

# RAISING THE LEVELS OF MODULAR REPRESENTATIONS

Kenneth A. RIBET

## 1 Introduction

Let  $\ell$  be a prime number, and let  $\mathbf{F}$  be an algebraic closure of the prime field  $\mathbf{F}_\ell$ . Suppose that

$$\rho : \text{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \rightarrow \mathbf{GL}(2, \mathbf{F})$$

is an irreducible (continuous) representation. We say that  $\rho$  is *modular of level  $N$* , for an integer  $N \geq 1$ , if  $\rho$  arises from cusp forms of weight 2 and trivial character on  $\Gamma_o(N)$ .

The term “arises from” may be interpreted in several equivalent ways. For our present purposes, it is simplest to work with maximal ideals of the Hecke algebra for weight-2 cusp forms on  $\Gamma_o(N)$ . Namely, let  $S(N)$  be the  $\mathbf{C}$ -vector space consisting of such forms, and for each  $n \geq 1$  let  $T_n \in \text{End } S(N)$  be the  $n^{\text{th}}$  Hecke operator. Let  $\mathbf{T} = \mathbf{T}_N$  be the subring of  $\text{End } S(N)$  generated by these operators. As is well known ([3], Th. 6.7 and [7], §5), for each maximal ideal  $\mathfrak{m}$  of  $\mathbf{T}$ , there is a semisimple representation

$$\rho_{\mathfrak{m}} : \text{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \rightarrow \mathbf{GL}(2, \mathbf{T}/\mathfrak{m}),$$

unique up to isomorphism, satisfying

$$\text{tr } \rho_{\mathfrak{m}}(\text{Frob}_r) = T_r \pmod{\mathfrak{m}}, \quad \det \rho_{\mathfrak{m}}(\text{Frob}_r) = r \pmod{\mathfrak{m}}$$

for almost all primes  $r$ . (Here  $\text{Frob}_r$  is a Frobenius element in  $\text{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$  for the prime  $r$ .) This representation is in fact unramified at every prime  $r$  prime to  $\ell N$ , and the indicated relations hold for all such primes. We understand that  $\rho$  is modular of level  $N$  if there is a maximal ideal  $\mathfrak{m}$  of  $\mathbf{T}$ , together with an inclusion  $\omega: \mathbf{T}/\mathfrak{m} \hookrightarrow \mathbf{F}$ , so that the representations  $\rho$  and  $\rho_{\mathfrak{m}} \otimes_{\omega} \mathbf{F}$  are isomorphic. (Cf. [7], §5.)

The representations  $\rho_{\mathfrak{m}}$  are nothing other than the Galois representations attached to mod  $\ell$  eigenforms of weight 2 on  $\Gamma_o(N)$ . Indeed, let  $\mathcal{L}$  be the space of

forms in  $S(N)$  which have rational integral  $q$ -expansions. As is well known,  $\mathcal{L}$  is a lattice in  $S(N)$ , cf. [3], Proposition 2.7. The space  $\overline{\mathcal{L}} = \mathcal{L}/\ell\mathcal{L}$  is the space of mod  $\ell$  cusp forms on  $\Gamma_o(N)$ . The  $\mathbf{F}_\ell$ -algebra  $\mathcal{A}$  generated by the Hecke operators  $T_n$  in  $\text{End } \overline{\mathcal{L}}$  may be identified with  $\mathbf{T}/\ell\mathbf{T}$  (see, for example, [7], §5). To give a pair  $(\mathfrak{m}, \omega)$  as above is to give a character (i.e., homomorphism)

$$\epsilon : \mathcal{A} \rightarrow \mathbf{F}.$$

If  $f$  is a non-zero element of  $\overline{\mathcal{L}} \otimes_{\mathbf{F}_\ell} \mathbf{F}$  which is an eigenvector for all  $T_n$ , the action of  $\mathcal{A}$  on the line generated by  $f$  defines such a character  $\epsilon$ . It is an elementary fact that all characters  $\epsilon$  arise in this manner.

