendix, §3.) □

Old and new

Let $\mathbf{T} = \mathbf{T}_{M_q}$ be the subring of $\mathrm{End}(J_0(Mq))$ generated by all Hecke operators T_n for $n \geqq 1$. The action of $\mathbf{T}$ on the cotangent space S of the dual of $J_0(Mq)_{\mathbf{C}}$ identifies $\mathbf{T}$ with a ring of endomorphisms of S. Since the dual of $J_0(Mq)$ is simply the Albanese variety of $X_0(Mq)$, S is the classical space $S_2(\Gamma_0(Mq))$ of weight-2 cusp forms on $\Gamma_0(Mq)$. Since the action of T_n on S obtained in this manner coincides with the classical action, $\mathbf{T}$ is the usual subring of $\mathrm{End}(S)$ generated by the Hecke operators. In particular, the ring $\mathbf{T}$ is a free $\mathbf{Z}$-module whose rank is the dimension of S, i.e., the dimension of the abelian variety $J_0(Mq)$ ([39], Th. 3.45).

The q-old subspace of S (cf. [1]) is defined to be the direct sum

$$S_0 = \alpha^*(S_2(\Gamma_0(M))) \oplus \beta^*(S_2(\Gamma_0(M)))$$

of two copies of $S_2(\Gamma_0(M))$ which occurs naturally in $S = S_2(\Gamma_0(Mq))$. The corresponding new space is the orthogonal complement S_1 to S_0 in S, relative to the Petersson inner product on S. Both S_0 and S_1 are $\mathbf{T}$-stable subspaces of S; let $\mathbf{T}_0$ and $\mathbf{T}_1$ be the images of $\mathbf{T}$ in the endomorphism rings of these spaces. We say that $\mathbf{T}_0$ and $\mathbf{T}_1$ are the *q-old* and *q-new* quotients of $\mathbf{T}$. The product map

$$\mathbf{T} \to \mathbf{T}_0 \times \mathbf{T}_1$$

identifies $\mathbf{T}$ with a subring of finite index of $\mathbf{T}_0 \times \mathbf{T}_1$.

Consider now the fiber in characteristic q of the Néron model of $J_0(Mq)$. This $\mathbf{F}_q$-group is an extension of a finite group Φ by its connected component J. As is well known (cf. [18], Appendix), the results of Raynaud [24] and Deligne-Rapoport [4] combine to produce an exact sequence

$$1 \to T \to J^0 \to J_0(M) \times J_0(M) \to 0\,, \tag{5}$$

where $T = \mathrm{Hom}(X, \mathbf{G}_m)$ is the torus whose character group is studied above. All endomorphisms of $J_0(Mq)$ which are defined over $\mathbf{Q}$ extend to the Néron model of $J_0(Mq)$ and operate via (5) on T and on $J_0(M) \times J_0(M)$. The action of $\mathbf{T}$ on T corresponds to the action of $\mathbf{T}$ on X which is discussed above. The action of $\mathbf{T}$ on $J_0(M) \times J_0(M)$ is completely transparent, except for the endomorphism of $J_0(M) \times J_0(M)$ arising from T_q. This endomorphism is not (necessarily) the same as that gotten by making the endomorphism $T_q \in \mathbf{T}_M$ act diagonally on the product. It is given by a 2-by-2 matrix of endomorphisms of $J_0(M)$ which could be made explicit without difficulty. It is to be noted, in this connection, that the map ω: $J^0 \to J_0(M) \times J_0(M)$ which appears above is deduced by Pic functoriality from a pair of maps $X_0(M) \rightrightarrows X_0(Mq)$ which exist naturally only in characteristic q. The map ω is to be distinguished from the map $J^0 \to J_0(M) \times J_0(M)$ gotten by Albanese functoriality from the two degeneracy maps $X_0(Mq) \rightrightarrows X_0(M)$ in characteristic 0.

Remark 3.9. The degeneracy maps α and β introduced above combine to produce (by Pic functoriality) a map

$$\rho: J_0(M) \times J_0(M) \to J_0(Mq)\,,$$

which is easily seen to have finite kernel. (The kernel was determined in [28].) It follows from the finiteness of the kernel that there is a unique endomorphism ξ of $J_0(M) \times J_0(M)$ (considered as an abelian variety up to isogeny) such that $\rho\xi = T_q\rho$. This endomorphism is explicitly given as

$$(x, y) \mapsto (\tau x + qy,\ -x)\,,$$

where τ is the q^{th} Hecke operator of $J_0(M)$. (Cf. (3.19) below.)

Theorem 3.10. *The action of* $\mathbf{T}$ *on the torus* T *cuts out the* q*-new quotient* $\mathbf{T}_1$ *of* $\mathbf{T}$. *I.e., an element* t *of* $\mathbf{T}$ *is* 0 *on* T *if and only if it is* 0 *on the* q*-new subspace* S_1 *of* S.

Proof. Let A be the image of the map ρ of (3.9), and let Q be the cokernel of ρ. (We refer to A and Q as the q-old subvariety and the q-new quotient of $J_0(Mq)$, cf. [19].) Dualizing the exact sequence of abelian varieties

$$0 \to A \to J_0(Mq) \to Q \to 0$$

and applying the cotangent functor over $\mathbf{C}$, we obtain the exact sequence of $\mathbf{C}$-vector spaces

$$0 \to S_0 \to S \to S_1 \to 0\,.$$

(We identify the orthogonal complement S_1 to S_0 with the indicated quotient of S.) An element t of $\mathbf{T}$ thus maps to 0 in $\mathbf{T}_1$ if and only if it acts as 0 on Q.

It is clear that the abelian variety Q has purely toric reduction in characteristic q, as A has good reduction at q and the dimensions of T and Q coincide. Let U be the connected component of 0 in the fiber at q of the Néron model of Q, so that U is a torus of the same dimension as T. By a well known property of abelian varieties with purely toric reduction, the action of $\mathrm{End}_{\mathbf{Q}}(Q)$ on U is faithful. Therefore, $t \in \mathbf{T}$ maps to 0 in $\mathbf{T}_1$ if and only if it acts as 0 on U.

The structural map $\pi: J_0(Mq) \to Q$ induces a homomorphism $J^0 \to U$. Combining this map with the inclusion of T in J^0, we get a T-equivariant map $\pi_*: T \to U$. Choose a map $\eta: Q \to J_0(Mq)$ for which $\pi\eta$ is an isogeny from Q to Q. We obtain in characteristic q a map $\eta_*: U \to T$ for which $\pi_*\eta_*$ is an isogeny. Since T and U have the same dimensions, π_* is an isogeny. Hence $t \in \mathbf{T}$ maps to 0 in $\mathbf{T}_1$ if and only if it acts as 0 on T. □

Theorem 3.11. *View $J_0(M) \times J_0(M)$ as a* **T***-module via* (5). *Let t be an element of* **T**. *Then t acts as* 0 *on $J_0(M) \times J_0(M)$ if and only if t is* 0 *in* $\mathbf{T}_0$.

Proof. This is similar to (3.10). With A as above, $t \in \mathbf{T}$ acts as 0 on A if and only if it acts as 0 on S_0. The inclusion of A in $J_0(Mq)$ induces in characteristic q a map $A \to J^0$. The composition of this map with the map $J^0 \to J_0(M) \times J_0(M)$ of (5) is an isogeny. Hence t acts as 0 on S_0 if and only if it acts as 0 on $J_0(M) \times J_0(M)$. □

Action of Hecke operators on Φ

We now study the action of the Hecke operators $T_n \in \mathrm{End}(J_0(qM))$ on the component group Φ associated with the reduction of $X_0(qM)$ over $\mathbf{F}_q$. Our aim is to prove that Φ is "Eisenstein" in the sense that T_r operates on Φ by multiplication by $1 + r$, for almost all primes r. We do this by reducing the question to one involving supersingular elliptic curves over $\bar{\mathbf{F}}_q$. (See [30] and [8] for more information about component groups attached to Jacobians of modular curves.)

We first specialize to $X_0(qM)$ the description of Φ given in §2. Let Λ be the free abelian group on the set $\mathscr{S}$ of supersingular points of $X_0(M)_{\bar{\mathbf{F}}_q}$ and let $X \subset \Lambda$ be the subgroup of Λ consisting of elements of degree 0. Thus X is the character group of the torus T associated with $X_0(qM)_{\mathbf{F}_q}$. Note that $\mathscr{S}$ is the set of isomorphism classes of pairs $\mathbf{E} = (E, B)$, where E is a supersingular elliptic curve over $\bar{\mathbf{F}}_q$ and B is a cyclic subgroup of E of order M. (Thus $\mathbf{E}$ is an "enhanced elliptic curve" in the jargon introduced above.) For each $i \in \mathscr{S}$, we define $e(i)$ as above; the $e(i)$ furnish a diagonal pairing on Λ. We let

$$\kappa: \Lambda \to \Lambda^*$$

be the embedding of Λ into $\Lambda^* = \mathrm{Hom}(\Lambda, \mathbf{Z})$ defined by this pairing, and we define similarly

$$\iota: X \to X^*$$

by restricting the pairing to X.

The results of §2 (especially 2.3) provide us with an isomorphism

$$\Phi \approx \mathrm{coker}(\iota) .$$

In this model for Φ, the action of T_n on the target $X^* = \mathrm{Hom}(X, \mathbf{Z})$ of ι is the action $\mathrm{Hom}(T_n, \text{identity})$ induced by the standard action of T_n on X which we considered above. The action of T_n on the source X of ι, however, is that induced by the transpose $\xi_n = w_{qM} T_n w_{qM}$ acting on X. This circumstance arises because the source

of ι is naturally the character group occurring in the reduction of the Albanese variety to $X_0(qM)$; the Θ-polarization translates the action of T_n on the Albanese to the action of ξ_n on $J_0(qM)$.

These subtleties do not really intervene in our analysis, since we are interested only in the action on Φ of the T_r for r prime and prime to qM. As is well known, we have $T_r = \xi_r$ under this hypothesis on r. For such r, we define a correspondence η_r on $X_0(qM)$ by the formula

$$\eta_r = T_r - (1 + r) .$$

We consider the action of η_r by functoriality on Φ.

Theorem 3.12. *The group Φ is annihilated by η_r for all primes r with $(r, qM) = 1$.*

(For the statement of a slightly more precise result, see Theorem 3.22.)

Proof. Fix such a prime r. An action of T_r on Λ is obtained by linearity from the map

$$\mathbf{E} \mapsto \sum_H \mathbf{E}/H ,$$

where the sum runs over the $(r + 1)$ subgroups of E having order r. (The quotient $\mathbf{E}/H$ is simply the quotient E/H with the evident enhancement.) This action induces the functorial actions of T_r on the subgroup X of Λ and on the duals X^* and Λ^* of X and Λ. It is well known (and not hard to verify) that ι and κ commute with these actions. (This fact corresponds to the relation $T_r = \xi_r$.) The actions of η_r on these groups are realized by subtracting the endomorphisms T_r and "multiplication by $r + 1$" of these groups.

We have $\Phi = X^*/X$, where ι is used to embed X into X^*. Theorem (3.12) thus asserts that we have

$$\eta_r(X^*) \subset X .$$

In fact we shall prove the analogous inclusion

$$\eta_r(\Lambda^*) \subset \Lambda , \tag{6}$$

in which κ is used to embed Λ (and its subgroup X) into Λ^*.

Before doing this, we note that (6) implies the apparently stronger inclusion

$$\eta_r(\Lambda^*) \subset X , \tag{7}$$

from which Theorem (3.12) visibly follows. Indeed, take $\zeta \in \Lambda^*$. For $e = (\Lambda^* : \Lambda)$, we have $e\zeta \in \Lambda$. We then get $\eta_r(e\zeta) \in X$ because of the obvious inclusion $\eta_r(\Lambda) \subset X$. Assuming (6), we find that $\eta_r(\zeta)$ is an element of Λ for which $e \cdot \eta_r(\zeta) \in X$. Since Λ/X is the torsion-free group $\mathbf{Z}$, we have $\eta_r(\zeta) \in X$.

To prove (6), we first express this inclusion as a concrete divisibility. Let $\{i^*\}$ be the basis of Λ^* which is dual to the basis $\mathscr{S} = \{i\}$ of Λ. For each i^*, we must exhibit a $\lambda \in \Lambda$ such that $\eta_r(i^*)(j) = \lambda \cdot j$ for each $j \in \mathscr{S}$. By the definition of the action of η_r on Λ^*, $\eta_r(i^*)(j)$ represents the coefficient of i in $\eta_r(j)$, a number we may write

$$\frac{1}{e(i)} i \cdot \eta_r(j) = \frac{1}{e(i)} j \cdot \eta_r(i) ,$$

where we have used the η_r-equivariance of κ to equate the two displayed quantities. We may thus take $\lambda = \eta_r(i)/e(i)$ if $\eta_r(i) \in e(i)\Lambda$, i.e., if the coefficient of each j in $\eta_r(i)$ is divisible by $e(i)$. Since the sum of the coefficients of $\eta_r(i)$ is 0, it suffices to prove this divisibility only for $j \neq i$. For these j, the coefficient of j in $\eta_r(i)$ coincides with the coefficient of j in $T_r(i)$.

Fix, then, i and j with $i \neq j$, and let $\mathbf{E} = (E, B)$ and $\mathbf{F} = (F, C)$ be enhanced elliptic curves which represent these isomorphism classes. Let $e = e(i) = \mathrm{card}(A)$, where A is the finite group

$$\mathrm{Aut}(\mathbf{E})/\{\pm\}\,.$$

We must show that the number of subgroups H of E, having order r, for which $\mathbf{E}/H \approx \mathbf{F}$, is divisible by e.

There is an evident operation of A on the set of such H, and it suffices to show that this action is free. To do this, we suppose that we have $\mathbf{E}/H \approx \mathbf{F}$ and $\alpha(H) = H$ with $\alpha \in \mathrm{Aut}(\mathbf{E})$. We must show that we have $\alpha \in \{\pm 1\}$. Assuming the contrary, we observe that α has order 3, 4, or 6, since α may be regarded as a unit in some imaginary quadratic field. (Changing the sign of α if necessary, we may assume that it has order 4 or 6.)

Let R be the subring of $\mathrm{End}(\mathbf{E})$ generated by α, so that R is isomorphic to either the ring of Gaussian integers, or else the integer ring of $\mathbf{Q}(\sqrt{-3})$. We note that H is an R-submodule of the free rank-1 R/rR-module $E[r]$. Such submodules are in 1-1 correspondence with the ideals $\wp$ of R which contain (r). Since R is a principal ideal domain, we have $\wp = (\pi)$ for some π dividing r in R, and then H is the kernel of $\pi' = r/\pi$ on E. The endomorphism π' of $\mathbf{E}$ then induces an isomorphism $\mathbf{E}/H \approx \mathbf{E}$, contrary to our assumption that $\mathbf{E}$ and $\mathbf{F}$ are non-isomorphic.

Remark 3.13. The coefficients of $T_r(i)$ form the "i^{th} column" of a classical Brandt matrix. These coefficients have been frequently studied, and the divisibility just established is presumably well known.

The following result may be regarded as a structural explanation of (3.12). For another, see Theorem 3.22 below.

