IRREDUCIBLE GALOIS REPRESENTATIONS ARISING FROM COMPONENT GROUPS OF JACOBIANS

Kenneth A. Ribet

University of California, Berkeley

1. Introduction

Much has been written about component groups of Néron models of Jacobians of modular curves. In a variety of contexts, these groups have been shown to be "Eisenstein," which implies that they can be neglected in the study of irreducible two-dimensional representations of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$.

The first theorem to this effect may be extracted from Mazur's landmark article [11], which concerns the Jacobian $J_0(N)$ when N is a prime. In this article, Mazur studies the action of Hecke operators on the "cuspidal subgroup" of the Jacobian, and obtains information about the relevant component group as an application [11, p. 98]. More precisely, consider the fiber in characteristic N of the Néron model of $J_0(N)$. This commutative group scheme is an extension of a finite étale group scheme Φ by an algebraic torus; one is interested in the functorial action of Hecke operators on Φ. Mazur proves for all prime numbers $p \neq N$ that the pth Hecke operator T_p acts on Φ by multiplication by $1+p$, and also that T_N is the identity on Φ. The "Eisenstein" terminology arises from the fact that $1+p$ is the pth coefficient of the standard Eisenstein series of weight two on $\Gamma_0(N)$.

In his first article on Serre's conjectures [13], the author generalized Mazur's result to the Jacobian $J_0(N)$ where N is the product of a positive integer M and a prime number q prime to M. According to Theorem 3.12 of [13], one again has the identity $T_p = 1+p$ for all prime numbers p prime to N on the group of connected components of the Néron reduction $J_0(N)_{/\mathbf{F}_q}$. (A slightly more refined statement appears as Theorem 3.22 of [13]; for the proof, see [14].) Subsequently, B. Edixhoven showed in [6] that an analogous result holds for every reduction $J_0(N)_{/\mathbf{F}_q}$ with $q > 3$; here, the new element is that N is allowed to be divisible by an arbitrary power of q.

In another article on Serre's conjectures [15], the author discusses the component group Φ attached to the mod q reduction of the Jacobian of the modular curve derived from $\Gamma_1(N) \cap \Gamma_0(q)$; here N is a positive integer and q is a prime number not dividing N. The analysis of [15], pp. 672–673 proves the identity $T_p = 1+p$ on Φ for all prime numbers $p \nmid qN$ and establishes at the same time that the "diamond bracket" operators $\langle d \rangle$ act as the identity on Φ.

This work was partially supported by NSF Grant #DMS 93-06898. The author wishes to thank B. Edixhoven, H. W. Lenstra, Jr., D. Lorenzini, N. Skoruppa, D. Ulmer, and A. Wilkinson for helpful correspondence and suggestions. We also thank the International Scientific Committee and the local organizers of the Hong Kong conference on Fermat's Last Theorem for their generous invitation.

In this article, we consider the situation in which $\Gamma_1(N)$ is replaced by a subgroup Γ intermediate between $\Gamma_0(N)$ and $\Gamma_1(N)$. In other words, we study the component group Φ_Γ associated to the mod q reduction coming from $\Gamma \cap \Gamma_0(q)$. (We continue to assume that q is prime to N.) Since Φ_Γ is Eisenstein in the two extreme situations $\Gamma = \Gamma_0(N)$ and $\Gamma = \Gamma_1(N)$, it is natural to ask whether Φ_Γ is Eisenstein for intermediate groups.

In order to rule out trivial counterexamples, we will generalize slightly our definition of "Eisenstein." Let $\mathcal{S}$ be the complex vector space of weight-two cusp forms on $\Gamma \cap \Gamma_0(q)$, and let $\widetilde{\mathbb{T}}$ be the subring of $\operatorname{End}\mathcal{S}$ generated by the Hecke operators T_n and $\langle d\rangle$ for n a prime number prime to qN and d prime to N. As we shall recall below, there is a natural action of these operators on Φ_Γ. We shall be interested in the set of maximal ideals $\mathfrak{m}$ of $\widetilde{\mathbb{T}}$ which lie in the support of Φ_Γ as a $\widetilde{\mathbb{T}}$-module, i.e., the set of maximal ideals in the image of $\widetilde{\mathbb{T}}$ in $\operatorname{End}\Phi_\Gamma$.

To each $\mathfrak{m}$, one associates as usual a continuous semisimple representation

$$\rho_{\mathfrak{m}}\colon \operatorname{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathbf{GL}(2, \widetilde{\mathbb{T}}/\mathfrak{m}).$$

This representation is characterized up to isomorphism by the fact that the trace of $\rho_{\mathfrak{m}}(\mathrm{Frob}_p)$ is T_p mod $\mathfrak{m}$ and the determinant of this matrix is $p\langle p\rangle$ mod $\mathfrak{m}$, for all but finitely many prime numbers p. (Here, Frob_p is an arithmetic Frobenius element for p in $\operatorname{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. See, e.g., [15, §7] for some of the relevant background.) It is worth stressing that Φ_Γ gives rise through this construction to a collection of two-dimensional representations of $\operatorname{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, despite the fact there is no natural action of $\operatorname{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ on the group Φ_Γ.

We shall say that Φ_Γ is *Eisenstein* if all $\mathfrak{m}$ in the support of Φ_Γ give rise to representations $\rho_{\mathfrak{m}}$ which are *reducible.* We say that Φ_Γ is *strongly Eisenstein* if the operators $\langle d\rangle$ are trivial on Φ_Γ and one has $T_p = 1+p$ on Φ_Γ for all but finitely many prime numbers p. It is easy to show that "strongly Eisenstein" implies "Eisenstein" by using the Cebotarev Density Theorem and the Brauer-Nesbitt Theorem [13, 5.2c].

To be sure, one's guess that Φ_Γ is Eisenstein turns out to be not very far off the mark. Indeed, Φ_Γ is strongly Eisenstein in most cases, and the prime-to-6 part of Φ_Γ is strongly Eisenstein in *all* cases. Nonetheless, the blanket assertion that Φ_Γ is Eisenstein is definitely false. To convince the reader of this fact, we exhibit in the next section some non-Eisenstein component groups; our construction is a digression which is intended to motivate the more systematic study which follows.

This article's main contribution is an analysis of Φ_Γ in the case of general Γ and q. As we indicated above, the ℓ-primary parts of Φ_Γ are strongly Eisenstein (and cyclic as abelian groups) for all prime numbers $\ell \geq 5$. After recalling this simple result, we investigate the 2-primary and the 3-primary components of Φ_Γ. In case Φ_Γ is non-Eisenstein, we identify the non-Eisenstein "pieces" and describe on these pieces the action of the Hecke operators T_n and $\langle d\rangle$.

From the point of view of Galois representations, our main result is the identification of all irreducible representations with values in $\mathbf{GL}(2, \overline{\mathbf{F}}_2)$ and $\mathbf{GL}(2, \overline{\mathbf{F}}_3)$ that can be associated with component groups. These are induced representations, coming from certain characters $\operatorname{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}(\sqrt{-1})) \to \overline{\mathbf{F}}_2^*$ and $\operatorname{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}(\sqrt{-3})) \to \overline{\mathbf{F}}_3^*$, respectively. For a character θ to intervene in some component group, it is necessary and sufficient that all residue classes modulo its conductor be represented by rational integers.

This article is an outgrowth of the author's talks at the Hong Kong conference on Fermat's Last Theorem. These talks outlined portions of A. Wiles's manuscript [20]. This manuscript provides ample motivation for a detailed analysis of mod 3 representations of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ which arise from modular forms. Indeed, Wiles's attack on the Taniyama-Shimura conjecture begins with a theorem of J. Tunnell [19] which implies that the mod 3 representation of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ arising from an elliptic curve over $\mathbf{Q}$ is associated to some Hecke eigenform. Assuming that this mod 3 representation is irreducible, one shows that the eigenform may be chosen in accordance with the conjectures of [16]. For this, attention must be directed to the special problems posed by mod 3 representations; see F. Diamond's article in this volume [5], which provides an update on Serre's conjectures. In reflecting on mod 3 representations, the author was forced to abandon his "axiom" that component groups are Eisenstein; this led to the study which is presented below.