Assume now that  $\rho$  is modular of level  $Np$ , where  $p$  is a prime number not dividing  $N$ . We say that  $\rho$  is  $p$ -new (of level  $pN$ ) if  $\rho$  arises in a similar manner from the  $p$ -new subspace  $S(pN)_{p\text{-new}}$  of  $S(pN)$ . Recall that there are two natural inclusions (or degeneracy maps)  $S(N) \rightrightarrows S(pN)$  and dually two trace maps  $S(pN) \rightrightarrows S(N)$ . (See [1] for the former maps.) The two maps  $S(N) \rightrightarrows S(pN)$  combine to give an inclusion  $S(N) \oplus S(N) \hookrightarrow S(pN)$ , whose image is known as the  $p$ -old subspace  $S(pN)_{p\text{-old}}$  of  $S(pN)$ . The space  $S(pN)_{p\text{-new}}$  is defined as the orthogonal complement to  $S(pN)_{p\text{-old}}$  in  $S(pN)$ , under the Petersson inner product on  $S(pN)$ . It may also be characterized algebraically as the intersection of the kernels of the two trace maps; this definition is due to Serre. The space  $S(pN)_{p\text{-new}}$  is  $\mathbf{T}_{pN}$ -stable.

The image of  $\mathbf{T}_{pN}$  in  $\text{End } S(pN)_{p\text{-new}}$  is the  $p$ -new quotient

$$\overline{\mathbf{T}}_{pN} = \mathbf{T}_{pN/p\text{-new}}$$

of  $\mathbf{T}_{pN}$ . We say that  $\rho$  is  $p$ -new if  $\mathfrak{m} \subset \mathbf{T}_{pN}$  and  $\omega$  may be found, as above, in such a way that the maximal ideal  $\mathfrak{m}$  of  $\mathbf{T}_{pN}$  is the inverse image of a maximal ideal of  $\overline{\mathbf{T}}_{pN}$ , under the canonical quotient map  $\mathbf{T}_{pN} \rightarrow \overline{\mathbf{T}}_{pN}$ . On a concrete level, this means that the character

$$\epsilon : \mathbf{T}_{pN} \rightarrow \mathbf{F}$$

coming from  $(\mathfrak{m}, \omega)$  is defined by an eigenform in the mod  $\ell$  reduction of the space

$S(pN)_{p\text{-new}}$ , i.e., in the  $\mathbf{F}$ -vector space  $\Lambda \otimes_{\mathbf{Z}} \mathbf{F}$ , where  $\Lambda$  is the lattice in  $S(pN)_{p\text{-new}}$  consisting of forms with rational integral coefficients.

**THEOREM 1** *Let  $\rho$  be modular of level  $N$ . Let  $p \nmid \ell N$  be a prime satisfying one or both of the identities*

$$\mathrm{tr} \rho(\mathrm{Frob}_p) = \pm(p+1) \pmod{\ell}. \quad (1)$$

*Then  $\rho$  is  $p$ -new of level  $pN$ .*

*Remarks.*

- 1.** In the Theorem, and in the discussion below, we assume that  $\rho$  is irreducible, as above.
- 2.** A slightly stronger conclusion may be obtained if one assumes that  $\rho$  is  $q$ -new of level  $N$ , where  $q$  is a prime number which divides  $N$ , but not  $N/q$ . Under this hypothesis, plus the hypothesis of Theorem 1, one may show that  $\rho$  is  $pq$ -new of level  $pN$ , in a sense which is easy to make precise as above. (See [7], §7, where a theorem to this effect is proved, under the superfluous additional hypothesis  $p \equiv -1 \pmod{\ell}$ .) The interest of Theorem 1 is that no hypothesis is made about the existence of a prime number  $q$ .
- 3.** The case  $p = \ell$  can be included in the Theorem if its hypothesis (1) is reformulated. Namely, (1) tacitly relies on the fact that  $\rho$  is unramified outside the primes dividing  $\ell N$ . Choose a maximal ideal  $\mathfrak{m}$  for  $\rho$  as in the definition of “modular of level  $N$ .” Then (1) may be re-written as the congruence

$$T_p \equiv \pm(p+1) \pmod{\mathfrak{m}}.$$

Assuming simply that  $p$  is prime to  $N$ , but permitting the case  $p = \ell$ , one proves that  $\rho$  is  $p$ -new of level  $pN$  if this congruence is satisfied (with at least one choice of  $\pm$ ).