Proposition 3.14. *For each prime number r prime to qM, the map η_r: $\Lambda^* \to X$ deduced from* (7) *induces an injection*

$$\Phi \to X/\eta_r X\,.$$

Proof. Write

$$\Phi = X^*/X = \Lambda^*/(X \oplus X^\perp)\,,$$

where $X^\perp$ is the subgroup of Λ^* consisting of linear forms on Λ which vanish on X. The map η_r preserves X and hence also $X^\perp$. Thus, η_r maps $X^\perp$ to $X^\perp \cap X = 0$. It follows that η_r induces a map σ: $\Phi \to X/\eta_r X$ as indicated.

From Weil's Riemann Hypothesis, we may deduce that the endomorphism η_r of $J_0(qM)$ is an isogeny. Hence η_r acts injectively on X (so that $X/\eta_r X$ is a finite group). We conclude next that the kernel of

$$\eta_r\colon \Lambda^* \to X$$

is $X^{\perp}$, since the quotient $\Lambda^*/X^{\perp}$ is torsion free. Hence if $\eta_r(\zeta) = \eta_r(x)$ with $x \in X$ and $\zeta \in \Lambda^*$, we get that $\zeta - x \in X^{\perp}$. This gives the injectivity of σ. □

Comparison with $X_0(pqM)$

Let X again be the group of degree-0 divisors on the set of supersingular points of $X_0(M)_{\bar{\mathbf{F}}_q}$. Let L be the analogue of X with M replaced by pM, i.e., the character group associated with $X_0(pqM)_{\bar{\mathbf{F}}_q}$. (We recall that p is a prime number which is prime to qM.) The analogue of proposition (3.1) for $X_0(pqM)$ describes L in terms of supersingular elliptic curves which are enhanced by cyclic subgroups of order pM. We prefer to regard such objects as p-isogenies

$$\mathbf{E}_1 \to \mathbf{E}_2 ,$$

where $\mathbf{E}_1$ and $\mathbf{E}_2$ are enhanced by subgroups of order M as before. (We will continue to understand that "enhanced elliptic curves" are elliptic curves which are enhanced by cyclic subgroups of order M.)

There are two natural degeneracy maps

$$\alpha, \beta: X_0(pqM) \rightrightarrows X_0(qM) ,$$

defined as in the discussion before (3.7), but with p replacing q. These induce two maps $\alpha_*, \beta_*: L \rightrightarrows X$, which are realized explicitly by the maps sending $[\mathbf{E}_1 \to \mathbf{E}_2]$ to $\mathbf{E}_1$ or $\mathbf{E}_2$. They combine to make a single degeneracy map

$$\delta: L \to (X \oplus X) .$$

Theorem 3.15. *The map δ is surjective.*

We give a proof based on two lemmas, derived from results of Eichler concerning the arithmetic of Eichler orders in quaternion algebras.

Lemma 3.16. *Let* $\mathbf{E}$ *be an enhanced supersingular elliptic curve over* $\mathbf{F}_q$. *There is a non-zero endomorphism of* $\mathbf{E}$ *whose degree (as an endomorphism of* E*) is an odd power of* p.

Proof. For $x \in R = \mathrm{End}(\mathbf{E})$, the degree of x as an endomorphism coincides with the reduced norm of x as an element of H. To prove (3.16) is to verify that p is the reduced norm of some element of the order $R[p^{-1}]$ of H. This follows from [41], Cor. 5.9, page 90, since all positive rational numbers are reduced norms of elements of H ([41], Th. 4.1, page 80). □

Lemma 3.17. *Let* $\mathbf{E}_1$ *and* $\mathbf{E}_2$ *be enhanced elliptic curves. There is an isogeny* $\mathbf{E}_1 \to \mathbf{E}_2$ *whose degree is a power of* p.

Proof. Let $R = \mathrm{End}(\mathbf{E}_1)$, and consider the locally free rank-1 right R-module

$$T = \mathrm{Hom}(\mathbf{E}_1, \mathbf{E}_2) .$$

For $x \in I$, $x \neq 0$, the square of the degree of x as a homomorphism is the index $[T: xR]$. Thus the content of the lemma is that T becomes a free R-module once the

prime p is inverted (i.e., after tensoring with $\mathbf{Z}[p^{-1}]$). This statement follows from [41], Th. 5.7, page 89. □

We now prove (3.15). Let $\mathbf{E}$ and $\mathbf{E}'$ be enhanced elliptic curves. It will be enough to show that the image of δ contains the two elements $(\mathbf{E} - \mathbf{E}', 0)$ and $(0, \mathbf{E} - \mathbf{E}')$ of $X \oplus X$. By (3.16) and (3.17), there exists an isogeny $\mathbf{E} \to \mathbf{E}'$ whose degree is an *even* power of p, say p^{2i}. Set $\mathbf{E} = \mathbf{E}_0$, $\mathbf{E}' = \mathbf{E}_{2i}$, and factor $\mathbf{E} \to \mathbf{E}'$ into a product of isogenies of degree p: $\pi_0 : \mathbf{E}_0 \to \mathbf{E}_1, \pi_1 : \mathbf{E}_1 \to \mathbf{E}_2, \ldots, \pi_{2i-1} : \mathbf{E}_{2i-1} \to \mathbf{E}_{2i}$. Let θ_j be the isogeny which is dual to π_j, for each j. Form the element

$$\lambda = \pi_0 - \theta_1 + \pi_2 - \theta_3 + \ldots + \pi_{2i-2} - \theta_{2i-1}$$

of L. One checks immediately that $\delta(\lambda) = (\mathbf{E} - \mathbf{E}', 0)$. By replacing all π's and θ's by their duals, we obtain an analogous element λ' for which $\delta(\lambda') = (0, \mathbf{E} - \mathbf{E}')$. □

Remark 3.18. Another proof of (3.15), based on connectivity properties of graphs, has been suggested by Ron Livné and by Bas Edixhoven (independently).

For all $n \geqq 1$, we now consider the Hecke correspondence T_n on $X_0(Mpq)$. As above, the T_n induce operators on $J_0(Mpq)$ and L. We compare these operators with the operators T_n on X arising from the Hecke correspondences on $X_0(Mq)$. The degeneracy map δ is visibly equivariant with respect to the actions of T_n on L and on $X \oplus X$, provided that $(n, p) = 1$. On the other hand, the Hecke operator T_p of L induces on $X \oplus X$ an operator which must be distinguished from the operator coming from the p^{th} Hecke operator of $X_0(qM)$. Let τ denote this latter operator (and the operator it induces on X), and reserve the symbol T_p for operators coming from the p^{th} Hecke operator of $X_0(pqM)$. Let w_p be the Atkin-Lehner operator of $X_0(pqM)$ relative to the divisor p of pqM. Finally, let Y be the kernel of δ, so that we have the exact sequence

$$0 \to Y \to L \to X \oplus X \to 0 .$$

Theorem 3.19. *The operator T_p of L preserves Y. We have the formula $T_p = -w_p$ on Y. The endomorphism of $X \oplus X$ given by T_p is the map*

$$(x, y) \mapsto (\tau(x) - y, px) .$$

Proof. We first observe the elementary identities

$$\alpha w_p = \beta, \qquad \beta w_p = \alpha$$

involving degeneracy maps. These imply that w_p preserves Y and induces the map $(x, y) \mapsto (y, x)$ on $X \oplus X$. Next, consider the operator $T_p + w_p$. As in the proof of (3.7), we see that $T_p + w_p$ is obtained by composing $\alpha_* : L \to X$ with the map $\beta^* : X \to L$ obtained from $\beta : X_0(pqM) \to X_0(qM)$ via Albanese functoriality of Jacobians. Therefore, $T_p + w_p$ vanishes on Y, a subgroup of the kernel of α_*.

We have, on the other hand, the identities

$$p + 1 = \alpha_* \alpha^* = \beta_* \beta^*$$

$$\tau = \beta_* \alpha^* = \alpha_* \beta^*$$

on X. These imply that $T_p + w_p = \beta^* \alpha_*$ induces $(x, y) \mapsto (\tau x, (p + 1)x)$ on $X \oplus X$. Subtracting w_p, we obtain the desired formula for T_p on $X \oplus X$. □

Consider now the subring $\mathbf{T} = \mathbf{T}_{Mpq}$ of $\mathrm{End}(J_0(Mpq))$ generated by all T_n with $n \geqq 1$. In our discussion of $X_0(Mq)$, we defined the q-old and q-new quotients of $\mathbf{T}_{Mq}$. We define analogously the p-old, p-new, q-old, and q-new quotients of $\mathbf{T}$. In addition, we define the pq-new quotient $\bar{\mathbf{T}}$ of $\mathbf{T}$ as follows. The space

$$S = S_2(\Gamma_0(Mpq))$$

contains two subspaces isomorphic respectively to

$$S_2(\Gamma_0(Mq)) \oplus S_2(\Gamma_0(Mq)), \qquad S_2(\Gamma_0(Mp)) \oplus S_2(\Gamma_0(Mp)) .$$

Let $S_{pq\text{-old}}$ be the sum of these two subspaces (the sum is not necessarily direct), and let $S_{pq\text{-new}}$ be the orthogonal complement to $S_{pq\text{-old}}$ in S, with respect to the Petersson inner product. The spaces $S_{pq\text{-old}}$ and $S_{pq\text{-new}}$ are $\mathbf{T}$-stable. We let $\bar{\mathbf{T}}$ be the quotient of $\mathbf{T}$ cut out by $S_{pq\text{-new}}$, i.e., the image of $\mathbf{T}$ in $\mathrm{End}(S_{pq\text{-new}})$.

Theorem 3.20. *The* $\mathbf{T}$*-module* Y *cuts out the* pq-new *quotient* $\bar{\mathbf{T}}$ *of* $\mathbf{T}$*: an element* t *of* $\mathbf{T}$ *is* 0 *in* $\bar{\mathbf{T}}$ *if and only if it acts on* Y *as* 0.

Proof. Fix $t \in \mathbf{T}$. As in the proof of (3.10), t is 0 in $\bar{\mathbf{T}}$ if and only if t acts as 0 on the "pq-new" quotient R of $J_0(Mpq)$ which is obtained by dividing $J_0(Mpq)$ by the image of the natural degeneracy map

$$J_0(Mq) \times J_0(Mq) \times J_0(Mp) \times J_0(Mp) \to J_0(Mpq) .$$

This quotient has purely toric reduction in characteristic q, since it is a quotient of the q-new quotient Q of $J_0(Mpq)$, which already has purely toric reduction (cf. (3.10) and its proof). Let V be the torus $(R_{\mathbf{F}_q})^0$, i.e., the connected component of the fiber at q of the Néron model of R. The analogous torus for $J_0(Mpq)$ is (by definition) $\mathrm{Hom}(L, \mathbf{G}_m)$, while the analogous torus for $J_0(Mq)$ is $\mathrm{Hom}(X, \mathbf{G}_m)$.

The quotient map $\pi: J_0(Mpq) \to R$ induces a map $\mathrm{Hom}(L, \mathbf{G}_m) \to V$; this latter map is trivial on $\mathrm{Hom}(X, \mathbf{G}_m) \times \mathrm{Hom}(X, \mathbf{G}_m)$ because π is trivial on (the image in $J_0(Mpq)$ of) $J_0(Mq) \times J_0(Mq)$. Hence π induces a map $\lambda: \mathrm{Hom}(Y, \mathbf{G}_m) \to V$. It is an easy task to check that the source and target of λ are tori of the same dimension. Indeed, we have

$$\begin{aligned} \dim(L) &= \dim J_0(Mpq) - 2\dim J_0(Mp) \\ &= \dim(S) - 2\dim S_2(\Gamma_0(Mp)) , \\ \dim(X) &= \dim S_2(\Gamma_0(Mq)) - 2\dim S_2(\Gamma_0(M)) , \end{aligned}$$

so that

$$\begin{aligned} \dim(Y) = \dim(S) &- 2\dim S_2(\Gamma_0(Mp)) \\ &- 2\dim S_2(\Gamma_0(Mq)) + 4\dim S_2(\Gamma_0(M)) . \end{aligned}$$

Also, $\dim(V) = \dim(R) = \dim(S_{pq\text{-new}})$, and the latter number agrees with the dimension of Y because the intersection of $S_2(\Gamma_0(Mp)) \oplus S_2(\Gamma_0(Mp))$ and $S_2(\Gamma_0(Mq)) \oplus S_2(\Gamma_0(Mq))$ in S is the direct sum of four copies of $S_2(\Gamma_0(M))$. By using the same idea as in the proof of (3.10), we find a map $\eta: V \to \mathrm{Hom}(Y, \mathbf{G}_m)$ such that $\lambda\eta$ is an isogeny $V \to V$. It follows that λ is an isogeny of tori. Hence t acts as 0 on Y if and only if t acts as 0 on V; since R has purely toric reduction, the latter condition means that t acts as 0 on R, and the theorem is proved. □

In yet another variant, we define the q-new/p-old quotient of $\mathbf{T}$ to be that quotient $\mathbf{T}_{q\text{-new}/p\text{-old}}$ cut out by the intersection $S_{q\text{-new}/p\text{-old}}$ in $S = S_2(\Gamma_0(Mpq))$ of $S_{q\text{-new}}$ and $S_{p\text{-old}}$.

Theorem 3.21. *The Hecke algebra* $\mathbf{T}$ *acts on* $X \oplus X$ *through its quotient* $\mathbf{T}_{q\text{-new}/p\text{-old}}$, *which acts faithfully on* $X \oplus X$.

Proof. The group $X \oplus X$ is naturally isogenous to the character group of the torus arising from the mod q reduction of the q-new quotient of $J_0(Mq) \times J_0(Mq)$, cf. (3.10) and its proof. On the other hand, $J_0(Mq) \times J_0(Mq)$ is isogenous to the p-old subvariety of $J_0(Mpq)$. Therefore, the q-new quotient of $J_0(Mq) \times J_0(Mq)$ is isogenous to the q-new quotient of the p-old subvariety of $J_0(Mpq)$. The tangent space to the dual of this subquotient is isomorphic to $S_{q\text{-new}/p\text{-old}}$. □

In our discussions of $J_0(Mq)_{\mathbf{F}_q}$ we considered the component group Φ attached to this reduction. Let Θ denote the analogous group for $J_0(Mpq)_{\mathbf{F}_q}$. The degeneracy map

$$J_0(Mq) \times J_0(Mq) \to J_0(Mpq)$$

induces a map of finite groups

$$\theta: \Phi \times \Phi \to \Theta .$$

Let K and C be the kernel and cokernel of θ, so that we have an exact sequence

$$0 \to K \to \Phi \times \Phi \to \Theta \to C \to 0 . \tag{8}$$

Theorem 3.22. *The group* K *contains the image of* Φ *in* $\Phi \times \Phi$ *under the antidiagonal embedding* $f \mapsto (f, -f)$.

The proof of (3.22) is a variant of our demonstration of (3.12). It is presented in [30]. We wish to point out here that (3.22) may be viewed as a refinement of Theorem 3.12. Namely, the endomorphism μ of $\Phi \times \Phi$ gotten by composing the map $\Phi \times \Phi \to \Theta$ of (8) with the map $\Theta \to \Phi \times \Phi$ coming from Albanese functoriality of Jacobians is given by the formula

$$\mu: (x, y) \mapsto ((p+1)x + \tau y, \tau x + (p+1)\, y) ,$$

where τ is the p^{th} Hecke operator of $J_0(Mq)$. Therefore, (3.22) implies that Φ is annihilated by $\tau - (p+1)$, i.e., by the operator η_p in the statement of (3.12). Since p is an arbitrary prime which is prime to qM, we get (3.12).