2. Some non-Eisenstein component groups

Consider the irreducible continuous representation $\rho\colon\ \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathbf{GL}(2, \mathbf{F}_3)$ arising from the space of forms of weight two on $\Gamma_1(13)$. This space has dimension two, and the two Hecke eigenforms in the space are complex conjugates of each other. Their coefficients lie in the ring of integers of $\mathbf{Q}(\sqrt{-3})$; ρ is the mod $(\sqrt{-3})$ representation of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ associated with either of them. The determinant of ρ is the product of the mod 3 cyclotomic character of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ and the character of order two which corresponds to the quadratic extension $\mathbf{Q}(\sqrt{13})$ of $\mathbf{Q}$. Let H be the group of squares in $(\mathbf{Z}/13\mathbf{Z})^*$. Then conjecture $(3.2.4_?)$ of Serre's article [16] predicts that ρ should arise from a Hecke eigenform in the space of weight-two cusp forms on the group

$$\Gamma = \Gamma_H(13) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbf{SL}(2,\mathbf{Z}) \;\middle|\; c \equiv 0 \bmod 13,\ d \in H \right\}.$$

However, as Serre pointed out in a letter to the author [17], this space of forms is zero — the conjecture is false as stated.

One way to deal with this apparent difficulty is to reformulate Serre's conjecture as a relation between mod p Galois representations and mod p modular forms in the sense of Katz [9]. Such a reformulation is presented as Conjecture 4.2 of Edixhoven's article [7], which attributes the reformulation to Serre. The characters which appear in the conjecture are then naturally $\overline{\mathbf{F}}_p^*$-valued, and the difficulty becomes invisible. On the other hand, this solution hides a problem that may be genuinely of interest, since one wants to characterize those spaces of forms which give rise to a given Galois representation.

One certainly knows that problems of the sort exemplified by ρ occur only for mod 2 and mod 3 representations of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. Further, among all mod 3 representations, only those which become abelian on $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}(\sqrt{-3}))$ can give trouble, cf. [2, p. 796]. Finally, let $q > 2$ be a prime number which is congruent to 2 modulo 3. Then the difficulty in the case of ρ "disappears" when the level is augmented by an auxiliary $\Gamma_0(q)$ structure: Lemme 1 of [2] implies that ρ arises from the space of weight-two cusp forms on $\Gamma \cap \Gamma_0(q)$. (The author is grateful to N. Skoruppa for undertaking a numerical verification of this assertion when $q = 5$.)

Let J be the Jacobian of the modular curve over $\mathbf{Q}$ associated with $\Gamma \cap \Gamma_0(q)$. (We again write J for the Néron model of this abelian variety.) As above, we let Φ_Γ be the component group associated with the reduction of J mod q.

Theorem 1. *The group Φ_Γ is non-Eisenstein.*

Proof. Let V be a two-dimensional $\mathbf{F}_3$-vector space affording the representation ρ, and for each $r \nmid 13q$ let $a_r \in \mathbf{F}_3$ be the trace of $\rho(\mathrm{Frob}_r)$, where Frob_r is a Frobenius element for r in $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. The fact that ρ arises from $\Gamma \cap \Gamma_0(q)$ implies that there is a $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$-equivariant embedding $V \hookrightarrow J(\overline{\mathbf{Q}})$ with the following property: For each prime number $r \nmid 13q$, the endomorphism T_r of J acts on V as the homothety a_r. Since q is prime to 39, V is unramified at q. Thus (after choosing a place of $\overline{\mathbf{Q}}$ lying over q), we may view V as embedded in $J_{/\mathbf{F}_q}(\overline{\mathbf{F}}_q)$.

We claim now that V does not land entirely in the connected component $J^o_{/\mathbf{F}_q}$ of $J_{/\mathbf{F}_q}$. In other words, we assert that the image W of V in the group of connected components of $J_{/\mathbf{F}_q}$ is non-trivial. Since the group of connected components in question is none other than Φ_Γ, our claim implies that Φ_Γ contains a non-zero subgroup of exponent 3 on which each Hecke operator T_r acts as a_r. That the a_r are traces of an *irreducible* representation indicates that this subgroup is non-Eisenstein, thereby proving the Theorem.

The claim concerning V is proved by an appeal to results of Deligne-Rapoport [4] and general theorems of Grothendieck and Raynaud. This body of work is summarized in [12], [13, §2], [15, §8], and the discussion which occurs in §3 below. The main point is that by using [4, Th. 6.9, p. 286], one sees that $J^o_{/\mathbf{F}_q}$ is a certain extension of an abelian variety by a torus. The abelian variety in question appears as the product of two copies of the Jacobian of the modular curve associated with the group Γ. However, this modular curve has genus zero, so its Jacobian is zero. Thus $J^o_{/\mathbf{F}_q}$ coincides with its "toric part" T. Therefore, the statement that V falls entirely in $J^o_{/\mathbf{F}_q}(\overline{\mathbf{F}}_q)$ is the statement that V is a subgroup of $T(\overline{\mathbf{F}}_q)$. The argument given at the conclusion of [15, §8] shows that the inclusion $V \hookrightarrow T(\overline{\mathbf{F}}_q)$ is possible only when $q \equiv 1 \bmod 3$; the choice of q thus guarantees that W is non-zero. This proves the claim. □

3. A concrete description of Φ_Γ

In this section, we present a nuts-and-bolts description of Φ_Γ as an abelian group furnished with a family of Hecke operators T_r and $\langle d\rangle$. This material is now quite well known, at least in the case where $\Gamma = \Gamma_0(N)$ [1, 12].

Let N be a positive integer. Subgroups Γ between $\Gamma_1(N)$ and $\Gamma_0(N)$ are in 1-1 correspondence with subgroups of $(\mathbf{Z}/N\mathbf{Z})^*$. Let H be such a subgroup, and set

$$\Gamma = \Gamma_H(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbf{SL}(2,\mathbf{Z}) \;\middle|\; c \equiv 0 \bmod N,\ d \in H \right\}.$$

Thus $\Gamma = \Gamma_1(N)$ in case H is the trivial subgroup of $(\mathbf{Z}/N\mathbf{Z})^*$, while $\Gamma = \Gamma_0(N)$ if $H = (\mathbf{Z}/N\mathbf{Z})^*$. The modular curve corresponding to Γ will be called $X_H(N)$; thus, $X_H(N)$ is the quotient of $X_1(N)$ by the image of H in the Galois group $(\mathbf{Z}/N\mathbf{Z})^*/\{\pm 1\}$ of the covering $X_1(N) \to X_0(N)$. Postponing the assumption that q is prime, we let q be a positive integer prime to N, and put

$$\Gamma(H,q) = \Gamma_H(N) \cap \Gamma_0(q).$$

(A more precise, but less compact, name for this group would have been $\Gamma_H(N,q)$)

The modular curve $X(H,q)$ corresponding to $\Gamma(H,q)$ is the quotient of $X_1(Nq)$ by the image of $H \times (\mathbf{Z}/q\mathbf{Z})^*$ in $(\mathbf{Z}/Nq\mathbf{Z})^*/\{\pm 1\}$. This image is unchanged if we augment H by $\{\pm 1\}$; thus we can, and will, assume that H contains -1. (If $N \leq 2$, we have $-1 = +1$ in $(\mathbf{Z}/N\mathbf{Z})^*$, and we are imposing no condition on H.) We view $X(H,q)$ as classifying elliptic curves E which are furnished with a subgroup C of order q and a point P of order N. In the classification, the point P is considered "mod H" in the sense that the triples (E,C,P) and (E,C,hP) are identified for all $h \in H$. (Compare [4, IV, §3].) The orbit of P mod H will be called α_P; we will say that $X(H,q)$ classifies triples (E,C,α) where α is a point of order N on E which is taken "mod H."

Define $J_H(N)$ and $J(H,q)$ to be the Jacobians of the modular curves $X_H(N)$ and $X(H,q)$, respectively.

From now on, we assume that q is a *prime* number. For convenience, we impose the assumption $q \geq 5$ at this point. (The cases $q = 2$ and $q = 3$ presumably could be included with little modification in what follows.) Consider the reduction of $J(H,q)$ modulo q. The group of components associated with this reduction is the group Φ_Γ in the discussion above; of course, this group depends on q as well as on Γ.

A description of Φ_Γ can be deduced in a standard way from the theorem of Deligne and Rapoport which we cited above [4, Th. 6.9, p. 286]. The theorem provides a model $\mathcal{C}$ of $X(H,q)$ over $\mathbf{Z}_q$ which is an "admissible curve" in the sense of [8, §3] and [13, §2]. The special fiber of $\mathcal{C}$ has two irreducible components, each isomorphic to the modular curve $X_H(N)$.