**COROLLARY** *Let  $\rho$  be modular of level  $N$ . Then there are infinitely many primes  $p$ , prime to  $\ell N$ , such that  $\rho$  is  $p$ -new of level  $pN$ .*

Indeed, suppose that  $p$  is prime to  $\ell N$ . Then  $p$  is unramified in  $\rho$ , so that a Frobenius element  $\text{Frob}_p$  is well defined, up to conjugation, in the image of  $\rho$ . By the Chebotarev Density Theorem, there are infinitely many such  $p$  such that  $\text{Frob}_p$  is conjugate to  $\rho(c)$ , where  $c$  is a complex conjugation in  $\text{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ . Both sides of the congruence (1) are then 0, so that (1) is satisfied. (Cf. [7], Lemma 7.1.)

Our corollary is stated (in terms of mod  $\ell$  eigenforms) as “Théorème (A)” in a recent preprint of Carayol [2]. Carayol describes his Théorème (A) as having been proved in preliminary versions of [7], as an application of results in [6]. In later versions of [7], Théorème (A) was replaced by a theorem involving  $pq$ -new forms (alluded to above), which is proved by methods involving Shimura curves. The aim of this present note is to resurrect Théorème (A).

Our derivation of Theorem 1 is based on the results of [6]. Although we couch our results in the language of Jacobians of modular curves, it should be clear to the reader that we use no fine arithmetic properties of these Jacobians: the argument is entirely cohomological. As F. Diamond has recently shown [4], an elaboration of these methods leads to results for cusp forms of weight  $k \geq 2$ .

## 2 Summary of [6]

First let  $N$  be a positive integer, and consider the modular curve  $X_o(N)_{\mathbf{C}}$ , along with its Jacobian  $J_o(N) = \text{Pic}^o(X_o(N))$ . The curve  $X_o(N)$  comes equipped with standard Hecke correspondences  $T_n$ , which induce endomorphisms of  $J_o(N)$  by Pic functoriality (cf. [7], §3). These endomorphisms, in turn, act on the space of holomorphic differentials on the abelian variety dual to  $J_o(N)$ , which is the Albanese variety of  $X_o(N)$ . This space of differentials is canonically identified with  $S(N)$ , and via this identification the endomorphism  $T_n$  of  $J_o(N)$  acts on the space of differentials as the usual Hecke operator  $T_n$  of  $S(N)$ . Since the action of  $\text{End}(J_o(N))$  on  $S(N)$  is faithful, it follows that the subring of  $\text{End}(J_o(N))$  generated by the  $T_n$  is “nothing other” than the ring  $\mathbf{T}_N$ .

We now choose a prime  $p$  prime to  $N$  and consider  $X_o(pN)$  and  $J_o(pN)$ , to which the same remarks apply. The two curves  $X_o(pN)$  and  $X_o(N)$  are linked by a pair of natural degeneracy maps  $\delta_1, \delta_p: X_o(pN) \rightrightarrows X_o(N)$ , with the following (naive) modular interpretation. The curve  $X_o(pN)$  is associated to the moduli problem of classifying elliptic curves  $E$  which are furnished with cyclic subgroups  $C_N$  and  $C_p$  of order  $N$  and  $p$ , respectively. Similarly,  $X_o(N)$  classifies elliptic curves with cyclic subgroups of order  $N$ . The degeneracy map  $\delta_1$  maps  $(E, C_N, C_p)$  to  $(E, C_N)$ , while  $\delta_p$  maps  $(E, C_N, C_p)$  to  $(E/C_p, C'_N)$ , where  $C'_N$  is the image of  $C_N$  on  $E/C_p$ .

In a similar vein, we recall the modular interpretation of the correspondences  $T_p$  on  $X_o(N)$  and on  $X_o(pN)$ . First, for  $X_o(N)$  we have

$$T_p : (E, C_N) \mapsto \sum_D (E/D, (C_N \oplus D)/D),$$

where the sum is taken over the  $(p+1)$  different subgroups  $D$  of order  $p$  in  $E$ . For  $X_o(pN)$ , we have a sum of  $p$  terms

$$T_p : (E, C_N, C_p) \mapsto \sum_{D \neq C_p} (E/D, (C_N \oplus D)/D, E[p]/D),$$

where  $E[p]$  is the group of  $p$ -division points on  $E$ . (This latter group is the direct sum  $C_p \oplus D$ .) These formulas lead immediately to the relations among correspondences

$$\delta_1 \circ T_p = T_p \circ \delta_1 - \delta_p, \quad \delta_p \circ T_p = p \cdot \delta_1. \quad (2)$$