Recall now that we have $\Phi = X^*/X$, $\Theta = L^*/L$, where X^* and L^* are the linear duals of X and L, and where X and L are embedded in these duals via the pairing ι discussed above (e.g., in the proof of (3.12)) and its analogue for L. The map $\theta: \Phi \times \Phi \to \Theta$ is induced by the dual of the degeneracy map $\delta: L \to (X \oplus X)$ and the map

$$\sigma: (X \oplus X) \to L$$

which arises from the two degeneracy maps $X_0(pqM) \rightrightarrows X_0(qM)$ and Albanese functoriality of the Jacobian. It follows from the definition of the p^{th} Hecke correspondence τ on $X_0(qM)$ that the composite $\delta\sigma$ is the endomorphism of

$X \oplus X$ given by the 2×2 matrix $\mu = \begin{pmatrix} p+1 & \tau \\ \tau & p+1 \end{pmatrix}$. Let Y^* be the linear dual of Y. Restrict to Y the pairing on L to obtain an embedding $Y \to Y^*$.

Proposition 3.23. *There is a natural exact sequence*

$$0 \to K \to (X \oplus X)/\mu(X \oplus X) \to Y^*/Y \to C \to 0\,,$$

Proof. Consider the commutative diagram of exact sequences

$$\begin{array}{ccccccc} 0 \to & L/Y & \to & L^*/Y & \to & \Theta & \to 0 \\ & {\scriptstyle\sigma}\uparrow & & {\scriptstyle\delta^*}\uparrow & & {\scriptstyle\theta}\uparrow & \\ 0 \to & X \oplus X & \to & X^* \oplus X^* & \to & \Phi \times \Phi & \to 0\,. \end{array}$$

The cokernel of the middle vertical map is Y^*/Y, since $L^*/(X^* \oplus X^*)$ is Y^*. This group is finite, since the pairing on Y satisfies $y \cdot y > 0$ for $y \neq 0$. Since L^*/Y and $X^* \oplus X^*$ have the same rank, δ^* is injective. Also, the cokernel of the first vertical map σ becomes $(X \oplus X)/\mu(X \oplus X)$, after δ is used to identify L/Y with $X \oplus X$, so that σ is identified with μ. An application of the snake lemma to the commutative diagram now gives the desired 4-term exact sequence. □

Remark 3.24. The exact sequence of (3.23) is "Hecke compatible" provided that one takes the appropriate action of each Hecke operator T_n on the groups above. Care must be taken with two points. The first, already discussed on several occasions, is that the p^{th} Hecke operator used on $J_0(qM)^2$ is not induced by the usual p^{th} Hecke operator τ of $J_0(qM)$, cf. (3.19). The second point is that both the Picard and Albanese actions of T_n on L and X intervene in the actions of T_n on the component groups Θ and Φ. Namely, in the case of $J_0(pqM)$, say, the correspondence T_n of $X_0(pqM)$ induces endomorphisms T_n and ξ_n of $J_0(pqM)$, by Picard and Albanese functoriality, respectively. These induce endomorphisms of L, the character group of the maximal torus in the mod q reduction of $J_0(pqM)$. For simplicity, call these endomorphisms T_n and ξ_n. They lead to two $\mathbf{T}$-module structures on L. In the usual (Picard) structure, $T_n \in \mathbf{T}$ operates on L as $T_n \in \mathrm{End}(L)$. In the Albanese structure, T_n operates on L as $\xi_n \in \mathrm{End}(L)$. These two $\mathbf{T}$-module structures on L in fact give *isomorphic* $\mathbf{T}$-modules, since the Atkin-Lehner involution $w = w_{pqM}$ of $J_0(pqM)$ induces an automorphism of the abelian group L which is an intertwining operator for the two structures.

As discussed above, the endomorphism of $\Theta = L^*/L$ induced by T_n is obtained by combining the endomorphism $(T_n)^* = \mathrm{Hom}(T_n, \mathrm{id})$. on $L^* = \mathrm{Hom}(L, \mathbf{Z})$ with the endomorphism ξ_n of L. Similar remarks apply for Φ. It follows that the exact sequence of (3.23), as constructed by the snake lemma, is an exact sequence of $\mathbf{T}$-modules, provided that $\mathbf{T}$ acts in the evident (Picard) manner on all groups other than $(X \oplus X)/\mu(X \oplus X)$, and in the Albanese fashion on $(X \oplus X)/\mu(X \oplus X)$.

On the other hand, the Picard and Albanese $\mathbf{T}$-module structures on $(X \oplus X)/\mu(X \oplus X)$ lead to isomorphic $\mathbf{T}$-modules; the intertwining operator is again that involution of $(X \oplus X)/\mu(X \oplus X)$ which corresponds to w_{pqM}. This involution is induced by the composition of the Atkin-Lehner operator $w_{qM} \in \mathrm{Aut}(X)$ (acting diagonally on $X \oplus X$) and the map $(x, y) \mapsto (y, x)$ of $X \oplus X$.

The composition commutes with μ, since w_{qM} commutes with the p^{th} Hecke operator τ on X. Therefore, (3.23) is correct as stated, even when $(X \oplus X)/\mu(X \oplus X)$ is given its (more usual) Picard **T**-module structure. In what follows, the Picard structure will be systematically chosen.

Proposition 3.25. *Let* $\gamma = (T_p)^2 - 1 \in \mathbf{T}$. *Then* $\mu(X \oplus X) = \gamma(X \oplus X)$.

Proof. Consider the automorphism λ of $X \oplus X$ given by

$$(x, y) \mapsto (-x, \tau x - y).$$

A computation shows that we have $\gamma = \mu\lambda$. □

4. Bad reduction of Shimura curves

This § exploits a result of Cerednik-Drinfeld ([3] and [7], §4) concerning the mod p reduction of certain Shimura curves. Their result is a well known tool in the arithmetical study of these curves (see, e.g., [13, 14, 16]). We deduce from it some geometrical relations between Shimura curves and the curves $X_0(Mq)$ and $X_0(Mpq)$ which were studied in §3. These relations may be viewed as geometrical realizations of the Jacquet-Langlands correspondence between quaternion algebras and $\mathbf{GL}_2$. In the presentation given here, our relations are deduced from bijections that are not entirely canonical. Indeed, they arise from fixed isomorphisms between orders in quaternion algebras which "happen to be isomorphic." They are not uniquely isomorphic because these orders have non-trivial normalizers. A detailed exploration of the questions posed by the non-uniqueness, from a more modular point of view, is given in [29].

A forthcoming work of Jordan and Livné will deal with generalizations of the method presented here.

Let p and q again be distinct primes, and let M be an integer prime to pq. Let B be an indefinite quaternion division algebra over $\mathbf{Q}$ of discriminant pq. (Up to isomorphism, B is unique.) Let $\mathcal{O}$ be an Eichler order of level M (i.e., reduced discriminant Mpq) in B. Let Γ_∞ be the group of elements of $\mathcal{O}$ with (reduced) norm 1. After fixing an embedding $B \to \mathrm{M}(2, \mathbf{R})$, we obtain in particular an embedding $\Gamma_\infty \to \mathbf{SL}(2, \mathbf{R})$ and therefore an action of Γ_∞ on the Poincaré upper half-plane H. Let C be the standard canonical model, over $\mathbf{Q}$, of the compact Riemann surface $\Gamma_\infty \backslash H$, and let J be the Jacobian $\mathrm{Pic}^0(C)$. The curve C is furnished with Hecke correspondences T_n for $n \geqq 1$. In analogy with the situation in §2, we write again T_n for the endomorphism of J induced by T_n via Pic functoriality and write ξ_n for the endomorphism of J induced by T_n using Albanese functoriality.

For simplicity, write simply C for the curve $C_{\mathbf{Q}_p}$ and J for $J_{\mathbf{Q}_p}$. A model $\mathscr{C}$ for C over $\mathbf{Z}_p$ of the type we considered in §2 was constructed by Cerednik in [3]; in [7], Drinfeld gave a moduli-theoretic interpretation of Cerednik's construction. It follows, in particular, from their work that J has purely toric reduction at p. Let Z be the character group of the torus $(J_{\mathbf{F}_p})^0$ and let $\Psi = Z^*/Z$ be the group of components of $(R_{\mathbf{F}_p})$. (There is a natural bilinear pairing on Z, as discussed in §2, which embeds Z in Z^*.)

Let $\tilde{\mathbf{T}}$ be the formal polynomial ring $\mathbf{Z}[\ldots T_n \ldots]$ generated by commuting indeterminates T_n. There are two actions of $\tilde{\mathbf{T}}$ on J: the "standard action," in which $T_n \in \tilde{\mathbf{T}}$ acts as T_n on J, and the Albanese action, in which T_n acts as ξ_n. We shall encounter both actions of $\tilde{\mathbf{T}}$ on Z, but only the standard action of $\tilde{\mathbf{T}}$ on Ψ. (In the relation $\Psi = Z^*/Z$, the standard action of $\tilde{\mathbf{T}}$ on Ψ arises from the standard action of $\tilde{\mathbf{T}}$ on $Z^* = \mathrm{Hom}(Z, \mathbf{Z})$, together with the Albanese action of $\tilde{\mathbf{T}}$ on the submodule Z of Z^*.)

The object of this § is to relate Z and Ψ to the $\mathbf{T}$-modules L, $X \oplus X$, Y, Φ, ... of §3. (Since the Hecke operators T_n on $J_0(Mpq)$ make $\mathbf{T}$ a quotient of $\tilde{\mathbf{T}}$, every $\mathbf{T}$-module is naturally a $\tilde{\mathbf{T}}$-module.) Here is the main result:

Theorem 4.1. *There is a $\tilde{\mathbf{T}}$-isomorphism $Z \approx Y$ under which the bilinear pairing on Z corresponds to the restriction to Y of the natural pairing on L.*

In the statement of this theorem, we understand the actions of $\tilde{\mathbf{T}}$ on Z and on Y to be the standard (Pic) actions. As a corollary, we may deduce that Z and Y, with the Albanese actions of $\tilde{\mathbf{T}}$, are again isomorphic. This follows from the fact that T_n and ξ_n are adjoint operators on L (resp. Z) under the pairing $L \times L \to \mathbf{Z}$ of §3 (resp. the natural pairing $Z \times Z \to \mathbf{Z}$).

Recall that $\bar{\mathbf{T}}$ is the quotient of $\mathbf{T}$ cut out by the space $S_{pq\text{-new}}$ of forms on $\Gamma_0(pqM)$ which are new relative to p and to q. It is also the quotient of $\mathbf{T}$ cut out by Y (3.20). (For the purpose of orientation, we recall that the module Y was introduced just before the statement of (3.19).) Also, since J has purely toric reduction, $\mathrm{End}_{\mathbf{Q}}(J)$ operates faithfully on Z. Therefore, (4.1) implies:

Corollary 4.2. *There is a unique injection $\bar{\mathbf{T}} \to \mathrm{End}(J)$ mapping the n^{th} Hecke operator in $\bar{\mathbf{T}}$ to the n^{th} Hecke operator on J.*

One can certainly recover classical trace identities from (4.2) by interpreting in two different ways the numbers $\mathrm{trace}_{\bar{\mathbf{T}}/\mathbf{Z}}(T_n)$.

Take again $\gamma = (T_p)^2 - 1 \in \mathbf{T}$. The following variant of the main theorem of [14] results immediately from (3.23), (3.25) and (4.1).

Theorem 4.3 *There is an exact sequence of $\mathbf{T}$-modules*

$$0 \to K \to (X \oplus X)/\gamma(X \oplus X) \to \Psi \to C \to 0\,,$$

in which K and C are the groups appearing in (8).

[The description of Ψ as a $\mathbf{T}$-module is legitimate because (4.2) guarantees that $\tilde{\mathbf{T}}$ operates on Y through its quotient $\bar{\mathbf{T}}$ (which is a quotient of $\mathbf{T}$).]

As a first step toward proving (4.1), we summarize the theorem of Cerednik-Drinfeld [7], §4 (cf. [13]). This result furnishes as model for C over $\mathbf{Z}_p$ the scheme $\mathscr{C}$ for which the associated formal scheme over $\mathbf{Z}_p$ is the quotient

$$\mathbf{GL}(2, \mathbf{Q}_p)\backslash(\wp^{\mathrm{unr}} \times X)\,.$$

Here $\wp^{\mathrm{unr}}$ is a generalized "p-adic upper half plane" ([13], §4) and X is the p-adic space $K\backslash H_f^*/H^*$, where H is a quaternion algebra of discriminant q over $\mathbf{Q}$ and K is the product of the multiplicative groups of the completions away from p of a

certain Eichler order $R \subset H$ of level M (i.e., discriminant Mq). Thus K is the group of "prime-to-p ideles" of H arising from R.

(Apologies are owed to the reader for certain symbols which are used for two purposes. There optimally will be no confusion between the p-adic space X just introduced and the character group X which has frequently appeared above. Similarly, the adelic group K introduced here bears no relation to the finite group K in (8). Finally, the finite group C in (8) is to be distinguished from the Shimura curve C whose mod p reduction we are in the process of studying.)

In the Cerednik-Drinfeld theorem, the ring R is analogous to the Eichler orders $\mathrm{End}(\mathbf{E})$ of §3. It is obtained by fixing, over $\bar{\mathbf{F}}_p$, a 2-dimensional abelian variety A together with an embedding $L \subset \mathrm{End}(A)$, where L is a maximal order in the quaternion algebra B. The abelian variety A is "enhanced" by an L-stable subgroup D of $A[M]$ which is of order M^2 and is cyclic over L. It is further embellished by an $L \otimes \mathbf{Z}_p$-isomorphism ι between the formal group of A and a certain "standard" formal module Φ. The ring R is the commutant of L in $\mathrm{End}(\mathbf{A})$, where $\mathbf{A} = (A, D)$; i.e., we have

$$R = \mathrm{End}_L(\mathbf{A}) .$$

The ring R is an Eichler order of level M in $H = R \otimes \mathbf{Q}$, given explicitly as the intersection of the two maximal orders $\mathrm{End}_L(A)$ and $\mathrm{End}_L(A/D)$ of H.

The isomorphism ι furnishes R with an isomorphism

$$R \otimes \mathbf{Z}_p \approx \mathrm{M}(2, \mathbf{Z}_p) ,$$

so that we have an induced isomorphism $H \otimes \mathbf{Q}_p \approx \mathrm{M}(2, \mathbf{Q}_p)$.

The space X is the space of isomorphism classes of abelian varieties A' over $\bar{\mathbf{F}}_p$ which are given with the following data: an action of L, an "enhancement" $D' \subset A'[M]$, and an isomorphism between Φ and the formal group of A'. Given A', we choose an isogeny $A' \to A$ which is compatible with the actions of L, and use it to regard the adelic Tate module $T(A')$ as a submodule of $V(A) = T(A) \otimes \mathbf{Q}$. We have

$$T(A') = g^{-1} T(A)$$

for some $g \in (H_{\mathrm{f}})^*$, whose image in X classifies A' with its accompanying data.

Let $\mathbf{GL}(2, \mathbf{Q}_p)^+$ be the kernel of the map

$$v : \mathbf{GL}(2, \mathbf{Q}_p) \to \mathbf{Z}/2\mathbf{Z}$$

defined by the formula

$$v(\gamma) = \mathrm{ord}_p(\det \gamma) \pmod 2 .$$

By the method of [13], §4 (see especially Theorem 4.4), we may write the dual graph $\mathscr{G}$ attached to the special fiber of $\mathscr{C}$ as the quotient

$$\mathbf{GL}(2, \mathbf{Q}_p)^+ \backslash (\Delta \times X) ,$$

where Δ is the well-known tree attached to $\mathbf{SL}(2)$ ([33], Ch II, §1). This graph has been described explicitly by Kurihara [16] when $M = 1$. We now study the general case, which is not qualitatively different.