The set of singular points of $\mathcal{C}_{\overline{\mathbf{F}}_q}$ is in bijection with the set S of supersingular $\overline{\mathbf{F}}_q$-valued points of $X_H(N)$, i.e., those points which arise from pairs (E,P) where E is a supersingular elliptic curve over $\overline{\mathbf{F}}_q$ and P is a point of order N on E. To each $s \in S$ we associate an integer $e(s) \in \{1,2,3\}$ in the following way: If s is represented by the pair (E,P), then $2e(s)$ is the number of automorphisms of E which map P to some point hP with $h \in H$; in other words, $2e(s)$ is the number of automorphisms of (E,α_P). (Because -1 belongs to H, the automorphism "-1" of E induces an automorphism of (E,α_P). The number of such automorphisms is then 2, 4, or 6 because we have assumed $q \geq 5$.) The singular point of $\mathcal{C}$ corresponding to s is then described in $\mathcal{C}$ by the local equation $XY = q^{e(s)}$.

Consider now the diagonal pairing on $\mathbf{Z}^S$ for which $\langle s,s\rangle$ is the positive integer $e(s)$. Let L be the group of degree 0 elements in $\mathbf{Z}^S$, and let $\iota\colon L \hookrightarrow \mathrm{Hom}(L,\mathbf{Z})$ be the linear map which describes the restriction of this pairing to L. The following result is a consequence of the theorem of Deligne and Rapoport and work of Grothendieck and Raynaud. (See [12], and perhaps the discussion in [13, p. 438].)

Theorem 2. *The component group Φ_Γ may be identified with the cokernel of ι.*

One understands that the identification between Φ_Γ and $\operatorname{coker}\iota$ is compatible with the functorial actions of Hecke operators and of the Galois group $\mathrm{Gal}(\overline{\mathbf{F}}_q/\mathbf{F}_q)$. We shall discuss the Hecke operators.

As usual, Hecke operators act on $J(H,q)$ in two different ways, because the Jacobian construction is both covariant and contravariant. In what follows we adopt the contravariant point of view in which $J(H,q)$ is regarded as $\mathrm{Pic}^0(X(H,q))$. We describe the action of Hecke operators on Φ_Γ without supplying any substantial justification. However, the reader may consult [12], which discusses in detail the special case case where $H = (\mathbf{Z}/N\mathbf{Z})^*$.

First, let d be an integer prime to N. The association $(E, C, P) \mapsto (E, C, dP)$ defines a "diamond bracket" automorphism $\langle d\rangle$ on $X(H, q)$. Using the contravariant functoriality, we obtain automorphisms of $J(H, q)$ and then Φ_Γ, both of which we shall call simply $\langle d\rangle$. In the description of Φ_Γ as the cokernel of an injection $L \hookrightarrow \operatorname{Hom}(L, \mathbf{Z})$, the map $\langle d\rangle$ on Φ_Γ is induced from two automorphisms of L. Namely, consider the permutation of S which takes the class of a pair (E, P) to the class of (E, dP). This permutation induces an automorphism $\langle d\rangle_L$ of L, which we regard as a subgroup of $\mathbf{Z}^S$. Let $\langle d\rangle'_L$ be the *inverse* of this permutation. Then we have a commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & L \arrow[r, hook, "\iota"] \arrow[d] & \operatorname{Hom}(L,\mathbf{Z}) \arrow[r] \arrow[d] & \Phi_\Gamma \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & L \arrow[r, hook, "\iota"] & \operatorname{Hom}(L,\mathbf{Z}) \arrow[r] & \Phi_\Gamma \arrow[r] & 0
\end{tikzcd}$$

in which the three vertical arrows are respectively $\langle d\rangle'_L$, $\operatorname{Hom}(\langle d\rangle_L, \mathbf{Z})$ and $\langle d\rangle$.

Similarly, suppose that p is a prime number which does not divide qN. The symbol T_p then denotes a host of objects: the standard Hecke correspondence T_p on $X(H, q)$, the endomorphism of $J(H, q)$ which this correspondence induces by contravariant functoriality, and finally the endomorphism T_p of Φ_Γ which then arises from the functoriality of the Néron model. We seek to identify this latter endomorphism.

Fix p for the moment and let T be the correspondence on S defined by the rule $(E, \alpha) \mapsto \sum(E/D, \alpha \bmod D)$, where the sum is taken over the subgroups D of E having order p. In analogy with the situation above, we write T_L for the induced endomorphism of $L \subset \mathbf{Z}^S$. The analogue of $\langle d\rangle'_L$ is then the endomorphism $T'_L := \langle p\rangle_L^{-1} \circ T_L$. We have a commutative diagram like the one above in which the three vertical arrows are respectively T'_L, $\operatorname{Hom}(T_L, \mathbf{Z})$ and the endomorphism T_p of Φ_Γ. Since p may vary in what follows, we restore p to the notation, referring to the first of these operators as T'_p and the second as $\operatorname{Hom}(T_p, \mathbf{Z})$. In other words, we will permit T_p to denote the endomorphism of L induced from the correspondence $(E, \alpha) \mapsto \sum(E/D, \alpha \bmod D)$ on S by $\mathbf{Z}$-linearity.

4. Extra automorphisms

We will now determine those points $s \in S$ with $e(s) > 1$. A point s in S is defined by a supersingular elliptic curve E over $\overline{\mathbf{F}}_q$, together with a point P on E of order N. Write α for the orbit of P under H and C for the subgroup of E generated by P. Let $\overline{s}$ be the point on $X_0(N)$ defined by (E, C).

Let R be the subring $\mathbf{Z}[\operatorname{Aut} E]$ of $\operatorname{End} E$. If $e(s)$ is different from 1, then $\operatorname{Aut} E$ is different from $\{\pm 1\}$. Since $\operatorname{End}(E)$ is a definite quaternion algebra over $\mathbf{Q}$, $\operatorname{Aut} E$ is different from $\{\pm 1\}$ if and only if E has an automorphism of order 4 or 6. In fact, the condition $q > 3$ implies that the automorphism group of E can only be cyclic of order 2, order 4, or order 6. Hence R is either $\mathbf{Z}$, or else the integer ring in an imaginary quadratic field of discriminant -3 or -4. As is well known, E has an automorphism of order 4 if and only if its j-invariant is 1728. Since E is supersingular, the prime q must be congruent to 3 mod 4. Similarly, E has an automorphism of order 3 if and only if its j-invariant is zero; if the curve with this j-invariant is supersingular, we have $q \equiv 2 \bmod 3$. (Compare, for example, [18], page 103 and pp. 143–144.)

Suppose that $\operatorname{Aut} E \neq \{\pm 1\}$. Then (E, C) has a non-trivial automorphism if and only if $\operatorname{Aut} E$ coincides with its subgroup $\operatorname{Aut}(E, C)$, i.e., if and only if C is stable under R. If this condition is satisfied, then the group C is free of rank 1 over R/I, where I is the annihilator of C in R. Since C is cyclic, this puts a numerical constraint on N: No prime factor of N can remain inert in the ring R, and the prime which ramifies in R can occur in N only to the first power if it occurs at all. Further, the inclusion of $\mathbf{Z}$ in R induces an identification $R/I \xrightarrow{\sim} \mathbf{Z}/N\mathbf{Z}$. Thus the pair (E, C) has a non-trivial automorphism if and only if C is the kernel on E of an ideal I of R such that R/I is isomorphic to $\mathbf{Z}/N\mathbf{Z}$. Thus there is a 1-1 correspondence between cyclic subgroups C of order N which are stable by R and ideals I of R such that the additive group of R/I is cyclic of order N. One sees that distinct subgroups C lead to distinct point of $X_0(N)$. Indeed, if (E, C) and (E, C') are isomorphic, then the isomorphism between them is induced by an automorphism of E, which preserves C (and C') by the definition of R.

The conjugation map $r \mapsto \overline{r}$ of R induces an an involution on the set of I. This Atkin-Lehner style involution has no fixed points if $N > 3$. Indeed, suppose that $I = \overline{I}$. For each $r \in R$, there is an integer n such that $r - n$ lies in I. Since $\overline{n} = n$, $r - \overline{r}$ belongs to $I + \overline{I} = I$. Hence I contains $\sqrt{-3}$ or 2, according as the discriminant of R is -3 or -4. Hence N divides 3 in the former case and N divides 2 in the latter.