The maps  $\delta_1$  and  $\delta_p$  combine to induce a map on Jacobians

$$\alpha : J_o(N) \times J_o(N) \rightarrow J_o(pN), \quad (x, y) \mapsto \delta_1^*(x) + \delta_p^*(y).$$

The image of this map is by definition the  $p$ -old subvariety  $A$  of  $J_o(pN)$ ; the kernel of  $\alpha$  is a certain finite group which is calculated in [6].

Namely, let  $\mathbf{Sh}$  be the Shimura subgroup of  $J_o(N)$ , i.e., the kernel of the map  $J_o(N) \rightarrow J_1(N)$  which is induced by the covering of modular curves  $X_1(N) \rightarrow X_o(N)$ . The group  $\mathbf{Sh}$  is a finite group which may be calculated in the following way: Consider the maximal unramified subcovering  $X \rightarrow X_o(N)$  of  $X_1(N) \rightarrow X_o(N)$ , and

let  $\mathcal{G}$  be the covering group of this subcovering. Then  $\mathcal{G}$  and  $\mathbf{Sh}$  are canonically  $\mathbf{G}_m$ -dual.

Let  $\Sigma \subset J_o(N) \times J_o(N)$  be the image of  $\mathbf{Sh}$  under the antidiagonal embedding

$$J_o(N) \rightarrow J_o(N) \times J_o(N), \quad x \mapsto (x, -x).$$

According to [6], Theorem 4.3, we have

**PROPOSITION 1** *The kernel of  $\alpha$  is the group  $\Sigma$ .*

The map  $\alpha$  is equivariant with respect to Hecke operators  $T_n$  with  $(n, p) = 1$ . Namely, we have  $\alpha \circ T_n = T_n \circ \alpha$  for all  $n$  prime to  $p$ , with the understanding that the endomorphism  $T_n$  of  $J_o(N)$  acts diagonally on the product  $J_o(N) \times J_o(N)$ . On the other hand, this formula must be modified when  $n$  is replaced by  $p$ , as one sees from (2).

Before recording the correct formula for  $T_p$ , we introduce the notational device of reserving the symbol  $T_p$  for the  $p^{\text{th}}$  Hecke operator at level  $N$ , and the symbol  $U_p$  for the  $p^{\text{th}}$  Hecke operator at level  $pN$ . With this notation, we have (as a consequence of (2)) the formula

$$U_p \circ \alpha = \alpha \circ \begin{pmatrix} T_p & p \\ -1 & 0 \end{pmatrix}, \quad (3)$$

in which the matrix refers to the natural left action of  $M(2, \mathbf{T}_N)$  on the product  $J_o(N) \times J_o(N)$ .

Concerning the behavior of  $\mathbf{Sh}$  and  $\Sigma$  under Hecke operators, the following (easy) result is noted briefly in [6] and proved in detail in [8].

**PROPOSITION 2** *The Shimura subgroup  $\mathbf{Sh}$  of  $J_o(N)$  is annihilated by the endomorphisms*

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

*of  $J_o(N)$  for all primes  $r \nmid N$ .*

COROLLARY *The subgroup  $\Sigma$  of  $J_o(N) \times J_o(N)$  lies in the kernel of the endomorphism  $\begin{pmatrix} 1+p & T_p \\ T_p & 1+p \end{pmatrix}$  of  $J_o(N) \times J_o(N)$ . It is annihilated by the operators  $T_r - (r+1)$  for all prime numbers  $r$  not dividing  $pN$ .*

The significance of the endomorphism introduced in the corollary appears when we note the formula  $\beta \circ \alpha = \begin{pmatrix} 1+p & T_p \\ T_p & 1+p \end{pmatrix}$ , in which  $\beta : J_o(Np) \rightarrow J_o(N) \times J_o(N)$  is the map induced by the two degeneracy maps  $X_o(Np) \rightrightarrows X_o(N)$  and Albanese functoriality of the Jacobian. (The map  $\beta$  becomes the dual of  $\alpha$  when we use “autoduality of the Jacobian” to identify the Jacobians with their own duals.) The formula results from the fact that the two degeneracy maps are each of degree  $p+1$ , and from the usual definition of  $T_p$  as a correspondence in terms of degeneracy maps.