Let $S \subset R$ be the Eicher order of level Mp in H gotten by intersecting R with the evident Eichler order in $\mathrm{M}(2, \mathbf{Z}_p)$

$$\left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{M}(2, \mathbf{Z}) \,\middle|\, p \text{ divides } c \right\}.$$

Let $\mathscr{V}$ be the set of isomorphism classes of locally free rank-1 left R-modules, and let $\mathscr{E}$ be the set of isomorphism classes of locally free rank-1 left S-modules. We have canonically

$$\mathscr{V} = R_{\mathbf{f}}^* \backslash H_{\mathbf{f}}^* / H^* \qquad \mathscr{E} = S_{\mathbf{f}}^* \backslash H_{\mathbf{f}}^* / H^* .$$

The inclusion of S into R defines a degeneracy map

$$\alpha : \mathscr{E} \to \mathscr{V} .$$

A second degeneracy map

$$\beta : \mathscr{E} \to \mathscr{V}$$

is obtained by considering the Eichler order T of H which has level M, contains S, agrees with R locally at all places except for p, and is distinct from R. The order T is given adelically as mRm^{-1}, where m is trivial except at p, where it is the diagonal matrix $\mathrm{diag}(1, p)$. The analogue of α for T is a map from $\mathscr{E}$ to the double coset space

$$(mR_{\mathbf{f}}^* m^{-1}) \backslash H_{\mathbf{f}}^* / H^* .$$

We get β by identifying this space with $\mathscr{V}$ via multiplication by m^{-1} on $(H_f)^*$. Hence β maps the class of x in the double-coset space defining $\mathscr{V}$ to the class of $m^{-1}x$ in the double-coset space defining $\mathscr{V}$.

Proposition 4.4. *The set of edges of $\mathscr{G}$ is canonically the set $\mathscr{E}$. The set of vertices of $\mathscr{G}$ is the disjoint union $\mathscr{V} \times \{1, 2\}$ of two copies of $\mathscr{V}$. A given edge $e \in \mathscr{E}$ connects the vertex $(\alpha(e), 1)$ with the vertex $(\beta(e), 2)$.*

Proof. The quotient $\mathbf{GL}(2, \mathbf{Q}_p)^+ \backslash X$ is trivial because of strong approximation ((3.16) and its proof). It follows that the set of vertices of $\mathscr{G}$ is the quotient $\mathbf{GL}(2, \mathbf{Q}_p)^+ \backslash (\mathscr{V}_\Delta \times X)$, where $\mathscr{V}_\Delta$ is the set of vertices of Δ. We have

$$\mathscr{V}_\Delta = \mathbf{PGL}(2, \mathbf{Q}_p)/\mathbf{PGL}(2, \mathbf{Z}_p) = H_p^*/R_p^* \mathbf{Q}^* .$$

There are two orbits of $\mathscr{V}_\Delta$ under the action of $\mathbf{GL}(2, \mathbf{Q}_p)^+$. Consider first

$$\mathscr{V}_{\Delta +} = \mathbf{PGL}(2, \mathbf{Q}_p)^+ / \mathbf{PGL}(2, \mathbf{Z}_p) .$$

The set $\mathbf{GL}(2, \mathbf{Q}_p)^+ \backslash (\mathscr{V}_{\Delta +} \times X)$ is then a quotient of X; moreover $(1, x)$ and $(1, y)$ have the same image in $\mathbf{GL}(2, \mathbf{Q}_p)^+ \backslash (\mathscr{V}_{\Delta +} \times X)$ if and only if x and y have the same image in

$$\mathbf{GL}(2, \mathbf{Z}_p) \backslash X = \mathscr{V} .$$

Secondly, let $\mathscr{V}_{\Delta -}$ be the complement of $\mathscr{V}_{\Delta +}$ in $\mathscr{V}_\Delta$ and consider

$$\mathbf{GL}(2, \mathbf{Q}_p)^+ \backslash (\mathscr{V}_{\Delta +} \times X) .$$

Fix a matrix $m \in \mathbf{GL}(2, \mathbf{Q}_p)$ which is not in $\mathbf{GL}(2, \mathbf{Q}_p)^+$, for instance the diagonal

matrix diag(1, p) considered above. The map $x \mapsto (m, mx)$ induces a bijection

$$\mathscr{V} = \mathbf{GL}(2, \mathbf{Z}_p)\backslash X \to \mathbf{GL}(2, \mathbf{Q}_p)^+ \backslash (\mathscr{V}_{\Delta^-} \times X) .$$

Hence the set of vertices of $\mathscr{G}$ is naturally a disjoint union of two copies of $\mathscr{V}$.

For the edges of $\mathscr{G}$, we consider the quotient $\mathbf{GL}(2, \mathbf{Q}_p)^+ \backslash (\mathscr{E}_\Delta \times X)$, where $\mathscr{E}_\Delta$ is the set of edges of Δ. The set $\mathscr{E}_\Delta$ is the quotient $\mathbf{GL}(2, \mathbf{Q}_p)^+ / (S_p^* \mathbf{Q}^*)$; the group S_p^* is the multiplicative group of the Eichler order in $\mathrm{M}(2, \mathbf{Z}_p)$ which was defined above. The map $X \to \mathscr{E}_\Delta \times X$ sending x to $(1, x)$ identifies $\mathbf{GL}(2, \mathbf{Q}_p)^+ \backslash (\mathscr{E}_\Delta \times X)$ with the quotient $S_p^* \backslash X$, which is the double coset space defining $\mathscr{E}$.

Now take $x \in \mathbf{GL}(2, \mathbf{Q}_p)^+$. The element of $\mathscr{E}_\Delta$ defined by x is the edge of Δ which joins the vertices in $\mathscr{V}_\Delta$ represented by the matrices x and xm in $\mathbf{GL}(2, \mathbf{Q}_p)$. The edge of $\mathscr{G}$ so defined by x may be written as the class of $(1, x^{-1})$ in $\mathbf{GL}(2, \mathbf{Q}_p)^+ \backslash (\mathscr{E}_\Delta \times X)$. Accordingly, it maps to the class of x^{-1} in the double-coset space which defines $\mathscr{E}$. The two vertices $(x, 1)$ and $(xm, 1)$ joined by this edge may be rewritten $(1, x^{-1})$ and (m, x^{-1}), respectively. The first arises from the class of x^{-1} in the first copy of $\mathscr{V}$. The second arises from the class of $m^{-1}x^{-1}$ in the second copy of $\mathscr{V}$. These two elements of $\mathscr{V}$ are indeed obtained from the class of x^{-1} in $\mathscr{E}$ via the two degeneracy maps $\mathscr{E} \to \mathscr{V}$. □

It follows from (4.4) that the character group Z, *a priori* the group $H_1(\mathscr{G}, \mathbf{Z})$, is the kernel of the map $\omega: \mathbf{Z}^{\mathscr{E}} \to \mathbf{Z}^{\mathscr{V}} \times \mathbf{Z}^{\mathscr{V}}$ induced by (α, β): $\mathscr{E} \to \mathscr{V} \times \mathscr{V}$. An element of $\ker(\omega)$ visibly has degree 0 as a formal linear combination of elements of $\mathscr{E}$. Writing $(\mathbf{Z}^{\mathscr{E}})_0$ and $(\mathbf{Z}^{\mathscr{V}})_0$ for the group of degree-0 divisors on $\mathscr{E}$ and $\mathscr{V}$, we get:

Corollary 4.5. *The character group Z is the kernel of the degeneracy map*

$$(\mathbf{Z}^{\mathscr{E}})_0 \to (\mathbf{Z}^{\mathscr{V}})_0 \times (\mathbf{Z}^{\mathscr{V}})_0$$

induced by (α, β).

The bilinear pairing on Z coming from the geometry of the Cerednik-Drinfeld model $\mathscr{C}$ is the restriction to Z of the diagonal pairing on $\mathbf{Z}^{\mathscr{E}}$ whose value $o(e)$ on an edge $e \in \mathbf{GL}(2, \mathbf{Q}_p)^+ \backslash (\mathscr{E}_\Delta \times X)$ is computed as follows (cf. [13], §4). Take a representative $\tilde{e}$ of e in $\mathscr{E}_\Delta \times X$, and let $\Gamma \subset \mathbf{GL}(2, \mathbf{Q}_p)^+$ be the stabilizer in $\mathbf{GL}(2, \mathbf{Q}_p)^+$ of $\tilde{e}$. Then $o(e)$ is the order of the image of Γ in $\mathbf{PGL}(2, \mathbf{Q}_p)$.

Let W be a locally free rank-1 left S-module whose class in

$$\mathscr{E} = S_{\mathbf{f}}^* \backslash H_{\mathbf{f}}^* / H^*$$

is the edge e.

Proposition 4.6. *We have* $o(e) = \frac{1}{2}\mathrm{card}(\mathrm{Aut}_S(W))$.

Proof. Choose $x = (x_v) \in H_{\mathbf{f}}^*$ so that the class of x in $\mathscr{E}$ is e. Take W to be the S-submodule of H whose completions at the finite places v of $\mathbf{Q}$ are the modules $S_v \cdot x_v$. Then $\mathrm{Aut}_S(W)$ is the stabilizer in H^* of the class of x in $S_{\mathbf{f}}^* \backslash H_{\mathbf{f}}^*$. If $a \in H^*$ stabilizes x in $S_{\mathbf{f}}^* \backslash H_{\mathbf{f}}^*$, then we have $sx = xa$ for some $s \in S_{\mathbf{f}}^*$. Since s and a determine each other in this equation, $\mathrm{Aut}_S(W)$ is the stabilizer in $S_{\mathbf{f}}^*$ of x in $H_{\mathbf{f}}^* / H^*$.

On the other hand, the stabilizer Γ of $\tilde{e} = (1, x)$ in $\mathbf{GL}(2, \mathbf{Q}_p)^+$ is the stabilizer of $x \in X$ under the action of S_p^* on X. Also, projection onto the component at p identifies the stabilizer in $S_{\mathbf{f}}^*$ of x in $H_{\mathbf{f}}^* / H^*$ with the stabilizer in S_p^* of x in

$X = K\backslash H_f^*/H^*$. Indeed, take $s_p \in S_p^*$ and examine the equation

$$s_p x = \kappa x a$$

with $\kappa \in K$ and $a \in H^*$. We see that a is determined by s_p and x (through its component at p), and that κ is determined by s_p, x and a. Hence this equation holds for at most one κ (and at most one a), given s_p and x.

Therefore, Γ is the group $\mathrm{Aut}_S(W)$. To prove the proposition, it remains to verify that $\Gamma \cap \mathbf{Q}_p^*$ is the group $\{\pm 1\}$. For this, suppose that we have $s_p x = \kappa x a$ with $s_p \in \mathbf{Z}_p^*$. Then a is a rational number which agrees with s_p at p. Also, the prime-to-p part of a coincides with κ^{-1}. Therefore a is a unit locally at each finite place of $\mathbf{Q}$, so that $a = \pm 1$. Hence $s_p = \pm 1$. □

We now begin our comparison of the groups Z and Y. The latter group is defined to be the kernel of a natural degeneracy map $\delta: L \to X \oplus X$, where L and X are the groups of degree-0 divisors on the sets $\Sigma(Mp)$ and $\Sigma(M)$ of supersingular points of $X_0(Mp)$ and $X_0(M)$ in characteristic q. The former has an analogous description (4.5) with $\Sigma(Mp)$ replaced by $\mathscr{E}$ and $\Sigma(M)$ by $\mathscr{V}$. Taking first $M = Mp$ and then $M = M$ in Proposition (3.3), we find that $\Sigma(Mp)$ and $\Sigma(M)$ are double-coset spaces of the type defining $\mathscr{E}$ and $\mathscr{V}$, but with the orders S and R replaced by orders of the form $\mathrm{End}(\mathbf{E}_0, C_p)$ and $\mathrm{End}(\mathbf{E}_0)$. Here, $\mathbf{E}_0$ is (as usual) a supersingular elliptic curve E_0 in characteristic q which has been enhanced by a cyclic subgroup of order M, while C_p is a cyclic subgroup of E_0 having order p. To compare the pairs $(\mathscr{E}, \mathscr{V})$ and $(\Sigma(Mp), \Sigma(M))$, we will find $\mathbf{E}_0$, C_p such that $\mathrm{End}(\mathbf{E}_0, C_p) = S$ and $\mathrm{End}(\mathbf{E}_0) = R$.

The existence of the pair $(\mathbf{E}_0, C_p)$ is given by the following proposition, which is based on (3.6) and its proof. Before stating it, we introduce the symbol $\mathscr{M}$ to denote the maximal order $\mathrm{End}_L(A)$ of H. Thus R and S are Eichler orders of $\mathscr{M}$, of levels M and pM, respectively.

Proposition 4.7. *There is an enhanced supersingular elliptic curve* $\mathbf{E}_0 = (E_0, C_M)$, *a cyclic subgroup* C_p *of* E_0, *and an isomorphism* $\kappa: \mathrm{End}(E_0) \to \mathscr{M}$ *such that* R *corresponds to* $\mathrm{End}(\mathbf{E}_0)$ *and* S *to* $\mathrm{End}(\mathbf{E}_0, C_p)$ *under* κ.

Proof. Let $\mathbf{E}_0 = (E_0, C_M)$ and κ be the "output" of (3.6), applied with B taken to be $\mathscr{M}$ and B' taken to be $\mathrm{End}_L(A/D)$, so that the intersection $B \cap B'$, denoted S in (3.6), is R in our context. To construct C_p, we examine S and R locally at p, using κ to identify $S \otimes \mathbf{Z}_p$ and $R \otimes \mathbf{Z}_p$ with subrings of

$$\mathrm{End}(E_0) \otimes \mathbf{Q}_p = \mathrm{End}(V_p),$$

where V_p is the $\mathbf{Q}_p$-adic Tate module of E_0. Since R and $\mathscr{M}$ agree locally at p, $R \otimes \mathbf{Z}_p$ is identified with $\mathrm{End}(T_p)$, where T_p is the $\mathbf{Z}_p$-adic Tate module of E_0. The ring $S \otimes \mathbf{Z}_p$ is then an Eichler order of level p^{+1} (or "level 1," in this local context) in the maximal order $\mathrm{End}(T_p)$ of $\mathrm{End}(V_p)$. We have $S \otimes \mathbf{Z}_p = \mathrm{End}(T_p) \cap \mathrm{End}(U)$ for some lattice U in V_p, which is unique up to homothety. Scale U so that it is contained in T_p, but not in pT_p. The group T_p/U is then of order p, as is the image C_p of U in $E[p] = T_p/pT_p$. An endomorphism of T_p preserves C_p in T_p/pT_p if and only if it preserves U. Hence C_p has the property that

$$S \otimes \mathbf{Z}_p = \mathrm{End}(\mathbf{E}_0, C_p) \otimes \mathbf{Z}_p .$$

It follows that $S = \mathrm{End}(\mathbf{E}_0, C_p)$, since these orders agree respectively with R and with $\mathrm{End}(\mathbf{E}_0)$, and therefore with each other, outside p.