Suppose now that (E, C) has a non-trivial automorphism. Then $e(s) > 1$ if and only if $\operatorname{Aut}(E, \alpha) = \operatorname{Aut}(E, C)$. This equality translates into the statement that

$$(*) \qquad \mu \overset{?}{\subseteq} H \subseteq (\mathbf{Z}/N\mathbf{Z})^*,$$

where μ is the image in $(R/I)^*$ of the unit group of R. This condition involves only (E, C) and H; hence it applies simultaneously to all points on $X_H(N)$ which lie above the point $\overline{s}$ on $X_0(N)$. One checks that when $(*)$ is satisfied, the number of points on $X_H(N)$ which lie above $\overline{s}$ is precisely $((\mathbf{Z}/N\mathbf{Z})^* : H)$.

In summary, to find those points $s \in S$ with $e(s) > 1$, we first look for the supersingular points $\overline{s}$ in $X_0(N)(\overline{\mathbf{F}}_q)$ which satisfy the analogous condition $e(\overline{s}) > 1$. Mark off those points (if any) which satisfy the supplementary condition $(*)$. Above each marked point, we find $((\mathbf{Z}/N\mathbf{Z})^* : H)$ points in S with "extra automorphisms."

The condition $(*)$ may be true for some points $\overline{s}$ with $e(\overline{s}) > 1$ that arise from a given supersingular elliptic curve and false for others. For example, suppose that E has six automorphisms and that $N = 7 \cdot 13 = 91$. There are four ideals I of R with $R/I \approx \mathbf{Z}/91\mathbf{Z}$. For two of these ideals, the image of R^* in $(\mathbf{Z}/91\mathbf{Z})^*$ is the cyclic group generated by 10; for the other two, the image is generated by 17. If H is one of these two groups, then $(*)$ will be satisfied for two of the I, but not for all. Notice, however, that the set of I for which $(*)$ is satisfied is stable under the natural conjugation map on R. Indeed, R^* is stable under this conjugation. Furthermore, we have observed that the inequality $N > 3$ implies that an ideal I with $R/I \approx \mathbf{Z}/N\mathbf{Z}$ can never be its own conjugate. This gives

Lemma 1. *Suppose that $N \geq 4$. Then the set of points $\overline{s}$ for which $e(\overline{s}) > 1$ and for which $(*)$ is satisfied has an even number of elements. In particular, the number of such points is different from 1.*

The case $N \leq 3$ does not play an important role in the analysis which follows. In fact, one has

Lemma 2. *If $N \leq 12$ and there is at least one point s with $e(s) > 1$, then $H = (\mathbf{Z}/N\mathbf{Z})^*$.*

Proof. Assume that $N < 13$. If $e(s) = 3$, then there is an ideal I of $R = \mathbf{Z}[\frac{1+\sqrt{-3}}{2}]$ with $R/I \approx \mathbf{Z}/N\mathbf{Z}$. This implies that N is 3 or 7. In both cases, R^* maps onto $(\mathbf{Z}/N\mathbf{Z})^*$. If $e(s) = 2$, there is an ideal I of $R = Z[\sqrt{-1}]$ with $R/I \approx \mathbf{Z}/N\mathbf{Z}$. The possibilities for N are 2, 5, and 10. Again, R^* maps onto $(\mathbf{Z}/N\mathbf{Z})^*$ in all cases. □

The prime 13 splits both in $\mathbf{Z}[\frac{1+\sqrt{-3}}{2}]$ and in $Z[\sqrt{-1}]$. If R is one of these two rings, and if I is a prime lying over 13 in R, then the image of R^* in $(\mathbf{Z}/13\mathbf{Z})^*$ is strictly smaller than $(\mathbf{Z}/13\mathbf{Z})^*$. This circumstance (if not the discussion in §2) shows that 12 cannot be replaced by a larger integer in the statement of the Lemma.

5. A canonical subgroup of Φ_Γ

Let $\Phi = \Phi_\Gamma$. We shall discuss a cyclic subgroup Φ_0 of Φ which has already been studied in case $\Gamma = \Gamma_0(N)$ (see [13] and [12]).

For each element s of S, let $\varphi_s \colon L \to \mathbf{Z}$ be the linear form $\ell \mapsto \langle \ell, s\rangle$ and let ω_s be the linear form on L

$$\sum_t n_t t \mapsto n_s.$$

Clearly, $\mathrm{Hom}(L, \mathbf{Z})$ is generated by the ω_s, so that Φ is generated by their images $\overline{\omega}_s$ in $\Phi = \mathrm{Hom}(L, \mathbf{Z})/L$. One has $e(s)\omega(s) = \varphi_s$.

The class $\overline{\varphi}$ of φ_s in $\Phi = \mathrm{Hom}(L, \mathbf{Z})/L$ is independent of s, since $\varphi_s - \varphi_t$ is the image in $\mathrm{Hom}(L, \mathbf{Z})$ of $s - t \in L$, if $s, t \in S$. Let Φ_0 be the subgroup of Φ generated by the canonically given element $\overline{\varphi}$. We set

$$Q = \Phi/\Phi_0.$$

In view of the formula $e(s)\omega(s) = \varphi_s$, we have $e(s)\overline{\omega}_s = \overline{\varphi}$ for each s. Hence, as noted in [13, §2], we have a surjection

$$\bigoplus_{s \in S} (\mathbf{Z}/e(s)\mathbf{Z}) \longrightarrow Q, \qquad (a_s) \mapsto \sum_s a_s \overline{\omega}_s.$$

One may view $\mathbf{Z}^S$ as embedded in $\mathrm{Hom}(\mathbf{Z}^S, \mathbf{Z})$ via the symmetric bilinear pairing $\langle\, ,\rangle$ on $\mathbf{Z}^S$. Let $L^\perp \subset \mathrm{Hom}(\mathbf{Z}^S, \mathbf{Z})$ be the group of linear forms which vanish on L, and let $U = L^\perp \cap \mathbf{Z}^S$ be group of vectors in $\mathbf{Z}^S$ which are orthogonal to L under the pairing. Since $\mathrm{Hom}(L, \mathbf{Z}) = \mathrm{Hom}(\mathbf{Z}^S, \mathbf{Z})/L^\perp$, we have $\Phi = \mathrm{Hom}(\mathbf{Z}^S, \mathbf{Z})/(L \oplus L^\perp)$. The image of $\mathbf{Z}^S/U$ in Φ, i.e., the group $\mathbf{Z}^S/(L \oplus U)$, is clearly Φ_0. (Indeed, the image of $s \in \mathbf{Z}^S$ in $\mathrm{Hom}(\mathbf{Z}^S, \mathbf{Z})$ is φ_s.)

Now U is free of rank one over $\mathbf{Z}$; it consists of those multiples of $\sum \frac{1}{e(s)} s \in \mathbf{Q}^S$ which lie in $\mathbf{Z}^S$. Hence U is generated by $\sum \frac{m}{e(s)} s$, where m is the least common multiple of the $e(s)$. (Thus, m divides 6.) It follows that the order of $\Phi_0 = \mathbf{Z}^S/(L \oplus U)$ is $m \cdot \sum e(s)^{-1}$, cf. [12, p. 16]. Also, $L^\perp/U$ has order m, since $L^\perp$ is generated by the element $\sum \omega_s$ and since $m \sum \omega_s = \sum \frac{m}{e(s)} s$ in $\mathrm{Hom}(\mathbf{Z}^S, \mathbf{Z})$.

Consider the commutative diagram with exact rows

$$\begin{tikzcd}
0 \arrow[r] & L^\perp \arrow[r] & \mathrm{Hom}(\mathbf{Z}^S, \mathbf{Z}) \arrow[r] & \mathrm{Hom}(\mathbf{Z}^S, \mathbf{Z})/L^\perp \arrow[r] & 0 \\
0 \arrow[r] & U \arrow[r] \arrow[u] & \mathbf{Z}^S \arrow[r] \arrow[u] & \mathbf{Z}^S/U \arrow[r] \arrow[u] & 0
\end{tikzcd}$$

in which the central vertical map is the inclusion given by $\langle\,,\,\rangle$; the two other vertical maps are the evident, related inclusions. The cokernels of the vertical maps form the exact sequence $0 \to \mathbf{Z}/m\mathbf{Z} \to \bigoplus_{s\in S}(\mathbf{Z}/e(s)\mathbf{Z}) \to Q \to 0$, where the map from $m\mathbf{Z}$ to the direct sum takes $1 \in \mathbf{Z}/m\mathbf{Z}$ to the vector $(1,\ldots,1)$. Note that Q is now seen to have order $m^{-1}\prod e(s)$. Therefore, we recover the formula $\left(\prod_s e(s)\right)\cdot\left(\sum_s e(s)^{-1}\right)$ for the order of Φ, cf. [1, Ch. 9, Prop. 10].