Let  $\Delta \subset J_o(N) \times J_o(N)$  be the kernel of  $\begin{pmatrix} 1+p & T_p \\ T_p & 1+p \end{pmatrix}$ . Then  $\Delta$  is a finite subgroup of  $J_o(N) \times J_o(N)$ . Indeed,  $\Delta$  differs only by 2-torsion from the direct sums of the kernels of  $T_p \pm (p+1)$  on  $J_o(N)$ . These latter kernels are finite because neither number  $\pm(p+1)$  can be an eigenvalue of  $T_p$  on  $S(N)$ , in view of Weil’s Riemann hypothesis, which bounds  $T_p$ ’s eigenvalues by  $2\sqrt{p}$ . Further, the group  $\Delta$  comes equipped with a perfect  $\mathbf{G}_m$ -valued skew-symmetric pairing, in view of its interpretation as the kernel  $K(L)$  of a polarization map

$$\phi_L : J_o(N) \times J_o(N) \rightarrow (J_o(N) \times J_o(N))^\vee.$$

(One takes  $L$  to be the pullback by  $\alpha$  of the “theta divisor” on the Jacobian  $J_o(pN)$ .)

The subgroup  $\Sigma$  of  $\Delta$  is self-orthogonal under the pairing on  $\Delta$ . In other words, if we let  $\Sigma^\perp$  be the annihilator of  $\Sigma$  in the pairing, we have a chain of groups

$$\Delta \supset \Sigma^\perp \supset \Sigma.$$

Note also that  $\Delta/\Sigma$  is naturally a subgroup of the abelian variety  $A$ , since  $A$  and  $\Sigma$  are the image and kernel of  $\alpha$ , respectively. Thus the subquotient  $\Sigma^\perp/\Sigma$  of  $\Delta$  is in particular a subgroup of  $A$ .

On the other hand, the quotient  $\Delta/\Sigma^\perp$  is canonically the Cartier (i.e.,  $\mathbf{G}_m$ ) dual  $\Sigma^*$  of  $\Sigma$ . It is naturally a subgroup of  $A^\vee$ . Indeed,  $\Sigma$  is the kernel of the isogeny  $J_o(N) \times J_o(N) \rightarrow A$  induced by  $\alpha$ . The kernel of the dual homomorphism  $A^\vee \rightarrow (J_o(N) \times J_o(N))^\vee$  may be identified with  $\Sigma^*$ .

To state the final result that we need, we introduce the  $p$ -new abelian subvariety  $B$  of  $J_o(pN)$ . To define it, consider the map

$$J_o(pN)^\vee \rightarrow A^\vee$$

which is dual to the inclusion  $A \hookrightarrow J_o(pN)$ . Its kernel is an abelian subvariety  $Z$  of  $J_o(pN)^\vee$ . Using the autoduality of  $J_o(pN)$  to transport  $Z$  back to  $J_o(pN)$ , we obtain  $B$ . This subvariety of  $J_o(pN)$  is a complement to  $A$  in the sense that  $J_o(pN) = A+B$  and  $A \cap B$  is finite. It is  $p$ -new in that  $\mathbf{T}_{pN}$  stabilizes  $B$  and acts on  $B$  through its  $p$ -new quotient  $\overline{\mathbf{T}}_{pN}$  (which acts faithfully on  $B$ ). The following main result of [6] is a formal consequence of Proposition 2:

**THEOREM 2** *The finite groups  $A \cap B$  and  $\Sigma^\perp/\Sigma$  are equal.*

In the notation of [6],  $A \cap B$  is the group  $\Omega$ , which can be described directly in terms of  $\Delta$  and the kernel of  $\alpha$  ([6], pp. 508–509). Once this kernel is identified, the description of Theorem 2 is immediate.