We next construct bijections

$$\iota : \Sigma(Mp) \to \mathscr{E}, \qquad \lambda : \Sigma(M) \to \mathscr{V},$$

using the enhanced elliptic curve $\mathbf{E}_0$ and its subgroup C_p which are given by (4.7). We consider that $S = \mathrm{End}(\mathbf{E}_0, C_p)$ and $R = \mathrm{End}(\mathbf{E}_0)$, as in the latter part of the above proof; i.e., we suppress the isomorphism κ. To define ι, we suppose given a supersingular elliptic curve E over $\bar{\mathbf{F}}_q$, together with a cyclic subgroup of order Mp in E. We consider, as in §3, the adelic Tate module $T(E)$ of E, and note that the cyclic subgroup of E defines a sublattice $T'(E)$ of $T(E)$ which contains $pM \cdot T(E)$ and is such that $T'(E)/pM \cdot T(E)$ is cyclic of order pM. We have an analogous sublattice $T'(E_0)$ of $T(E_0)$, coming from the enhancement of E_0 and from the group C_p. After fixing a non-zero homomorphism $E \to E_0$, we may regard these four lattices as contained in $V(E_0) = T(E_0) \otimes \mathbf{Q}$. As in the discussion of §3, we may choose an element g of H_f^* such that we have simultaneously

$$T(E) = g^{-1} T(E_0), \qquad T'(E) = g^{-1} T'(E_0).$$

The class of g in $\mathscr{E} = S_f^* \backslash H_f^* / H^*$ depends only on E and its given cyclic subgroup. We define this class to be the value of ι on these data. We analogously define λ by considering cyclic subgroups of order M instead of cyclic subgroups of order Mp. That these two maps are bijections follows from (3.3) and its proof. (The completed Eichler order and the quaternion algebra have switched places in the double-coset representation because we used g^{-1} in defining ι and λ, whereas g^{+1} is used in §3.) □

We compare the degeneracy maps $\alpha, \beta : \mathscr{E} \rightrightarrows \mathscr{V}$ defined in this § with their namesakes $\alpha, \beta : \Sigma(Mp) \rightrightarrows \Sigma(M)$ defined in §3.

Proposition 4.8. *We have* $\lambda\alpha = \alpha\iota$ *and* $\lambda\beta = \beta\iota$.

Proof. Assume that we are given $T(E)$ and $T'(E)$ as above, with the quotient $T(E)/T'(E)$ cyclic of order pM. If we apply $\beta : \Sigma(Mp) \to \Sigma(M)$ in this situation, we replace $T(E)$ by the unique lattice $T(F)$ between $T'(E)$ and $T(E)$ for which $T(F)/T'(E)$ is cyclic of order M. (The notation is explained by the fact that $T(F)$ may be identified with the adelic Tate module of the elliptic curve gotten by dividing E by its given subgroup of order p.)

Let $m \in H_f^*$ again be the idele which is 1 locally except at p and the diagonal matrix $\mathrm{diag}(1, p)$ at p. Also, let $T'(E_0)$ be, as above, the sublattice of $T(E_0)$ associated with the cyclic subgroup of order pM in E_0. It is plain from the definition of S in terms of R and $\mathrm{M}(2, \mathbf{Z}_p)$ that $m^{-1} T'(E_0)$ is the sublattice of $T(E_0)$ attached to the cyclic subgroup of order M in E_0, whereas $mT(E_0)$ is the sublattice of $T(E_0)$ associated with the cyclic subgroup of order p in E_0. Applying λ to the couple $T(F)$, $T'(E)$ means finding $x \in H_f^*$ such that $T(F) = x^{-1} T(E_0)$, $T'(E) = x^{-1} m^{-1} T'(E_0)$. From the information at hand, we find that we may take $x = m^{-1} g$. Given that $\beta : \mathscr{E} \to \mathscr{V}$ is induced by multiplication by m^{-1} on H_f^*, we have verified the compatibility concerning β. That involving α is of no difficulty whatsoever. □

In view of (4.8), the bijection $\iota: \Sigma(Mp) \to \mathscr{E}$ induces an isomorphism $Y \approx Z$, which we shall also denote ι. To prove (4.3), we must establish that $\iota: Y \to Z$ is compatible with the natural pairings and the action of Hecke operators on these two modules.

We begin with the pairings. The module Y inherits from $\mathbf{Z}^{\Sigma(Mp)}$ the diagonal pairing whose value on a pair $\underline{\mathbf{E}} = (E, C)$, where $C \subset E$ is cyclic of order Mp, is the integer $\frac{1}{2}\mathrm{card}(\mathrm{Aut}(\underline{\mathbf{E}}))$. (The symbol $\underline{\mathbf{E}}$ will be used for pM-enhancement; we have been employing $\mathbf{E}$ to represent an elliptic curve which is enhanced by a subgroup of order M.) Write $\underline{\mathbf{E}}_0$ for the pair $(\mathbf{E}_0, C_p)$ appearing above, so that $S = \mathrm{End}(\underline{\mathbf{E}}_0)$, for example. As in §3, consider the locally free rank-1 left S-module $W = \mathrm{Hom}(\underline{\mathbf{E}}, \underline{\mathbf{E}}_0)$, whose class in $\mathscr{E}$ is just the edge $e = \iota(\underline{\mathbf{E}})$. It is known that $\mathrm{End}(\underline{\mathbf{E}})$ is the commutant of W, i.e., equal to the ring $\mathrm{End}_S(W)$; this may be viewed as a consequence of Tate's theorem on endomorphisms of abelian varieties over finite fields [40]. In particular, we have $\mathrm{Aut}(\underline{\mathbf{E}}) = \mathrm{Aut}_S(W)$. Hence, by (4.5) the integer $\frac{1}{2}\mathrm{card}(\mathrm{Aut}(\underline{\mathbf{E}}))$ is the number $o(e)$, which coincides with the value given to e by the natural diagonal pairing on $\mathbf{Z}^{\mathscr{E}}$.

We conclude with an examination of the action of Hecke operators, beginning with the involution T_p on Z and Y. We have quoted the theorem of [3] identifying the quotient $\mathbf{GL}(2, \mathbf{Q}_p)\backslash(\wp^{\mathrm{unr}} \times X)$ as a model for C over $\mathbf{Z}_p$. The scheme $\wp^{\mathrm{unr}}$ represents a functor involving formal groups. This functor is furnished with a natural action of the group $\mathbf{GL}(2, \mathbf{Q}_p) \times D^*$, where D is the unique quaternion division algebra (up to isomorphism) over $\mathbf{Q}_p$. The resulting action of $\mathbf{GL}(2, \mathbf{Q}_p) \times D^*$ on $\wp^{\mathrm{unr}}$ is explicited in [7], §2. From this point of view, the involution T_p of $\mathbf{GL}(2, \mathbf{Q}_p)\backslash(\wp^{\mathrm{unr}} \times X)$ is induced by the element $1 \times \pi$ of $\mathbf{GL}(2, \mathbf{Q}_p) \times D^*$, where π is a uniformizer in D. This element acts on $\wp^{\mathrm{unr}}$ as Fr^{-1}, where Fr is the Frobenius automorphism of $\wp^{\mathrm{unr}}$. Thus T_p induces the Frobenius automorphism (an involution) of $\mathscr{C}_{\mathbf{F}_p}$. By [13], Theorem 4.4, this automorphism induces the involution of $\mathscr{G} = \mathbf{GL}(2, \mathbf{Q}_p)^+\backslash(\Delta \times X)$ which is denoted w_p in [13] and $\tau(p)$ in [16]. This involution is obtained by choosing an element m of $\mathbf{GL}(2, \mathbf{Q}_p)$ which does not belong to $\mathbf{GL}(2, \mathbf{Q}_p)^+$; the resulting automorphism of $\Delta \times X$ induces an involution of $\mathscr{G}$ which is independent of the choice of m.

In the following discussion, we denote this involution by τ. We first examine the action of τ on $\mathscr{E}$, the set of edges of $\mathscr{G}$, using the notation introduced in the proof of (4.4). Take $x \in X$, and consider the image e of $(1, x) \in \mathscr{E}_\Delta \times X$ in $\mathbf{GL}(2, \mathbf{Q}_p)^+\backslash(\mathscr{E}_\Delta \times X) = \mathscr{E}$. The edge τe is represented by $(m \cdot 1, mx)$. Choose $u \in \mathbf{GL}(2, \mathbf{Q}_p)^+$ so that $um \cdot 1 = 1$ in $\mathscr{E}_\Delta$. Then τe is the class of umx in $\mathscr{E}$, thought of as $S_p^*\backslash X$. It follows that τ may be viewed as the involution of $S_p^*\backslash X$ which is induced by left multiplication by $n = um$ on X; n is easily seen to be an element of the normalizer of S_p^* in $\mathbf{GL}(2, \mathbf{Q}_p)$ which does not belong to S_p^*, and this description of n characterizes τ completely. We may take n to be the matrix $\begin{pmatrix} 0 & -1 \\ p & 0 \end{pmatrix}$, which recalls the Atkin-Lehner involution w_p of $\Sigma(Mp)$. Indeed, it is not hard to verify that $\iota: \Sigma(Mp) \to \mathscr{E}$ carries τ to w_p. The action of τ on the character group $Z \subset \mathbf{Z}^{\mathscr{E}}$, however, is the *negative* of the automorphism of $\mathbf{Z}^{\mathscr{E}}$ induced by this involution of $\mathscr{E}$. Indeed, the map τ on $\mathscr{G}$ changes the orientation of each edge $e \in \mathscr{E}$, as it evidently

maps vertices in the first copy of $\mathscr{V}$ to vertices in the second copy, and vice versa.

On the other hand, the Atkin-Lehner involution w_p of $X_0(Mpq)_{\mathbf{F}_q}$ induces a map of the associated character group $L \subset \mathbf{Z}^{\Sigma(Mp)}$ which is simply the restriction to L of the involution of $\mathbf{Z}^{\Sigma(Mp)}$ induced by w_p on $\Sigma(Mp)$. This is true because w_p preserves each of the two components of $X_0(Mpq)_{\mathbf{F}_q}$. Hence the action of w_p on $Y \subset L$ corresponds to the negative of the action of τ on Z, under the isomorphism $Y \approx Z$ induced by ι. Equivalently, the action of T_p on Z corresponds to the map $-w_p$ on Y. By (3.19), the map T_p on Z is carried to the map T_p on Y by the isomorphism ι. This completes our discussion of T_p.

The Hecke operators T_r with r prime, $r \neq p$, operate on the graph $\mathscr{G}$ through a transparent operation on X. This action is already visible on $K \backslash H_{\mathbf{f}}^*$, a space of marked L-stable lattices $T(A')$ in $V(A)$. To avoid confusion between Tate modules and Hecke operators, we temporarily refer to the r^{th} Hecke operator as ζ_r. The operator ζ_r acts on a lattice $T(A') = \Pi T_l(A')$ by "modifying" the r^{th} component $T_r(A')$ of the product, leaving the other factors untouched. Since ζ_r is a correspondence, the "modification" in fact involves replacing $T_r(A')$ by a sum of several lattices in $V_p(A)$. The sum contains $r+1$ terms for r prime to Mq, and r terms otherwise.

Since the operators ζ_r act in particular on the set of vertices of $\mathscr{G}$ through their action on X, the ζ_r preserve the decomposition of this set as a disjoint union of two copies of $\mathscr{V}$. It follows that the action of each ζ_r on the lattice Z is the restriction to Z of its action on $\mathbf{Z}^{\mathscr{E}}$.

The operator ζ_q replaces an $L \otimes \mathbf{Z}_q$-stable lattice $T \subset V_q(A)$ by a single lattice, the unique $L \otimes \mathbf{Z}_q$-lattice $T' \supseteq T$ for which $q^2 = (T' : T)$. Suppose that $T = g^{-1} T_q(A)$, with $g \in H_q^*$, where

$$H_q = \mathrm{End}_{L \otimes \mathbf{Q}_q}(V_q(A)) .$$

Then $T' = g^{-1} \pi^{-1} T_q$ if π is any uniformizer of the ring of integers of H_q. Hence the action of ζ_r on $\mathscr{E} = S_{\mathbf{f}}^* \backslash H_{\mathbf{f}}^* / H^*$ is induced by the map $x \mapsto \pi x$ on $H_{\mathbf{f}}^*$, where π now denotes an idele which is 1 away from q and a uniformizer at q. Identifying $\mathscr{E}$ with $\Sigma(Mp)$, we recognize this map as the Frobenius automorphism of $\Sigma(Mp)$, cf. Remark (3.5b). According to (3.8), applied with pM replacing M, this automorphism induces the Hecke operator T_q on Y. Hence our identification $Z \approx Y$ is compatible with the action of the q^{th} Hecke operator on the two sides.

We next consider the operator ζ_r with r a prime number prime to pqM. A lattice $T \subset V_r(A)$ is replaced by the formal sum of those lattices $T' \supseteq T$ with the property that T' is stable by $L \otimes \mathbf{Z}_r$ and $(T' : T) = r^2$. We construct these lattices (as usual) by considering the set $\mathscr{S}$ of elements of H_r^* which have reduced norm (i.e., determinant) r. We may write

$$\mathscr{S} = \coprod_{i=1}^{r+1} R_r^* a_i ,$$

with $a_i \in H_r^*$. If $T = g^{-1} T_r(A)$ with $g^{-1} \in H_r^*$, then

$$\zeta_r(T) = \sum_{i=1}^{r+1} g^{-1} a_i^{-1} T_r(A) .$$

Thus ζ_r operates on $\mathscr{E} = S_{\mathbf{f}}^* \backslash H_{\mathbf{f}}^* / H^*$ by sending $g \in H_{\mathbf{f}}^*$ to $\Sigma a_i g$. (Here the a_i are

considered as ideles through the natural inclusion of H_r^* in H_f^*. Note also that R_r and S_r coincide, since the Eichler orders R and S are equal except at p.) Identifying $\mathscr{E}$ with $\Sigma(Mp)$ as above, we again recognize a standard description of T_r in the elliptic modular case.

The final case is that where r divides M. One gets a sum of r terms, rather than a sum of $r+1$ terms, in interpreting ζ_r on $\mathscr{E}$. We omit the details.

5. Modular representations

Let N be a positive integer. Let $\mathbf{T} = \mathbf{T}_N$ be the ring generated by the Hecke operators $T_n (n \geqq 1)$ on the space of weight-2 cusp forms on $\Gamma_0(N)$. Let m be a maximal ideal of $\mathbf{T}$. The following result is a variant of [5], Th. 6.7.

Proposition 5.1. *There is a unique semisimple representation*

$$\rho_{\mathsf{m}}: G \to \mathbf{GL}(2, \mathbf{T}/\mathsf{m}),$$

where $G = \mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$, *satisfying*

$$\mathrm{trace}(\rho_{\mathsf{m}}(\mathrm{Frob}_r)) = T_r \pmod{\mathsf{m}}, \qquad \det(\rho_{\mathsf{m}}(\mathrm{Frob}_r)) = r \pmod{\mathsf{m}}$$

for almost all primes r. *The representation* ρ_{m} *is unramified at all primes* r *prime to* $\mathsf{m}N$, *and the displayed relations hold for all such primes.* (*We say that* ρ_{m} *is the representation of* G *attached to* m.)