Lemma 3. *The group Φ_0 is strongly Eisenstein. The identities $\langle d\rangle = 1$ and $T_p = 1+p$ hold on Φ_0 for $d \in (\mathbf{Z}/N\mathbf{Z})^*$ and p prime to qN.*

Proof. We first consider the action of T_p on $\overline{\varphi}$. Choose $s \in S$. From the perspective introduced at the end of §3, we see that the action of T_p on this element of Φ is derived from the action of $\mathrm{Hom}(T_L, \mathbf{Z})$ on $\varphi_s \in \mathrm{Hom}(L, \mathbf{Z})$. The map $\varphi_s \circ T_L$ is the linear form mapping $\ell \in L$ to $\langle T_L\ell, s\rangle = \langle \ell, T_L' s\rangle = \langle \ell, \langle p\rangle^{-1}T_L s\rangle$. Since $\langle p\rangle^{-1}T_L s$ is an element of $\mathbf{Z}^S$ of degree $p+1$, the image in Φ of $\ell \mapsto \langle \ell, \langle p\rangle^{-1}T_L s\rangle$ is $(p+1)\overline{\varphi}$. This establishes the first identity. The second is proved by an analogous computation. □

Corollary. *The group Φ is Eisenstein in each of the following situations:*
(i) $e(s) = 1$ *for all* $s \in S$*;*
(ii) $H = (\mathbf{Z}/N\mathbf{Z})^*$*;*
(iii) $N < 13$*;*
(iv) $H = \{\pm 1\}$.

Proof. In the first case, we have $\Phi_0 = \Phi$, so that the assertion to be proved is that given by the lemma. The assertion in the second case is given as Theorem 3.12 in [13]. In the third case, we are either in case (i) or case (ii) by Lemma 2. Suppose now that we are in the fourth case, which corresponds to the equality $X_H(N) = X_1(N)$. If N is at least 4, we are in case (i) by [10, Corollary 2.7.4]. If $N \leq 4$, then we are of course in case (iii). □

6. The structure of Q

In view of the Corollary above, we will now impose the condition $N \geq 13$.

Lemma 4. *Suppose that (E, C) represents a supersingular point of $X_0(N)_{/\overline{\mathbf{F}}_q}$. Let D be a cyclic subgroup of $E(\overline{\mathbf{F}}_q)$ of order prime to qN. Assume that the automorphism group of the triple (E, C, D) is larger than $\{\pm 1\}$. Then the pair $(E/D, C \bmod D)$ is isomorphic to (E, C).*

Proof. This statement is proved as Proposition 2 in [14]; we recall the proof for the convenience of the reader. Let ϵ be an automorphism of (E, C, D) which is different from ± 1, and let R be the subring of $\mathrm{End}(E, C, D)$ which is generated by ϵ. Thus R is isomorphic either to the ring of Gaussian integers or to the ring of integers of $\mathbf{Q}(\sqrt{-3})$. If $J = \mathrm{Ann}_R(D)$, then J is a principal ideal (r) of R, and D is the kernel of J on E. Thus the map "multiplication by r" on E induces an isomorphism $(E/D, (C \oplus D)/D) \xrightarrow{\sim} (E, C)$ as required. □

Recall now that Q is generated as an abelian group by the elements $\overline{\omega}_s$ with $s \in S$. Since $e(s)\overline{\omega}_s = 0$, it suffices to consider only those $\overline{\omega}_s$ with $e(s) > 1$. As we have seen, the inequality $e(s) > 1$ means that s lies over a supersingular point $\overline{s}$ of $X_0(N)(\overline{\mathbf{F}}_q)$ which satisfies the numerical condition $e(\overline{s}) > 1$ and the supplementary condition $(*)$.

Let $\overline{s}$ be such a point. Define $Q_{\overline{s}}$ to be the subgroup of Q generated by the $\overline{\omega}_s$ with s lying over $\overline{s}$. Thus $Q_{\overline{s}}$ is a quotient of the elementary abelian group $\bigoplus(\mathbf{Z}/e(\overline{s})\mathbf{Z})$, where the sum is extended over the set of points s lying over $\overline{s}$. As was mentioned above, the number of such points is the index $((\mathbf{Z}/N\mathbf{Z})^* : H)$. More precisely, the set of points s is a principal homogeneous space over $(\mathbf{Z}/N\mathbf{Z})^*/H$, the action of this group being given by the "diamond bracket" operators.

Proposition 1. *The group $Q_{\overline{s}}$ is free of rank $((\mathbf{Z}/N\mathbf{Z})^* : H)$ over $\mathbf{Z}/e(\overline{s})\mathbf{Z}$.*

Proof. Let S_0 be the inverse image of $\overline{s}$ in S. We must show that the direct sum $\bigoplus_{s\in S_0}(\mathbf{Z}/e(s)\mathbf{Z})$ has trivial intersection with the kernel of the map

$$\bigoplus_{s\in S}(\mathbf{Z}/e(s)\mathbf{Z}) \to Q.$$

As we have seen, this kernel is the cyclic group generated by the vector $(1,\dots,1)$ in the full direct sum. Hence it suffices to check that there is a point $s \in S \setminus S_0$ with $e(s) > 1$. This follows from Lemma 1, since $N \geq 13$. □

Proposition 2. *The subgroup $Q_{\overline{s}}$ of Q is stable under the Hecke operators T_p and $\langle d\rangle$.*

Proof. Let p be a prime number not dividing qN. As at the end of §3, we write T for the correspondence on S defined by the formula $(E,\alpha) \mapsto \sum(E/D, \alpha \bmod D)$. This correspondence is summarized by the matrix of natural numbers (a_{tu}) which one constructs by writing $Tu = \sum_{t\in S} a_{tu}\cdot t$ for $u \in S$. Recall that the action of T_p on Φ arises from the action of a map labeled $\mathrm{Hom}(T_L,\mathbf{Z})$ on $\mathrm{Hom}(L,\mathbf{Z})$. This group is generated by the elements ω_s for $s \in S$, and one finds that $\mathrm{Hom}(T_L,\mathbf{Z})$ maps ω_s to the sum $\sum_{t\in S} a_{st}\omega_t$.

To prove that $Q_{\overline{s}}$ is stable under T_p, it suffices to show that a_{st} is divisible by $e(t)$ whenever s maps to $\overline{s}$ and t does *not*. In other words, we wish to show that a_{tu} is divisible by $e(u)$ whenever t and u have distinct images on $X_0(N)$.

This divisibility can be established by the method used to prove [13, Th. 3.12]. Indeed, suppose that u is represented by (E,α). Let C be the cyclic subgroup of order N on E which is associated with α. The group $\mathrm{Aut}(E,\alpha)/\{\pm1\}$ operates on the set of cyclic subgroups of E of order p. Clearly, if D and D' are such subgroups which are equivalent under this action, then $(E/D, \alpha \bmod D)$ and $(E/D', \alpha \bmod D')$ are isomorphic. Moreover, suppose that the cyclic subgroup D has a non-trivial stabilizer under this action. Then Lemma 4 shows that (E,C) and $(E/D, (C\oplus D)/D)$ are isomorphic, i.e., that (E,α) and $(E/D, \alpha \bmod D)$ map down to the same point on $X_0(N)$. Now let t be a point of S whose image on $X_0(N)$ is distinct from that of s. Then the set of D for which $(E/D, \alpha \bmod D)$ represents t is a union of copies of the group $\mathrm{Aut}(E,\alpha)/\{\pm1\}$, whose cardinality is $e(u)$. Hence a_{tu} is divisible by $e(u)$, as was claimed.