### 3 Proof of Theorem 1

We assume from now on that  $\rho$  is modular of level  $N$ , and choose an ideal  $\mathfrak{m}$  of  $\mathbf{T}_N$ , plus an embedding  $\omega: \mathbf{T}_N/\mathfrak{m} \hookrightarrow \mathbf{F}$  as in the definition of “modular of level  $N$ .” Assuming that one of the two congruences (1) is satisfied, we will construct

1. A maximal ideal  $\mathcal{M}$  of  $\overline{\mathbf{T}}_{pN}$ , and
2. An isomorphism  $\mathbf{T}_N/\mathfrak{m} \approx \overline{\mathbf{T}}_{pN}/\mathcal{M}$  which takes  $T_r$  to  $T_r$  for all primes  $r \neq p$ .

This is enough to prove the theorem, since the representations  $\rho_{\mathfrak{m}}$  and  $\rho_{\mathcal{M}}$  will necessarily be isomorphic, in view of the  $T_r$ -compatible isomorphism between the residue fields of  $\mathfrak{m}$  and  $\mathcal{M}$ . Our procedure is to construct  $\mathcal{M}$  first as a maximal ideal of  $\mathbf{T}_{Np}$  and then to verify that  $\mathcal{M}$  in fact arises by pullback from a maximal ideal of  $\overline{\mathbf{T}}_{pN}$ .

It might be worth pointing out explicitly that our construction of  $\mathcal{M}$  depends on the sign  $\pm$  in (1). If  $p \not\equiv -1 \pmod{\ell}$ , then there is a unique sign  $\pm$  which makes (1) true, under the hypothesis of the theorem, and our construction proceeds in a mechanical way. In case  $p \equiv -1 \pmod{\ell}$ , both congruences (1) are satisfied under the hypothesis of the theorem, and the construction requires us to decide whether (1) should read  $0 \equiv +0$  or  $0 \equiv -0$ . The two choices of sign lead to different ideals  $\mathcal{M}$ , at least when  $\ell$  is odd, since our construction shows that  $U_p \equiv \pm 1 \pmod{\mathcal{M}}$ , with the same sign  $\pm$  as in (1).

Before beginning the construction, we introduce the following abbreviations:

$$R = \mathbf{T}_N, \quad k = \mathbf{T}_N/\mathfrak{m}, \quad \mathbf{T} = \mathbf{T}_{pN}, \quad \overline{\mathbf{T}} = \overline{\mathbf{T}}_{pN}.$$

Also, let

$$V = J_o(N)[\mathfrak{m}]$$

be the kernel of  $\mathfrak{m}$  on  $J_o(N)$ , i.e., the intersection of the kernels on  $J_o(N)$  of the various elements of  $\mathfrak{m}$ . This group is a finite  $k$ -vector space which is easily seen to be non-zero (cf. [5], or [7], Theorem 5.2). The group  $V \times V$  is then a finite subgroup of  $J_o(N) \times J_o(N)$ . This subgroup has zero intersection with  $\mathbf{Sh} \times \mathbf{Sh}$ , in view of the irreducibility of  $\rho_m$ , Proposition 2 above, and [7], Theorem 5.2(c). In particular,  $\alpha$  maps  $V \times V$  isomorphically into  $A$ . Therefore, we can (and will) regard  $V \times V$  as a subgroup of that abelian variety.

We now assume that one of the two congruences (1) is satisfied. To fix ideas we will treat only the case

$$\mathrm{tr} \rho(\mathrm{Frob}_p) \equiv -(p+1) \pmod{\ell}.$$

Using the isomorphism between  $\rho$  and  $\rho_{\mathfrak{m}} \otimes_{\omega} \mathbf{F}$ , we restate this congruence in the form

$$T_p \equiv -(p+1) \pmod{\mathfrak{m}}. \quad (4)$$

(The left-hand side of (4) is the trace of  $\rho_{\mathfrak{m}}(\mathbf{Frob}_p)$ .) We embed  $V$  in  $V \times V$  via the *diagonal* embedding; the antidiagonal embedding would be used instead if  $T_p$  were  $p+1$  modulo  $\mathfrak{m}$ . We have

$$V \hookrightarrow V \times V \hookrightarrow A.$$

**LEMMA 1** *The subgroup  $V$  of  $A$  is stable under  $\mathbf{T}$ . The action of  $\mathbf{T}$  on  $V$  is summarized by a homomorphism  $\gamma : \mathbf{T} \rightarrow k$  which takes  $T_n$  to  $T_n$  modulo  $\mathfrak{m}$  for  $(n, p) = 1$  and takes  $U_p$  to  $-1$ .*