For the convenience of the reader, we explain the relation of Proposition 5.1 to Théorème 6.7 of [5], which attaches a mod l representation of $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ to mod l modular forms which are eigenvectors for the Hecke operators T_n. Let $\mathscr{L}$ be the space of weight-2 cusp forms on $\Gamma_0(N)$ whose q-expansions at the standard cusp ∞ lie in $\mathbf{Z}[[q]]$. Then $\mathscr{L}$ and $\mathbf{T}$ are each free $\mathbf{Z}$-modules of the same rank, this rank being equal to the dimension d of the complex vector space $S_2(\Gamma_0(N))$ of all weight-2 cusp forms on $\Gamma_0(N)$. Let k be the residue field $\mathbf{T}/\mathsf{m}$. The q-expansion map

$$\mathscr{L} \to \mathbf{Z}[[q]] \tag{9}$$

induces an analogous map

$$\mathscr{L} \otimes_{\mathbf{Z}} k \to k[[q]].$$

This latter map is injective because the cokernel of (9) is torsion free.

Consider the bilinear pairing

$$(\mathscr{L} \otimes_{\mathbf{Z}} k) \times (\mathbf{T} \otimes_{\mathbf{Z}} k) \to k$$

which takes (f, T) to the coefficient of q in the q-expansion of $f \mid T$. This pairing may be viewed as a homomorphism

$$\mathscr{L} \otimes_{\mathbf{Z}} k \to \mathrm{Hom}_{\mathbf{Z}}(\mathbf{T}, k) \tag{10}$$

between k-vector spaces of dimension d. An argument borrowed from Chapter 3 of [39] shows that this homomorphism is an isomorphism. (See also [27], Th. 2.2.)

Indeed, it suffices to show that (10) is injective. An element f of the kernel has zero q-expansion, since its n^{th} q-expansion coefficient is the coefficient of q in $f|T_n$. The injectivity of the q-expansion map shows that f is 0.

Considering now the canonical map $T \mapsto (T \bmod \mathfrak{m})$ in $\mathrm{Hom}_{\mathbf{Z}}(\mathbf{T}, k)$, we find a form $f \in \mathscr{L} \otimes_{\mathbf{Z}} k$ whose q-expansion coefficients are the elements

$$t_n = (T_n \bmod \mathfrak{m})$$

of k. It is clear that f is an eigenform for the Hecke operators T_n with eigenvalues t_n.

To apply Théorème 6.7 of [5] to the form f, we should assure ourselves that f is a "cusp form mod l" in the sense that $\Sigma t_n q^n$ is the reduction (mod λ) of the q-expansion of a cusp form whose coefficients lie in a number field $K \subset \mathbf{C}$ and which are integral at a prime $\lambda | l$ of K. For this, choose a number field K and a prime $\lambda | l$ in K such that the residue field $\mathbf{F}$ of λ contains a subfield isomorphic to k. Fix an embedding $k \subsetneq \mathbf{F}$, and view f inside $\mathscr{L} \otimes_{\mathbf{Z}} \mathbf{F}$. Lift f to an element $\tilde{f}$ of $\mathscr{L} \otimes_{\mathbf{Z}} \mathcal{O}$, where $\mathcal{O}$ is the valuation ring of K at λ. The image of $\tilde{f}$ in $S_2(\Gamma_0(N))$ is then a cusp form with coefficients in $\mathcal{O}$ whose q-expansion mod λ is that of f. □

Now let $\mathfrak{m}$ be a maximal ideal of $\mathbf{T}$, and let $\rho_{\mathfrak{m}}$ be the representation of G attached to $\mathfrak{m}$. The condition on $\det(\rho_{\mathfrak{m}})$, plus the Cebotarev Density Theorem, implies that the determinant of $\rho_{\mathfrak{m}}$ is the mod l cyclotomic character of G, where l is the residue characteristic of $\mathfrak{m}$. In particular, $\rho_{\mathfrak{m}}$ is self Cartier-dual.

We consider along with $\rho_{\mathfrak{m}}$ the $(\mathbf{T}/\mathfrak{m})[G]$-module

$$W = J_0(N)[\mathfrak{m}] .$$

This "kernel of $\mathfrak{m}$ on $J_0(N)$" is defined to be the group of elements of $J_0(N)(\bar{\mathbf{Q}})$ which are annihilated by all elements of $\mathfrak{m}$. Thus, if l is the residue characteristic of $\mathbf{T}/\mathfrak{m}$, then W is a G-submodule of $J_0(N)[l]$.

Theorem 5.2. *Let $\mathfrak{m}$ be an ideal of $\mathbf{T}$ such that $\rho_{\mathfrak{m}}$ is irreducible.*

(a) *The $(\mathbf{T}/\mathfrak{m})[G]$-module W is non-zero. Its semisimplification is isomorphic to a product $V \times V \times \cdots \times V$, where V is the unique $(\mathbf{T}/\mathfrak{m})[G]$-module, up to isomorphism, which gives the representation $\rho_{\mathfrak{m}}$.*

(b) *Assume that l is prime to $2N$. Then we have $W \approx V$. That is, the product given in* (a) *has only one factor.*

(c) *Let S be a finite set of prime numbers. Let I be the ideal of $\mathbf{T}$ generated by the elements $\eta_r = 1 + r - T_r$, with r prime and $r \notin S$. Then the ideals $\mathfrak{m}$ and I are relaively prime.*

Proof. All three statements are elaborations of results of [18], with (a) and (b) coming from [18], Chapter II, Proposition 14.2. We therefore give only a brief indication of the proofs:

To prove (a), we first note that W is non-zero because the action of $\mathbf{T}$ on $J_0(N)$ is faithful. Form the direct sum D of W and its Cartier dual $\mathrm{Hom}(W, \mu_l)$. For all primes r prime to Nl, the characteristic polynomial of Frob_r acting on D, relative to the field $\mathbf{T}/\mathfrak{m}$, is then $(x^2 - T_r x + r)^n$, where n is the $\mathbf{T}/\mathfrak{m}$-dimension of W. By the Cebotarev Density and Brauer-Nesbitt theorems, it follows that the semisimplification of W is V^n. This gives (a).

To prove (b), we pick a minimal (non-zero) $(\mathbf{T}/\mathfrak{m})[G]$-submodule of W. By (a), this submodule is isomorphic to V. Hence we have an inclusion $V \subset W$, and we must prove that $V = W$. The hypothesis that N and l are relatively prime facilitates the consideration of $X_0(N)$ over $\mathbf{F}_l$. Let X denote the curve $X_0(N)$ over $\mathbf{F}_l$. The injective q-expansion map

$$H^0(X, \Omega^1) \to \mathbf{F}_l[[q]]$$

and the arguments of ([18], Ch. II, §9) show that $H^0(X, \Omega^1)[\mathfrak{m}]$ is of $\mathbf{T}/\mathfrak{m}$-dimension $\leqq 1$.

Since $J = J_0(N)$ is the Picard variety of $X_0(N)$, we find (computing over $\mathbf{F}_l$) that

$$H^1(J, \mathcal{O})/\mathfrak{m}H^1(J, \mathcal{O})$$

is of $\mathbf{T}/\mathfrak{m}$-dimension $\leqq 1$. We will deduce (5.2b) from this fact, together with arguments which parallel those given on pp. 116–117 of [18].

Let $\mathcal{J}$ be the Néron model model of J over $\mathbf{Q}_l$, so that $\mathcal{J}$ is an abelian scheme over $\mathbf{Z}_l$. Consider the Zariski closures $\mathcal{V}$ and $\mathcal{W}$ of V and W in $\mathcal{J}$. These are contained in the kernel $\mathcal{J}[l]$ of multiplication by l on $\mathcal{J}$, a group which is finite and flat over $\mathbf{Z}_l$, since $\mathcal{J}$ is an abelian scheme. Hence $\mathcal{V}$ and $\mathcal{W}$ are finite and flat. The hypothesis that l is prime to $2N$ gives in particular that $e < (l-1)$, where $e(=1)$ is the absolute ramification index of $\mathbf{Q}_l$. The results of [25], §3 therefore apply to show that $\mathcal{V}$ and $\mathcal{W}$ are $\mathbf{T}/\mathfrak{m}$-vector space schemes ([25], 3.3.2) and that $\mathcal{V}$ is a subgroup of $\mathcal{W}$ ([25], 3.3.6). Moreover, the quotient $\mathcal{W}/\mathcal{V}$ is finite and flat ([25], 3.3.6). Therefore, the following conditions are all equivalent:

1. $V = W$,
2. $\mathcal{V} = \mathcal{W}$,
3. $\mathcal{V}_s = \mathcal{W}_s$.

Here $\mathcal{V}_s$ and $\mathcal{W}_s$ are the special fibers of $\mathcal{V}$ and $\mathcal{W}$; they are $\mathbf{T}/\mathfrak{m}$-vector space schemes over $\mathbf{F}_l$.

In particular, the assertion (5.2b) means that the inclusion $\mathcal{V}_s \subset \mathcal{W}_s$ is an equality, i.e., that the quotient $\mathcal{W}_s/\mathcal{V}_s$ is 0. We note that $\mathcal{W}_s/\mathcal{V}_s$ is certainly a successive extension of copies of $\mathcal{V}_s$, and also that $\mathcal{V}_s$ is auto Cartier-dual. Indeed, these statements follow from (5.2a) and the auto-duality of V, by arguments using [25] which are analogous to those just given.

Let $\mathcal{D}$ be the contravariant Dieudonné-module functor of Oda [23], denoted M in [23] and on pp. 116–117 of [18]. We shall apply $\mathcal{D}$ to finite flat group schemes of type $(l, \ldots, l)$ over $k = \mathbf{F}_l$, thereby obtaining finite-dimensional k-vector spaces which come equipped with a Frobenius map ϕ and a Verschiebung v. These are commuting k-linear maps of the vector space; the composites ϕv and $v\phi$ are 0. Since we now consider only group schemes in characteristic l, we will write simply V and W for $\mathcal{V}_s$ and $\mathcal{W}_s$, J for the reduction of $J_0(N)$ mod l, and so forth. Finally, we will write Frob and Ver for the Frobenius and Verschiebung endomorphisms of a group scheme over $\mathbf{F}_l$.

By general properties of $\mathscr{D}$, we have a canonical isomorphism

$$\mathscr{D}(J[l]) \approx H^1_{\mathrm{DR}}(J/k)\,.$$

Moreover, the quotient $\mathscr{D}(J[\mathsf{Ver}])$ of $\mathscr{D}(J[l])$ corresponds to the quotient $H^1(J, \mathscr{O})$ of $H^1_{\mathrm{DR}}(J/k)$. By functoriality, we get that

$$\mathscr{D}(W[\mathsf{Ver}]) = H^1(J, \mathscr{O})/\mathsf{m}H^1(J, \mathscr{O})\,,$$

so that $\mathscr{D}(W[\mathsf{Ver}])$ is of dimension $\leqq 1$ over $\mathbf{T}/\mathsf{m}$. On the other hand, the auto-duality of V induces an auto-duality of $\mathscr{D}(V)$. Under this auto-duality, the maps ϕ and v of $\mathscr{D}(V)$ are interchanged. It follows that these maps have the same rank as endomorphisms of the 2-dimensional $\mathbf{T}/\mathsf{m}$-vector space $\mathscr{D}(V)$. Since their composite is 0, the common rank is either 0 or 1.

Now $\mathscr{D}(V[\mathsf{Ver}])$ is the cokernel of v on $\mathscr{D}(V)$, so that $\mathscr{D}(V[\mathsf{Ver}])$ has dimension 1 or 2 over $\mathbf{T}/\mathsf{m}$. Since $\mathscr{D}(V[\mathsf{Ver}])$ is a quotient of $\mathscr{D}(W[\mathsf{Ver}])$, which has rank at most 1, we conclude that $\mathscr{D}(V[\mathsf{Ver}])$ and $\mathscr{D}(W[\mathsf{Ver}])$ both have rank 1, and that the groups $V[\mathsf{Ver}]$ and $W[\mathsf{Ver}]$ are equal.

Let $Q = W/V$. We claim that $Q[\mathsf{Ver}] = 0$, i.e., that v is an automorphism of $\mathscr{D}(Q)$. This follows from an easy snake-lemma argument, which is axiomatized as Lemma (14.6) in [18]. Our claim follows from that lemma on taking $M_1 = \mathscr{D}(Q)$, $M_2 = \mathscr{D}(W)$, and $M_3 = \mathscr{D}(V)$.

From this claim, we are now able to conclude, as desired, that $Q = 0$. Indeed, were Q non-zero, we could find an inclusion $V \subset Q$, since Q is a successive extension of copies of V, as remarked above. This gives a contradiction, since $V[\mathsf{Ver}]$ is non-zero, whereas $Q[\mathsf{Ver}]$ is 0.

To prove (c), we assume that m and I are not relatively prime. We have then

$$T_r \equiv (1 + r) \pmod{\mathsf{m}}$$

for almost all r. The representation ρ_{m} then has the same characteristic polynomials as the direct sum of the 1-dimensional trivial representation and the 1-dimensional cyclotomic representation. In view of the Cebotarev Density and Brauer-Nesbitt theorems, we conclude that ρ_{m} has the same semisimplification as this direct sum. This contradicts the hypothesis that ρ_{m} is irreducible. □

Definition. Suppose that

$$\rho: G \to \mathbf{GL}(2, \mathbf{F})$$

is a continuous homomorphism, where $\mathbf{F}$ is a finite field. Let l be the characteristic of $\mathbf{F}$. We say that the representation ρ is *modular of level N* if the determinant of ρ is the mod l cyclotomic character and if there is a homomorphism

$$\omega: \mathbf{T} \to \bar{\mathbf{F}}$$

such that

$$\mathrm{trace}(\rho(\mathsf{Frob}_r)) = \omega(T_r)$$

for almost all prime numbers r.

Given ρ as in the definition, set $\mathsf{m} = \ker(\omega)$ and observe that ω embeds $\mathbf{T}/\mathsf{m}$ into $\bar{\mathbf{F}}$. The semisimplifications of ρ and ρ_{m} are then both defined over subfields of

the field $\bar{\mathbf{F}}$. Since their traces and determinants coincide, their semisimplifications are isomorphic over $\bar{\mathbf{F}}$.

The following complement to Theorem 5.2b is the principal result of [21].

Theorem 5.3. *Let* $\mathfrak{m}$ *be an ideal of* $\mathbf{T}$ *for which* $\rho_{\mathfrak{m}}$ *is irreducible. Suppose that the residue characteristic* l *of* $\mathfrak{m}$ *is an odd prime which divides* N. *Assume further that* l^2 *does not divide* N *and that the representation* $\rho_{\mathfrak{m}}$ *is not modular of level* N/l. *Then the group* $J_0(N)[\mathfrak{m}]$ *is of* $\mathbf{T}/\mathfrak{m}$*-dimension* 2. *In other words, we have* $V \approx W$ *in the notation of Theorem* 5.2.

6. A theorem of Mazur

Fix a positive integer M and a prime p not dividing M. Let $\mathbf{T} = \mathbf{T}_N$, where $N = pM$, be the Hecke ring of level N. Let $\mathfrak{m}$ be a maximal ideal of $\mathbf{T}$ and set $k = \mathbf{T}/\mathfrak{m}$. Let V be a $k[G]$-module which gives the representation $\rho_{\mathfrak{m}}$. Consider the following hypotheses:

(i) The representation $\rho_{\mathfrak{m}}$ is irreducible.
(ii) The residue characteristic l of $\mathfrak{m}$ is odd.
(iii) The representation $\rho_{\mathfrak{m}}$ is finite at p.