Now let d be an integer prime to N. The action of $\langle d\rangle$ on Φ is deduced from the automorphism $\mathrm{Hom}(\langle d\rangle_L,\mathbf{Z})$ introduced at the end of §3. This automorphism maps a given linear form ω_s to the linear form $\omega_{\langle d\rangle^{-1}s}$. Here, the automorphism labeled $\langle d\rangle^{-1}$ sends the class of (E,P) to the class of $(E, d^{-1}P)$; the quantity d^{-1} is computed mod N. Since P and $d^{-1}P$ generated the same subgroup of E, it is clear that $\langle d\rangle$ permutes the $\overline{\omega}_s$ with s having a given image on $X_0(N)$. Therefore, $\langle d\rangle$ preserves $Q_{\overline{s}}$. □

Let S_0 again be the inverse image of $\overline{s}$ in S. We observed above that the diamond bracket operation of $(\mathbf{Z}/N\mathbf{Z})^*$ on S_0 makes S_0 a principal homogeneous space over the group $\Delta := (\mathbf{Z}/N\mathbf{Z})^*/H$. Let us identify $Q_{\overline{s}}$ with the direct sum $\bigoplus_{s\in S_0}(\mathbf{Z}/e(\overline{s})\mathbf{Z})$, i.e., with the space of functions from S_0 to $\mathbf{Z}/e(\overline{s})\mathbf{Z}$. Then the diamond bracket operation discussed in Proposition 2, which involves an inverse, may be viewed as the natural action coming from the diamond bracket action of Δ on S_0.

Let $\ell = e(\overline{s})$; thus $\ell = 2$ or $\ell = 3$. Let $\mathbb{T} = \mathbf{F}_\ell[\Delta]$ be the group algebra consisting of sums $\sum_{\delta\in\Delta} n_\delta[\delta]$ where the n_δ are integers mod ℓ. Since $Q_{\overline{s}}$ is an $\mathbf{F}_\ell$-vector space with an action of Δ, $Q_{\overline{s}}$ may be viewed as a $\mathbb{T}$-module in a natural way.

Lemma 5. *The $\mathbb{T}$-module $Q_{\overline{s}}$ is free of rank one.*

Proof. Proposition 1 shows that $Q_{\overline{s}}$ is an $\mathbf{F}_\ell$ vector space of dimension $\#(\Delta) = \dim_{\mathbf{F}_\ell}\mathbb{T}$. Further, it is clear that $Q_{\overline{s}}$ is a cyclic $\mathbb{T}$-module, since Δ permutes the generators ω_s of $Q_{\overline{s}}$. □

Now choose a supersingular elliptic curve E over $\overline{\mathbf{F}}_q$ and a cyclic subgroup C on E so that the pair (E, C) defines the point $\overline{s}$ of $X_0(N)$. As usual, let R be the ring $\mathbf{Z}[\operatorname{Aut} E]$, and let I be the annihilator of C in R. The isomorphism $R/I \approx (\mathbf{Z}/N\mathbf{Z})^*$ gives a meaning to $[r]$ whenever $r \in R$ is prime to I. The element $[r]$ depends only on the ideal generated by r in R, since H contains the image of R^* in $(\mathbf{Z}/N\mathbf{Z})^*$.

In fact, this might be a good time to relate Δ to the Galois group $\operatorname{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. Let K be the imaginary quadratic field $\mathbf{Q}[\operatorname{Aut} E] = R \otimes \mathbf{Q}$. Since all fractional ideals of K are principal, the quotient of $(R/I)^*$ by R^* is the ray class group of K with conductor I. Via class field theory, this class group corresponds with an abelian extension L of K. It will be useful to fix an embedding $K \hookrightarrow \overline{\mathbf{Q}}$ and to view L as a subfield of $\overline{\mathbf{Q}}$. Since Δ is then a quotient of $\operatorname{Gal}(L/K)$, Δ becomes the Galois group of an abelian extension of K in $\overline{\mathbf{Q}}$. The conductor of this extension divides I.

For each prime $p \nmid qN$, we define an element τ_p of $\mathbb{T}$ by the formula:

$$\tau_p = \begin{cases} 0 & \text{if } p \text{ is inert in } R, \\ [\pi] + [\pi'] & \text{if } p = (\pi)(\pi') \text{ is split in } R, \\ [\pi] & \text{if } p = (\pi)^2 \text{ is ramified in } R. \end{cases}$$

The third case occurs only when $p = \ell$.

Theorem 3. *For each $p \nmid qN$, the Hecke operator T_p acts on $Q_{\overline{s}}$ by multiplication by τ_p.*

Proof. Let (a_{st}) be the Brandt matrix which was introduced in the course of the proof of Proposition 2. Recall that if t is the isomorphism class of the pair (E, P), where P is a point of order N lying in C, then a_{st} is the number of subgroups D of order p in E such that $(E/D, P \bmod D)$ defines s. We have seen that $a_{st} \equiv 0 \bmod \ell$ if s and t do not have the same image on $X_0(N)$. We must now calculate $a_{st} \bmod \ell$ in the case where s and t have the same image, namely $\overline{s}$.

Suppose first that p is inert in R. Then there is no subgroup of order p in E which is stable under $\operatorname{Aut} E$. Accordingly, the proof of Proposition 2 shows that a_{st} is divisible by ℓ, since the group $(\operatorname{Aut} E)/\{\pm 1\}$ acts freely on the set of D for which $(E/D, P \bmod D)$ defines s.

Next, let $p = (\pi)^2$ be ramified in R. Then $E[\pi]$ is the unique subgroup of order p on E which is stable under R. The pair $(E/D, P \bmod D)$ is isomorphic to $(E, \pi \cdot P)$ via π. With the obvious meaning of $\langle\pi\rangle$, we may write $a_{st} \equiv 0 \bmod \ell$ for $s \neq \langle\pi\rangle t$, while $a_{st} \equiv 1 \bmod \ell$ for $s = \langle\pi\rangle t$. Tracing through the definitions, one emerges with the desired assertion that T_p operates on $Q_{\overline{s}}$ as $[\pi]$.

In the final case where $p = (\pi)(\pi')$, there are two distinct subgroups D which are stable under $\operatorname{Aut} E$. The corresponding quotients of (E, α) are represented by $(E, \pi \cdot P)$ and $(E, \pi' \cdot P)$. Let $s_1 = \langle\pi\rangle t$ and $s_2 = \langle\pi'\rangle t$. If the two s_i are distinct, the numbers $a_{st} \bmod \ell$ are 1 for $s = s_1, s_2$ and zero otherwise. If $s_1 = s_2$, then $a_{st} = 2$ when $s = s_1 = s_2$ and $a_{st} = 0$ otherwise. This leads to the required formula $T_p = [\pi] + [\pi']$. □

Let $\widetilde{\mathbb{T}}$ be the subring of $\operatorname{End} J(H, q)$ generated by the endomorphisms T_p and $\langle d\rangle$ of $J(H, q)$. (There is a functorial, faithful action of $\widetilde{\mathbb{T}}$ on the space of weight-two cusp forms for $\Gamma \cap \Gamma_0(q)$; thus $\widetilde{\mathbb{T}}$ may be defined alternatively as in the Introduction.) Theorem 3 states that the action of $\widetilde{\mathbb{T}}$ on $Q_{\overline{s}}$ factors through the action of $\mathbb{T}$ on $Q_{\overline{s}}$, in such a way that $\langle d\rangle \in \widetilde{\mathbb{T}}$ acts as $[d] \in \mathbb{T}$ for all $d \in (\mathbf{Z}/N\mathbf{Z})^*$ that $T_p \in \widetilde{\mathbb{T}}$ acts as τ_p. Equivalently, there is a commutative triangle

$$\begin{tikzcd}
\widetilde{\mathbb{T}} \arrow[rr] \arrow[dr] & & \mathbb{T} \arrow[dl] \\
& \operatorname{End} Q_{\overline{s}} &
\end{tikzcd}$$

in which the left-hand diagonal arrow describes the action of Hecke operators on $Q_{\overline{s}}$ and the right-hand diagonal arrow is the structural map making $Q_{\overline{s}}$ into a $\mathbb{T}$-module. The horizontal arrow is visibly surjective, since $\mathbb{T} = \mathbf{F}_\ell[\Delta]$ is generated by the various $[d]$. By Lemma 5, $Q_{\overline{s}}$ is a free rank-one $\mathbb{T}$-module. Therefore, the map $\mathbb{T} \to \operatorname{End} Q_{\overline{s}}$ is injective. Accordingly, the image of $\widetilde{\mathbb{T}}$ in $\operatorname{End} Q_{\overline{s}}$ may be identified with $\mathbb{T}$. Via this identification, the set of maximal ideals of $\widetilde{\mathbb{T}}$ in the support of $Q_{\overline{s}}$ becomes the set of maximal ideals of $\mathbb{T} = \mathbf{F}_\ell[\Delta]$.