The last hypothesis means that there is a finite flat k-vector space scheme $\mathscr{V}$ over $\mathbf{Z}_p$ for which the resulting representation of $\mathrm{Gal}(\bar{\mathbf{Q}}_p/\mathbf{Q}_p)$ coincides with the restriction to $\mathrm{Gal}(\bar{\mathbf{Q}}_p/\mathbf{Q}_p)$ of $\rho_{\mathfrak{m}}$.

Theorem 6.1. (Mazur [20]) *Assume that the above hypothesis* (i), (ii), *and* (iii) *are satisfied. Suppose further that we have*

$$p \not\equiv 1 \pmod{l}.$$

Then the representation $\rho_{\mathfrak{m}}$ *is modular of level* $M = N/p$.

Proof. According to (5.2a), we may find an inclusion of $\mathbf{T}/\mathfrak{m}[G]$-modules $V \subset J[\mathfrak{m}]$, where $J = J_0(N)$. Fix such an inclusion, and view it as a map $\iota: V \to J$. Since $\rho_{\mathfrak{m}}$ is finite, V extends to a finite flat $\mathbf{T}/\mathfrak{m}$-vector space scheme $\mathscr{V}$ over $\mathbf{Z}_p$.

Lemma 6.2. *The map* ι *prolongs to a map* $\mathscr{V} \to \mathscr{J}$, *where* $\mathscr{J}$ *is the Néron model of* $J_{\mathbf{Q}_p}$.

Proof. This is evident when $p \neq l$, by the Néronian property of $\mathscr{J}$. Suppose now that $p = l$. Then $p > 2$, by (iii); hence the absolute ramification index e of $\mathbf{Q}_p$ (which is 1) satisfies the condition $e < p - 1$ of [25], Cor. 3.3.6. Also, $J_{\mathbf{Q}_p}$ has semistable reduction, since p^2 does not divide N.

Because of the semistable reduction, the kernel $\mathscr{J}[p]$ of p on $\mathscr{J}$ is a flat quasi-finite group scheme over $\mathbf{Z}_p$ ([11], 2.2.1). Let $\mathscr{J}[p]^{\mathrm{f}}$ be the "fixed part" of this group scheme ([11], 2.2.2). Then $\mathscr{J}[p]^{\mathrm{f}}$ is finite and flat, and the quotient

$$Q = \mathscr{J}[p]/\mathscr{J}[p]^{\mathrm{f}}$$

is étale and quasi-finite, and has trivial special fiber (cf. [19]). Moreover, the $\mathrm{Gal}(\bar{\mathbf{Q}}_p/\mathbf{Q}_p)$-module $Q(\bar{\mathbf{Q}}_p)$ is unramified. To see this, we apply the results of [11], §11.6, replacing $\mathbf{Q}_p$ by its maximal unramified extension K and $\mathbf{Z}_p$ by the ring of

integers of this field. The group Q becomes a quotient of the group scheme ${}_p\Psi$ appearing in [11], 11.6.6. In [11], 11.6.7, the generic fiber of ${}_p\Psi$ is identified with the group M/pM, where M is a certain constant group scheme. Hence Q_K is constant, which means that the inertia group $\mathrm{Gal}(\bar{\mathbf{Q}}_p/K)$ of $\mathrm{Gal}(\bar{\mathbf{Q}}_p/\mathbf{Q}_p)$ acts trivially on $Q(\bar{\mathbf{Q}}_p)$.

Express $\mathscr{V}$ in the usual way as an extension of an étale group scheme $\mathscr{V}^{\mathrm{et}}$ by a connected group scheme $\mathscr{V}^0$, and write $\mathscr{V}^{\mathrm{et}}$ and V^0 for the generic fibers of these finite flat group schemes over $\mathbf{Z}_p$. Considered as a $\mathrm{Gal}(\bar{\mathbf{Q}}_p/\mathbf{Q}_p)$-module, V^{et} is the largest unramified quotient of V because of [25], *loc. cit.*

It follows that the image of V^0 under ι lands in the generic fiber $J[p]^{\mathrm{f}}$ of $\mathscr{J}[p]^{\mathrm{f}}$, since Q is unramified. By [25], Cor. 3.3.6, the map $V^0 \to J[p]^{\mathrm{f}}$ induced by ι prolongs uniquely to a map $u: \mathscr{V}^0 \to \mathscr{J}[p]^{\mathrm{f}}$. We obtain the desired prolongation of ι from [11], lemme (5.9.2), applied with $G = \mathscr{V}$, $A = \mathscr{J}$, $v_\eta = \iota$, $G'' = \mathscr{V}^{\mathrm{et}}$, $G' = \mathscr{V}^0$, and $u = u$. This completes the proof of (6.2). □

We now (re-) introduce some notation which is essentially that of §3, except that p will now play the role of the prime q of §3. Write J_s for the special fiber of the Néron model J, and J^0 for the connected component of 0 in J_s. Then J^0 is an extension of the product $J_0(M) \times J_0(M)$ by a torus T. Let X be the character group of T. Let Φ be the group of components of J_s. Using the map $\mathscr{V} \to J$ of (6.2), together with the results of Raynaud [25], identify $\mathscr{V}$ with a subgroup of the largest finite flat subgroup H of $\mathscr{J}[l]$. Write $\mathscr{V}_s$ for the special fiber of $\mathscr{V}$.

Lift T to the torus

$$\underline{T} = \mathrm{Hom}(X, \mathbf{G}_m)$$

over $\mathbf{Z}_p$. According to [11], §5.1, $\underline{T}$ embeds into the formal completion of $\mathscr{J}$ along its special fiber. This implies that $\underline{T}[l]$ is naturally a finite, flat subgroup of H.

Lemma 6.3. *If ρ_{m} is not modular of level N/p, then the group $\mathscr{V}$ is a subgroup of $\underline{T}[l]$.*

Proof. The group $\mathscr{V}_s$ is contained in J^0 because of (3.12) and (5.2c). Further, if $\mathscr{V}_s$ maps non-trivially to $J_0(M) \times J_0(M)$, then the maximal ideal m of $\mathbf{T}$ arises from a maximal ideal of the p-old quotient $\mathbf{T}_0$ of $\mathbf{T}$ in view of (3.11). This implies that the representation ρ_{m} is modular of level $M = N/p$. Thus our assumption that ρ_{m} is not modular of level N/p implies that $\mathscr{V}_s$ is contained in T.

To prove that $\mathscr{V}$ is a subgroup of $T[l]$, we consider the composite v of the two maps

$$\mathscr{V} \to H, \qquad H \to H/\underline{T}[l] .$$

The map v has a finite, flat kernel, since we are in a limited-ramification situation in case $l = p$. (Since $l \geqq 3$, we have $p \geqq 3$ in case $p = l$.) However, the kernel of v contains $\mathscr{V}_s$ in view of what we have already proved. It follows that the kernel of v coincides with $\mathscr{V}$, proving (6.3). □

We now prove (6.1). Let $D = \mathrm{Gal}(\bar{\mathbf{Q}}_p/\mathbf{Q}_p)$, thought of as a decomposition group in $G = \mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$. Assuming that ρ_{m} is not modular of level N/p, we obtain from (6.3) the inclusion of $\mathbf{T}/\mathsf{m}[D]$-modules

$$V \subset \underline{T}[\mathsf{m}](\bar{\mathbf{Q}}_p) = \mathrm{Hom}(X/\mathsf{m}X, \mu_l) .$$

The action of D on $X/\mathfrak{m}X$ is unramified; it is given by the Frobenius automorphism of X (coming from the fact that T is defined over $\mathbf{F}_p$). The Frobenius automorphism of X coincides with the Hecke operator T_p (3.8). This operator is an involution, the negative of the Atkin-Lehner involution w_p. Therefore its action on $X/\mathfrak{m}X$ is given by either $+1$ or -1, since $\mathbf{T}/\mathfrak{m}$ is a field. It follows that the action of D on $\mathrm{Hom}(X/\mathfrak{m}X, \mu_l)$ is given by the $\mathbf{F}_l$-valued character $\varepsilon\chi$, where ε is an unramified quadratic character. This implies that D acts on V by $\varepsilon\chi$, since V is a submodule of $\mathrm{Hom}(X/\mathfrak{m}X, \mu_l)$.

In particular, the character giving the action of D on $\det_{\mathbf{T}/\mathfrak{m}}(V)$ is $\varepsilon^2\chi^2 = \chi^2$. On the other hand, the determinant of V is the cyclotomic character χ. Comparing the two expressions for the determinant, we get that χ is trivial, which is equivalent to the congruence $p \equiv 1 \pmod{l}$. □

A variant

Theorem 6.4. *Assume that* $\mathfrak{m}$ *is a maximal ideal of* $\mathbf{T}$ *which satisfies conditions* (i) *and* (ii) *above. Assume further that the residue characteristic* l *of* $\mathfrak{m}$ *is prime to* $pM(p-1)$. *Then the* $\mathbf{T}/\mathfrak{m}$*-vector space* $X/\mathfrak{m}X$ *is of dimension* $\leqq 1$.

Proof. Since l is prime to $N = pM$, (5.2b) implies that $V = J_0(N)[\mathfrak{m}]$ is a two-dimensional $\mathbf{T}/\mathfrak{m}$-vector space which gives the representation $\rho_{\mathfrak{m}}$. Since $\mathrm{Hom}(X/\mathfrak{m}X, \mu_l)$ is a subspace of V (considered as a $\mathbf{T}/\mathfrak{m}[D]$-module), $X/\mathfrak{m}X$ is of dimension $\leqq 2$. If $X/\mathfrak{m}X$ is of dimension 2, then we get the equality

$$V = \mathrm{Hom}(X/\mathfrak{m}X, \mu_l)\,.$$

Arguing as above, we get the congruence $p \equiv 1 \pmod{l}$. This is contrary to our assumption about l. □

7. Raising the level

Consider again two distinct primes p and q and a positive integer M prime to pq. The ring $\mathbf{T}_{pM}$ of Hecke operators of level pM is a ring of endomorphisms of the space $S_2(\Gamma_0(pM))$ of cusp forms of level pM (and weight 2). It operates diagonally on the sum $S_2(\Gamma_0(pM)) \oplus S_2(\Gamma_0(pM))$ of two copies of $S_2(\Gamma_0(pM))$, which we may regard as the q-old subspace of the space $S_2(\Gamma_0(pqM))$ of cusp forms of level pqM. The ring $\mathbf{T}_{pqM}$ operates faithfully on $S_2(\Gamma_0(pqM))$, and this operation preserves the subspace $S_2(\Gamma_0(pM)) \oplus S_2(\Gamma_0(pM))$. The image of $\mathbf{T}_{pqM}$ in the ring of endomorphisms of $S_2(\Gamma_0(pM)) \oplus S_2(\Gamma_0(pM))$ is the q-old quotient $\mathbf{T}_{pqM,q\text{-old}}$ of $\mathbf{T}_{pqM}$.

The two subrings $\mathbf{T}_{pM}$ and $\mathbf{T}_{pqM,\,q\text{-old}}$ of $\mathrm{End}(S_2(\Gamma_0(pM))^2)$ share a common subring: the ring R generated by the T_n with n prime to q. We have

$$\mathbf{T}_{pM} = R[\tau], \qquad \mathbf{T}_{pqM,\,q\text{-old}} = R[T_q]\,,$$

where τ and T_q are the q^{th} Hecke operators in level pM and pqM, respectively. These two Hecke operators commute with each other (and with the elements of R).

Moreover, they are connected by the quadratic equation

$$T_q^2 - T_q\tau + q = 0\,,$$

Given maximal ideals λ of $\mathbf{T}_{pM}$ and $\mathfrak{m}$ of $\mathbf{T}_{pqM,\,q\text{-old}}$, we say that they are *compatible* if there is a maximal ideal of the ring $\mathscr{R} = R[\tau, T_q]$ which contains them both. At the same time, we identify the set of maximal ideals of $\mathbf{T}_{pqM,\,q\text{-old}}$ with a subset of the set of maximal ideals of $\mathbf{T}_{pqM}$; we say that a maximal ideal of $\mathbf{T}_{pqM}$ is q-old if it arises from a maximal ideal of the quotient $\mathbf{T}_{pqM,\,q\text{-old}}$.

By the going-up theorem of Cohen-Seidenberg, every λ is compatible with at least one $\mathfrak{m}$. At the same time, it is evident that the representations ρ_λ and $\rho_\mathfrak{m}$ are isomorphic if λ and $\mathfrak{m}$ are compatible. Hence every representation which is modular of level pM is modular of level pqM.

Finally, suppose that λ is p-new, i.e., that λ arises from the quotient $\mathbf{T}_{pM,\,p\text{-new}}$ of $\mathbf{T}_{pM}$ which is associated with the Petersson-orthogonal complement of $S_2(\Gamma_0(M)) \oplus S_2(\Gamma_0(M))$ in $S_2(\Gamma_0(pM))$. Then there are maximal ideals $\mathfrak{m}$ of $\mathbf{T}_{pqM}$ which are p-new and which are compatible with λ. (Such $\mathfrak{m}$ are then p-new and q-old.) One sees this by working in the p-new subspace of $S_2(\Gamma_0(pqM))$ rather than in $S_2(\Gamma_0(pqM))$ itself.

Lemma 7.1. *Let p and M be given, and let λ be a maximal ideal of $\mathbf{T}_{pM}$. Then there exist infinitely many prime numbers q, prime to $pM\lambda$, for which $\rho_\lambda(\mathrm{Frob}_q)$ has trace 0 and determinant -1.*

Proof. Let c be a complex conjugation in the Galois group G. The matrix $\rho_\lambda(c)$ has trace 0 and determinant -1. By the Cebotarev Density Theorem, there are infinitely many q for which $\rho_\lambda(\mathrm{Frob}_q)$ is conjugate to $\rho_\lambda(c)$. Such q satisfy the given condition. □

Remark 7.2. The determinant of $\rho_\lambda(\mathrm{Frob}_q)$ is q modulo λ, i.e., $q \bmod l$, if l is the residue characteristic of λ. Hence $\rho_\lambda(\mathrm{Frob}_q)$ has determinant -1 if and only if we have $q \equiv -1 \pmod{l}$.

Theorem 7.3. *Let p and M be given, and let λ be a maximal ideal of $\mathbf{T}_{pM}$ which is p-new. Assume that ρ_λ is irreducible. Let q be a prime number satisfying the condition of* (7.1), *and let $\mathfrak{m}$ be a p-new maximal ideal of $\mathbf{T}_{pqM}$ which is compatible with λ. Then $\mathfrak{m}$ is pq-new*; i.e., $\mathfrak{m}$ *arises from a maximal ideal of the pq-new quotient $\bar{\mathbf{T}}_{pqM}$ of $\mathbf{T}_{pqM}$.*

Remarks 7.4. a. The conclusion of (7.3) may seem paradoxical, since $\mathfrak{m}$ is visibly q-old. However, it is possible for an ideal of $\mathbf{T}_{pqM}$ to be both q-new and q-old. This reflects the fact that newforms and oldforms may be congruent modulo l. In a terminology introduced by Mazur, $\mathfrak{m}$ is an *ideal of fusion* between the q-old and the q-new subspaces of $S_2(\Gamma_0(pqM))$.

b. Essentially the same information as that given by (7.3) may be obtained by the techniques of [28]. This possibility is explored in [31].

Theorem 7.5. *Let q and M be given, and let λ be a maximal ideal of $\mathbf{T}_{qM}$ which is q-new. Assume that ρ_λ is irreducible. Let p be a prime number prime to $qM\lambda$ for which $\rho_\lambda(\mathrm{Frob}_p)$ has trace 0 and determinant -1. Let $\mathfrak{m}$ be a q-new maximal ideal of $\mathbf{T}_{pqM}$ which is compatible with λ. Then $\mathfrak{m}$ is pq-new*; i.e., $\mathfrak{m}$ *arises from a maximal ideal of the pq-new quotient $\bar{\mathbf{T}}_{pqM}$ of $\mathbf{T}_{pqM}$.*

Theorems (7.3) and (7.5) are obviously equivalent: one passes between them by reversing the roles of p and q. Theorem (7.3) is needed in our application, whereas Theorem (7.5) is more convenient to prove with the notation introduced in §4. This explains why they are both stated here. To establish (7.5), we first prove:

Lemma 7.6. *In the situation of* (7.5), *one has* $(T_p)^2 - 1 \in \mathsf{m}$.

Proof. Consider the (commutative) subring $\mathscr{R}$ of $\mathrm{End}(S_2(\Gamma_0(qM)) \oplus S_2(\Gamma_0(qM))$ which is generated by T_{pM} and by $\mathbf{T}_{qpM,\,p\text{-old}}$. (Thus $\mathscr{R}$ is the ring denoted by this symbol above, but with the roles of p and q appropriately reversed.) By the definition of "compatible," there is a maximal ideal I of $\mathscr{R}$ which contains m and λ. We have

$$T_p^2 - 1 = \tau T_p - (p+1)\,.$$

Since τ and $p+1$ are elements of λ, $T_p^2 - 1 \in I$. Since $I \cap \mathbf{T}_{qpM,\,p\text{-old}} = \mathsf{m}$, we get (7.6). □

To prove (7.5), we consider the character group X associated with the toric part of the reduction of $J_0(Mq)$ at the prime q. The group $X \oplus X$ is then a $\mathbf{T}_{qpM}$-module, and $\mathbf{T}_{qpM}$ acts on $X \oplus X$ through its p-old/q-new quotient, which acts faithfully on $X \oplus X$, cf. (3.21). Since m is q-new and p-old, it follows that m belongs to the support of the $\mathbf{T}_{qpM}$-module $X \oplus X$. From (7.6), we find then that m belongs to the support of the $\mathbf{T}_{qpM}$-module $(X \oplus X)/(T_p^2 - 1)(X \oplus X)$. By (4.3), (3.12) and (5.2c), m belongs to the support of the $\mathbf{T}_{qpM}$-module denoted Ψ in (4.3). (In invoking (5.2c), we use the hypothesis that ρ_λ is irreducible.) However, $\mathbf{T}_{qpM}$ acts on Ψ through its pq-new quotient $\bar{\mathbf{T}}_{pqM}$. In particular, the ideal m of $\mathbf{T}_{qpM}$ does not generate the unit ideal of $\bar{\mathbf{T}}_{pqM}$. This is what is needed to prove (7.5).

8. Lowering the level

In this § we again consider two distinct primes p and q, together with a positive integer M prime to pq. We let $\mathbf{T} = \mathbf{T}_{pqM}$ and let $\bar{\mathbf{T}}$ be its pq-new quotient. We let m be a maximal ideal of $\bar{\mathbf{T}}$, and let l be the residue characteristic of m. We assume that l is odd and that ρ_{m} is irreducible.

Theorem 8.1. *Suppose that l is prime to qM and that ρ_{m} is finite at p. Assume that the prime number q does not satisfy $q \equiv 1 \pmod{l}$. Then ρ_{m} is modular of level qM.*

Proof. By (6.1), we may assume that $p \equiv 1 \pmod{l}$. In particular, we may (and do) assume that l is prime to pqM. Let C be the Shimura curve studied in §4: the curve associated with the group of norm-1 units in an Eichler order of level M in "the" quaternion algebra over $\mathbf{Q}$ of discriminant pq. Let $J = \mathrm{Pic}^0(C)$ be the Jacobian of C. (We take the field of definition of C to be $\mathbf{Q}$, as in §4.) Consider the $\mathbf{T}/\mathsf{m}[G]$-module

$$W = J(\bar{\mathbf{Q}})[\mathsf{m}]\,,$$

cf. §5. Because of the Eichler-Shimura relations for J ([37], 11.17 or [38], 2.23), the

proof of (5.2a) shows that W is a successive extension of copies of the $\mathbf{T}/\mathfrak{m}[G]$-module V which corresponds to the representation $\rho_{\mathfrak{m}}$. Since $\mathfrak{m}$ is an ideal of $\bar{\mathbf{T}}$, W is non-zero. Hence there is an embedding of $\mathbf{T}/\mathfrak{m}[G]$-modules $V \subsetneq W$.

Fixing such an embedding and using the hypothesis that V is finite at p (since l and p are distinct, this hypothesis means that V is unramified at p), we identify V with a subgroup of $J(\bar{\mathbf{F}}_p)$. This identification respects the natural actions of $\mathbf{T}$ and $\mathrm{Frob}_p \in \mathrm{Gal}(\bar{\mathbf{F}}_p/\mathbf{F}_p)$ on V and $J(\bar{\mathbf{F}}_p)$. Let Ψ be the group of components and let Z be the character group of the torus attached to the reduction of J at p. If the image of V in Ψ is non-zero, then $\mathfrak{m}$ belongs to the support of Ψ. By (4.3), (3.12) and (5.2c), $\mathfrak{m}$ belongs to the support of the $\mathbf{T}$-module $X \oplus X$, where X is again the character group arising from the bad reduction of $J_0(qM)$ at q. This implies that $\mathfrak{m}$ comes from the q-new/p-old quotient of $\mathbf{T}$ (3.21). It follows easily from this that $\rho_{\mathfrak{m}}$ is isomorphic to ρ_λ for some maximal ideal λ of $\mathbf{T}_{qM}$. Hence $\rho_{\mathfrak{m}}$ is modular of level qM.

It remains to treat the case where the image of V in Ψ is zero, i.e., where V is contained in the group $\mathrm{Hom}(Z/\mathfrak{m}Z, \mu_l)$. We have then

$$\dim_{\mathbf{T}/\mathfrak{m}}(Z/\mathfrak{m}Z) \geqq 2 .$$

By (4.1), we have $\dim_{\mathbf{T}/\mathfrak{m}}(Y/\mathfrak{m}Y) \geqq 2$, where Y is the $\mathbf{T}$-module defined in §3 as the kernel of the surjection $L \to (X \oplus X)$, L being the character group of the torus arising from the reduction of $J_0(pqM)$ at q. We may assume that $\mathfrak{m}$ does not belong to the support of $X \oplus X$, since we have already established that the conclusion of the theorem holds if it does belong to the support of $X \oplus X$.

Under this assumption, we have an isomorphism

$$Y/\mathfrak{m}Y \approx L/\mathfrak{m}L ,$$

giving finally the statement $\dim_{\mathbf{T}/\mathfrak{m}}(L/\mathfrak{m}L) \geqq 2$. We get a contradiction by applying (6.4) to the group L. (We apply the theorem with p replaced by q and M replaced by pM). □

Theorem 8.2. (Main Theorem) *Let* $\rho: \mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}) \to \mathbf{GL}(2, \mathbf{F})$ *be an irreducible* mod l *modular representation of level* Mp, *where* p *is a prime not dividing* M. *Assume that* ρ *is finite at* p. *Then* ρ *is modular of level* M *provided that at least one of the following two conditions holds*:

(i) *The prime* l *is a not a divisor of* M;

(ii) *We do not have* $p \equiv 1 \pmod{l}$.

Proof. We have $\rho \approx \rho_\lambda$ for some maximal ideal λ of $\mathbf{T}_{Mp}$. By (6.1), we know that ρ is modular of level M if (ii) holds. Hence we may assume that $p \equiv 1 \pmod{l}$, and in particular that p and l are distinct.

Also, if λ arises from the p-old quotient of $\mathbf{T}_{Mp}$, then there is nothing to prove. Hence we may assume that λ does not arise from the p-old quotient of $\mathbf{T}_{Mp}$, which implies in particular that it *does* arise from the p-new quotient of $\mathbf{T}_{Mp}$.

Assuming that λ arises from this quotient, we choose a prime number q as in (7.1) and pick a p-new maximal ideal $\mathfrak{m}$ of $\mathbf{T} = \mathbf{T}_{Mqp}$ which is compatible with λ. By (7.3), $\mathfrak{m}$ is a pq-new maximal ideal of $\mathbf{T}$. If (i) holds, then (8.1) applies to show that ρ is modular of level qM. (Note that we have $q \equiv -1 \pmod{l}$; since l is odd, we do

not have $q \equiv +1 \pmod{l}$.) Applying (6.1), with p replaced by q, we deduce that ρ is modular of level M. □

References

1. Atkin, A.O.L., Lehner, J.: Hecke operators on $\Gamma_0(m)$. Math. Ann. **185**, 134–160 (1970)
2. Carayol, H.: Sur la mauvaise réduction des courbes de Shimura. Compos. Math. **59**, 151–230 (1986)
3. Cerednik, I.V.: Uniformization of algebraic curves by discrete arithmetic subgroups of $\mathrm{PGL}_2(k_w)$ with compact quotients (in Russian). Mat. Sb. **100**, 59–88 (1976). Translation in Math. USSR Sb. **29**, 55–78 (1976)
4. Deligne, P., Rapoport, M.: Les schémas de modules de courbes elliptiques. (Lecture Notes in Math. Vol. **349**, pp. 143–316.) Berlin-Heidelberg-New York: Springer 1973
5. Deligne, P., Serre, J-P.: Formes modulaires de poids 1. Ann. Sci. Ec. Norm. Sup., IV. Ser. **7**, 507–530 (1974)
6. Deuring, M.: Die Typen der Multiplikatorenringe elliptischer Funktionenkörper. Abh. Math. Semin. Univ. Hamb. **14**, 197–272 (1941)
7. Drinfeld, V.G.: Coverings of p-adic symmetric regions (in Russian). Funkts. Anal. Prilozn **10**, 29–40 (1976). Translation in Funct. Anal. Appl. **10**, 107–115 (1976)
8. Edixhoven, S.J.: L'action de l'algèbre de Hecke sur les groupes de composantes des jacobiennes des courbes modulaires est "Eisenstein". Preprint
9. Eichler, M.: Quadratische Formen und Modulfunktionen. Acta Arith. **4**, 217–239 (1958)
10. Frey, G.: Links between stable elliptic curves and certain diophantine equations. Ann. Univ. Sarav., Ser Math. **1**, 1–40 (1986)
11. Grothendieck, A.: SGA7 I, Exposé IX. (Lecture Notes in Math. Vol. **288**, pp. 313–523.) Berlin-Heidelberg-New York: Springer 1972
12. Jacquet, H., Langlands, R.P.: Automorphic forms on GL(2). (Lecture Notes in Math. Vol. **114**.) Berlin-Heidelberg-New York: Springer 1970
13. Jordan, B., Livné, R.: Local diophantine properties of Shimura curves. Math. Ann. **270**, 235–248 (1985)
14. Jordan, B., Livné, R.: On the Néron model of Jacobians of Shimura curves. Compos. Math. **60**, 227–236 (1986)
15. Katz, N.M., Mazur, B.: Arithmetic Moduli of Elliptic Curves. Ann. Math. Stud. **108** (1985)
16. Kurihara, A.: On some examples of equations defining Shimura curves and the Mumford uniformization. J. Fac., Sci., Univ. Tokyo, Sec. IA **25**, 277–300 (1979)
17. Langlands, R.P.: Some contemporary problems with origins in the Jugendtraum. Proc. Symp. Pure Math. **28**, 401–418 (1976)
18. Mazur, B.: Modular curves and the Eisenstein ideal. Publ. Math., Inst. Hautes Etud. Sci. **47**, 33–186 (1977)
19. Mazur, B.: Rational isogenies of prime degree. Invent. Math. **44**, 129–162 (1978)
20. Mazur, B.: Letter to J-F. Mestre (16 August 1985)
21. Mazur, B., Ribet, K.: Two-dimensional representations in the arithmetic of modular curves. Astérisque (to appear)
22. Milne, J.: Etude d'une classe d'isogénie. In: Variétés de Shimura et Fonctions L, Breen, L., Labesse, J-P. (eds.) Publ. Math. Univ. Paris VII **6**, 73–81 (1979)
23. Oda, T.: The first de Rham cohomology group and Dieudonné modules. Ann. Sci. Ec. Norm. Sup. IV, Ser. **2**, 63–135 (1969)
24. Raynaud, M.: Spécialisation du foncteur de Picard. Publ. Math., Inst. Hautes Etud. Sci. **38**, 27–76 (1970)
25. Raynaud, M.: Schémas en groupes de type $(p, \ldots, p)$. Bull. Soc. Math. France **102**, 241–280 (1974)
26. Ribet, K.: Sur les variétés abéliennes à multiplications réelles. C.R. Acad. Sc. Paris, Sér. A **291**, 121–123 (1980)
27. Ribet, K.: Mod p Hecke operators and congruences between modular forms. Invent. Math. **71**, 193–205 (1983)

28. Ribet, K.: Congruence relations between modular forms. Proc. Int. Congr. Math. pp. 503–514 (1983)
29. Ribet, K.: Bimodules and abelian surfaces. Adv. Stud. Pure Math. **17**, 359–407 (1989)
30. Ribet, K.: On the component groups and the Shimura subgroup of $J_0(N)$. Sém. Th. Nombres, Université Bordeaux, 1987–88
31. Ribet, K.: Raising the levels of modular representations, Séminaire de Théorie des Nombres, Paris 1987–88. Progr. Math. **81**, 259–271 (1990) .
32. Serre, J-P.: Complex multiplication. In: Algebraic Number Theory, Cassels, JWS, Fröhlich, A. (eds.). Washington, DC: Thompson Book Company 1967
33. Serre, J-P.: Arbres, Amalgames, SL_2. Astérisque **46** (1977). English translation: Trees. Berlin-Heidelberg-New York: Springer 1980
34. Serre, J-P.: Lettre à J-F. Mestre (13 août 1985). Contemp. Math. **67**, 263–268 (1987)
35. Serre, J-P.: Sur les représentations modulaires de degré 2 de $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$. Duke Math. J. **54**, 179–230 (1987)
36. Shimizu, H.: On the zeta functions of quaternion algebras. Ann. Math. **81**, 166–193 (1965)
37. Shimura, G.: Construction of class fields and zeta functions of algebraic curves. Ann. Math. **85**, 58–159 (1967)
38. Shimura, G.: On canonical models of arithmetic quotients of bounded symmetric domains. Ann. Math. **91**, 144–222 (1970)
39. Shimura, G.: Introduction to the Airthmetic Theory of Automorphic Functions. Princeton: Princeton University Press 1971
40. Tate, J.: Endomorphisms of abelian varieties over finite fields. Invent. Math. **2**, 134–144 (1966)
41. Vignéras, M-F.: Arithmétique des Algèbres de Quaternions. (Lecture Notes in Math., Vol. **800**.) Berlin-Heidelberg-New York: Springer 1980
42. Waterhouse, W.C.: Abelian varieties over finite fields. Ann. Sci. Ec. Norm. Sup. IV. Ser. **2**, 521–560 (1969)
[EGA IV] Grothendieck, A.: Etude locale des schémas et des morphismes de schémas (quatrième partie). Publ. Math, Inst. Hautes Etud. Sci. **32**, 5–361 (1967)

Oblatum 27-IX-1988 & 20-XI-1989