This latter set may be viewed as a set of conjugacy classes of characters. Indeed, if $\mathfrak{m}$ is a maximal ideal of $\mathbb{T}$, then $\mathbb{T}/\mathfrak{m}$ is a finite field of characteristic ℓ. Hence $\mathfrak{m}$ may be obtained as the kernel of some ring homomorphism $\mathbb{T} \to \overline{\mathbf{F}}_\ell$. On the other hand, restriction to Δ yields a 1-1 correspondence between ring homomorphisms $\mathbb{T} \to \overline{\mathbf{F}}_\ell$ and group homomorphisms $\theta\colon \Delta \to \overline{\mathbf{F}}_\ell^*$. By Galois theory, two ring homomorphisms $\mathbb{T} \rightrightarrows \overline{\mathbf{F}}_\ell$ have the same kernel if and only if they are conjugate under $\operatorname{Gal}(\overline{\mathbf{F}}_\ell/\mathbf{F}_\ell)$. It follows that the set of maximal ideals of $\mathbb{T}$ is in correspondence with the set of $\operatorname{Gal}(\overline{\mathbf{F}}_\ell/\mathbf{F}_\ell)$-conjugacy classes of characters θ.

As was noted above, Δ may be viewed as the Galois group of an abelian extension of K in $\overline{\mathbf{Q}}$. Accordingly, the characters θ become homomorphisms $\operatorname{Gal}(\overline{\mathbf{Q}}/K) \to \overline{\mathbf{F}}_\ell^*$ which factor through the Galois group we called $\operatorname{Gal}(L/K)$. For each such homomorphism, we let θ' be the map $\operatorname{Gal}(\overline{\mathbf{Q}}/K) \to \overline{\mathbf{F}}_\ell^*$ defined by

$$\theta'(x) = \theta(gxg^{-1}),$$

where g is an element of $\operatorname{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ which does not belong to $\operatorname{Gal}(\overline{\mathbf{Q}}/K)$.

Lemma 6. *We have $\theta = \theta'$ if and only if θ is identically 1.*

Proof. If θ is identically 1, it certainly coincides with θ'. Conversely, suppose that $\theta = \theta'$. Let $\mathfrak{f}$ be the conductor of θ. As is well known, the conductor of θ' is the image of $\mathfrak{f}$ under the non-trivial involution $K \to K$. Because $\theta = \theta'$, $\mathfrak{f}$ is invariant under this involution. It is in any case a divisor of I. It follows that $\mathfrak{f}$ divides $(\sqrt{-3})$ in the case where $K = \mathbf{Q}(\sqrt{-3})$ and that $\mathfrak{f}$ divides $(1+\sqrt{-1})$ in case $K = \mathbf{Q}(\sqrt{-1})$. In the former case, θ is a map $\mathbf{F}_3^* \to \overline{\mathbf{F}}_3^*$ which is trivial on $\{\pm 1\}$. In the latter case, θ is a map $\mathbf{F}_2^* \to \overline{\mathbf{F}}_2^*$. Hence θ is the trivial map in either case. □

Now let $\operatorname{Ind}\theta$ be the induced representation

$$\operatorname{Ind}_{\mathrm{Gal}(\overline{\mathbf{Q}}/K)}^{\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})}\theta\colon\ \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathbf{GL}(2, \overline{\mathbf{F}}_\ell).$$

We can make an explicit model for $\operatorname{Ind}\theta$ by choosing $g \notin \mathrm{Gal}(\overline{\mathbf{Q}}/K)$ as above and defining

$$\operatorname{Ind}\theta(x) = \begin{cases} \begin{pmatrix} \theta(x) & 0 \\ 0 & \theta'(x) \end{pmatrix} & \text{for } x \in \mathrm{Gal}(\overline{\mathbf{Q}}/K), \\ \begin{pmatrix} 0 & \theta(xg) \\ \theta(g^{-1}x) & 0 \end{pmatrix} & \text{for } x \notin \mathrm{Gal}(\overline{\mathbf{Q}}/K). \end{cases}$$

In particular, one reads from this model the well known formula

$$\mathrm{tr}(\operatorname{Ind}\theta(x)) = \begin{cases} \theta(x) + \theta'(x) & \text{if } x \in \mathrm{Gal}(\overline{\mathbf{Q}}/K), \\ 0 & \text{if } x \notin \mathrm{Gal}(\overline{\mathbf{Q}}/K) \end{cases}$$

for the trace of $\operatorname{Ind}\theta$. The determinant of $\operatorname{Ind}\theta$ is the product of two characters, the first of which is the homomorphism $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \{\pm 1\}$ which corresponds to the quadratic subfield K of $\overline{\mathbf{Q}}$. This homomorphism may be described alternatively as the mod ℓ cyclotomic character χ_ℓ which gives the action of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ on the group of ℓth roots of 1 in $\overline{\mathbf{Q}}$. It has order two if $\ell = 3$, while it is trivial if $\ell = 2$. The second of the two characters is $\theta \circ \mathrm{Ver}$, where Ver is the Verlagerung map from $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ to the abelianization of $\mathrm{Gal}(\overline{\mathbf{Q}}/K)$. It is obtained by composing: the mod N cyclotomic character $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to (\mathbf{Z}/N\mathbf{Z})^*$, the identification $(\mathbf{Z}/N\mathbf{Z})^* \xrightarrow{\sim} (R/I)^*$, and the character $\theta\colon (R/I)^* \to \overline{\mathbf{F}}_\ell^*$.

Lemma 7. *If θ is non-trivial, the representation* $\operatorname{Ind}\theta$ *is irreducible. Suppose instead that θ is trivial. Then the image of* $\operatorname{Ind}\theta$ *has order two; the kernel of* $\operatorname{Ind}\theta$ *is* $\mathrm{Gal}(\overline{\mathbf{Q}}/K)$. *When $\ell = 3$,* $\operatorname{Ind}\theta$ *is the direct sum of the trivial representation and the one-dimensional representation with character χ_3. When $\ell = 2$,* $\operatorname{Ind}\theta$ *is indecomposable and its semisimplification is the direct sum of two copies of the trivial representation.*

Proof. Suppose that θ is non-trivial. Then by Lemma 6, θ and θ' are distinct. The restriction of $\operatorname{Ind}\theta$ to $\mathrm{Gal}(\overline{\mathbf{Q}}/K)$ is thus the direct sum of two *distinct* characters. It follows that there are precisely two lines in the representation space of $\operatorname{Ind}\theta$ which are invariant under $\mathrm{Gal}(\overline{\mathbf{Q}}/K)$. These lines are permuted by the element g; in particular, no line is stable under the full Galois group $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. If θ is trivial, then the required assertions are clear from the model of $\operatorname{Ind}\theta$ presented above. □

Note that, in the case where $\ell = 2$ and $\theta = 1$, the representation $\operatorname{Ind}\theta$ is that given by the unique non-trivial extension of $\mathbf{Z}/2\mathbf{Z}$ by μ_2 in the category of commutative group schemes of type $(2, \ldots, 2)$ over $\operatorname{Spec}\mathbf{Z}$. (See [11, Ch. II, §12].)

Let $\mathfrak{m}$ be the maximal ideal of $\widetilde{\mathbb{T}}$ arising from θ. The quotient $\widetilde{\mathbb{T}}/\mathfrak{m}$ becomes a subfield of $\overline{\mathbf{F}}_\ell$ via the embedding $\widetilde{\mathbb{T}}/\mathfrak{m} \hookrightarrow \overline{\mathbf{F}}_\ell$ induced by θ. To θ we associate the representation

$$\rho_\theta = \rho_{\mathfrak{m}} \otimes_{\widetilde{\mathbb{T}}/\mathfrak{m}} \overline{\mathbf{F}}_\ell \colon \operatorname{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathbf{GL}(2, \overline{\mathbf{F}}_\ell)$$

obtained by composing $\rho_{\mathfrak{m}}$ with the inclusion $\mathbf{GL}(2, \widetilde{\mathbb{T}}/\mathfrak{m}) \hookrightarrow \mathbf{GL}(2, \overline{\mathbf{F}}_\ell)$. By varying θ over the set of characters $\Delta \to \overline{\mathbf{F}}_\ell^*$, we obtain from $Q_{\overline{s}}$ a family of representations $\operatorname{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \overline{\mathbf{F}}_\ell^*$. We seek to describe this family.

Proposition 3. *Let p be a prime number which does not divide $qN\ell$. Then the trace of $\rho_\theta(\operatorname{Frob}_p)$ is*

$$\begin{cases} 0 & \text{if } p \text{ is inert in } K, \\ \theta(\pi) + \theta(\pi') & \text{if } p = (\pi)(\pi') \text{ is split in } K, \end{cases}$$

while the determinant of $\rho_\theta(\operatorname{Frob}_p)$ is $p\theta(p) = \pm\theta(p)$.

Proof. The matrix $\rho_{\mathfrak{m}}(\operatorname{Frob}_p)$ has trace $T_p \bmod \mathfrak{m}$ and determinant $p\langle p\rangle$. Viewing $\widetilde{\mathbb{T}}/\mathfrak{m}$ as a quotient of $\mathbb{T}$, we can replace $\langle p\rangle$ by $[p]$ and T_p by τ_p. The map θ sends each $[\delta] \in \mathbb{T}$ to $\theta(\delta)$. The desired formulas now follow. □

Theorem 4. *For each θ, ρ_θ is the semisimplification of the induced representation $\operatorname{Ind}\theta$.*

Proof. This follows easily from Proposition 3, the Cebotarev Density Theorem, the Brauer-Nesbitt Theorem and the formulas given above for the trace and determinant of $\operatorname{Ind}\theta$. □

It is time now to recapitulate. The group $Q = \Phi/\Phi_0$ is the sum of subgroups $Q_{\overline{s}}$ belonging to the supersingular points $\overline{s}$ of $X_0(N)(\overline{\mathbf{F}}_q)$ which have extra automorphisms and which satisfy the condition $(*)$ of §4. To each such point is associated one of the quadratic fields $\mathbf{Q}(\sqrt{-3})$, $\mathbf{Q}(\sqrt{-1})$; call this field K. The point $\overline{s}$ and the group H determine an abelian extension L/K. We induce those characters $\theta\colon \operatorname{Gal}(\overline{\mathbf{Q}}/K) \to \overline{\mathbf{F}}_\ell^*$ which factor through $\operatorname{Gal}(L/K)$ to obtain two-dimensional ρ representations of $\operatorname{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. According to Lemma 7, the representations ρ are irreducible when θ is non-trivial. The semisimplifications of the induced representations ρ are the $\overline{\mathbf{F}}_\ell$-linear two-dimensional representations of $\operatorname{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ which arise from $Q_{\overline{s}}$.

From another point of view, let K be one of the two fields $\mathbf{Q}(\sqrt{-3})$, $\mathbf{Q}(\sqrt{-1})$. To fix ideas, take the former field and embed it in $\overline{\mathbf{Q}}$. Let R be the ring of integers of K, and let $\mathfrak{f}$ be a non-zero integral ideal of R for which $R/\mathfrak{f}$ is cyclic as an abelian group. Consider the group $\mathcal{C}_{\mathfrak{f}}$ of ideal classes of K modulo $\mathfrak{f}$, and let θ be a non-trivial homomorphism $\mathcal{C}_{\mathfrak{f}} \to \overline{\mathbf{F}}_3^*$. Using class field theory, regard θ as being defined on $\operatorname{Gal}(\overline{\mathbf{Q}}/K)$ and induce θ to obtain a two-dimensional representation ρ of $\operatorname{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. This representation is irreducible. Let N be the norm of $\mathfrak{f}$, and let H be the image of R^* in $(R/\mathfrak{f})^* = (\mathbf{Z}/N\mathbf{Z})^*$.

Theorem 5. *The representation ρ arises from the component group in the mod q reduction of $J(H,q)$ whenever q is a prime number which does not divide $2N$ and which is congruent to 2 modulo 3.*

Proof. Since q is 2 modulo 3, we may choose a supersingular elliptic curve E over $\overline{\mathbf{F}}_q$ whose automorphism group is cyclic of order six. Identify $\mathbf{Z}[\operatorname{Aut} E]$ with R and let C be the kernel of $\mathfrak{f}$ on E. The pair (E,C) then represents a point $\overline{s}$ on $X_0(N)$ which has extra automorphisms and satisfies condition $(*)$. We have seen that ρ arises from the subquotient $Q_{\overline{s}}$ of the component group associated with $J(H,q)$. □

As an application of the Theorem, we obtain the following statement, which could presumably be proved much more directly.

Corollary. *The representation ρ arises from the space of weight-two cusp forms on $\Gamma_1(N)$.*

Proof. Let q be a prime number as in the statement of Theorem 5. The conclusion of the Theorem implies that ρ arises from the space of weight-two cusp forms on $\Gamma_H(N)\cap\Gamma_0(q)$, and hence from the space of cusp forms on $\Gamma_1(N)\cap\Gamma_0(q)$. Since ρ is unramified at q, the desired conclusion now follows from "Mazur's Principle" [15, Theorem 8.1]. □

In the situation of Theorem 5, one can ask whether or not ρ arises from the space of weight-two cusp forms on $\Gamma_H(N)$. In the example treated in §2, this space is zero, so the response is negative. It might be interesting to answer this question in general.

References

1. S. Bosch, W. Lütkebohmert and M. Raynaud, *Néron models*, Springer-Verlag, Berlin and New York, 1990.
2. H. Carayol, *Sur les représentations galoisiennes modulo ℓ attachées aux formes modulaires*, Duke Math. J. **59** (1989), 785–801.
3. H. Cohen, N. Skoruppa and D. Zagier, *Tables of coefficients of modular forms* (to appear).
4. P. Deligne and M. Rapoport, *Les schémas de modules de courbes elliptiques*, Lecture Notes in Math., vol. 349, Springer-Verlag, Berlin and New York, 1973, pp. 143–316.
5. F. Diamond, *The refined Serre conjecture*, This volume.
6. B. Edixhoven, *L'action de l'algèbre de Hecke sur les groupes de composantes des jacobiennes des courbes modulaires est "Eisenstein"*, Astérisque **196–197** (1991), 159–170.
7. ———, *The weight in Serre's conjectures on modular forms*, Invent. Math **109** (1992), 563–594.
8. B. Jordan and R. Livné, *Local diophantine properties of Shimura curves*, Math. Ann. **270** (1985), 235–248.
9. N. M. Katz, *p-adic properties of modular schemes and modular forms*, Lecture Notes in Math., vol. 350, Springer-Verlag, Berlin and New York, 1973, pp. 69–190.
10. ——— and B. Mazur, *Arithmetic moduli of elliptic curves*, Annals of Math. Studies **108**, Princeton University Press, Princeton, 1985.
11. B. Mazur, *Modular curves and the Eisenstein ideal*, Publ. Math. IHES **47** (1977), 33–186.
12. M. Raynaud, *Jacobienne des courbes modulaires et opérateurs de Hecke*, Astérisque **196–197** (1991), 9–25.
13. K. A. Ribet, *On modular representations of* $\operatorname{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ *arising from modular forms*, Invent. Math **100** (1990), 431–476.
14. ———, *On the Component Groups and the Shimura Subgroup of $J_o(N)$*, exposé 6, Sém. Th. des Nombres de l'Université de Bordeaux (1987–88).
15. ———, *Report on mod ℓ representations of* $\operatorname{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, Proceedings of Symposia in Pure Mathematics **55 (2)** (1994), 639–676.

16. J-P. Serre, *Sur les représentations modulaires de degré 2 de* $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, Duke Math. J. **54** (1987), 179–230.
17. ———, *Letter to K. Ribet (15 April 1987)*, unpublished.
18. J. H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Math., vol. 106, Springer-Verlag, Berlin and New York, 1986.
19. J. Tunnell, *Artin's conjecture for representations of octahedral type*, Bull. AMS (new series) **5** (1981), 173–175.
20. A. Wiles, *Modular elliptic curves and Fermat's Last Theorem*, uncirculated manuscript.

UC Mathematics Department, Berkeley, CA 94720-3840 USA
E-mail address: ribet@math.berkeley.edu