*Proof.* That  $T_n \in \mathbf{T}$  acts on  $V$  in the indicated way, for  $n$  prime to  $p$ , follows from the equivariance of  $\alpha$  with respect to such  $T_n$ . The statement relative to  $U_p$  then follows from (3) and (4). ■

Define  $\mathcal{M} = \ker \gamma$ , so that we have an inclusion  $\mathbf{T}/\mathcal{M} \hookrightarrow k = R/\mathfrak{m}$ . This map is in fact an *isomorphism* since  $k$  is generated by the images of the  $T_n$  with  $n$  prime to  $p$ . Indeed,  $T_p$  lies in the prime field  $\mathbf{F}_\ell$  of  $k$  because of (4).

To conclude our proof of Theorem 1, we must show that the maximal ideal  $\mathcal{M}$  of  $\mathbf{T}$  arises by pullback from  $\overline{\mathbf{T}}$ . For this, it suffices to show that  $\mathbf{T}$  acts on  $V$  through its quotient  $\overline{\mathbf{T}}$ . This fact follows from

**LEMMA 2** *The subgroup  $V$  of  $A$  lies in the intersection  $A \cap B$ .*

*Proof.* We first note that  $V$ , considered diagonally as a subgroup of  $J_o(N) \times J_o(N)$ , lies in the group  $\Delta$ . Indeed,  $V \subset J_o(N)$  is killed by  $T_p + p + 1$  by virtue of (4). The isomorphic image of  $V$  in  $J_o(pN)$  therefore lies in  $\Delta/\Sigma$ . To prove the lemma, we must show that this image lies in the subgroup  $A \cap B = \Sigma^\perp/\Sigma$  of  $\Delta/\Sigma$ . In other words, we must show that the image of  $V$  in  $\Delta/\Sigma^\perp$  is 0.

A somewhat painless way to see this is to view the varieties  $J_o(N)$ ,  $J_o(Np)$ ,  $A$ ,  $\dots$  as being defined over  $\mathbf{Q}$ . The group  $\Delta/\Sigma^\perp$  is canonically the  $\mathbf{G}_m$ -dual of  $\Sigma$ , which may be identified  $\text{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ -equivariantly with the Shimura subgroup  $\mathbf{Sh}$  of  $J_o(N)$ . This latter group is in turn the  $\mathbf{G}_m$ -dual of the covering group  $\mathcal{G}$  introduced above. It follows that the action of  $\text{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$  on  $\Delta/\Sigma^\perp$  is trivial. (We note in passing that the action of  $\text{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$  on  $\mathbf{Sh}$  is given by the cyclotomic character  $\text{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \rightarrow \hat{\mathbf{Z}}^*$ .) Hence if  $V$  maps non-trivially to  $\Delta/\Sigma^\perp$ , the semisimplification of  $V$  (as a  $\mathbf{F}_\ell[\text{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})]$ -module) contains the trivial representation. This semisimplification may be constructed by the following recipe: find the semisimplification  $W$  on  $V$  as a  $k[\text{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})]$ -module, and consider  $W$  as an  $\mathbf{F}_\ell$ -module. (A simple representation over  $k$  remains semisimple after “restriction of scalars” from  $k$  to  $\mathbf{F}_\ell$ .) Hence  $W$  contains  $\text{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ -invariant vectors, if  $V$  maps non-trivially to  $\Delta/\Sigma^\perp$ . This conclusion is absurd, since  $W$  is the direct sum of a number of copies of the  $k$ -simple 2-dimensional representation  $\rho_m$  ([5], Chapter II, Proposition 14.2). ■

## Bibliography

- [1] Atkin, A.O.L. and Lehner, J. Hecke operators on  $\Gamma_o(m)$ . Math. Ann. **185**, 134–160 (1970)
- [2] Carayol, H. Sur les représentations Galoisiennes modulo  $\ell$  attachées aux formes modulaires. Preprint
- [3] Deligne, P. and Serre, J-P. Formes modulaires de poids 1. Ann. Sci. Ec. Norm. Sup. **7**, 507–530 (1974)
- [4] Diamond, F. I. Congruence primes for cusp forms of weight  $k \geq 2$ . To appear
- [5] Mazur, B. Modular curves and the Eisenstein ideal. Publ. Math. IHES **47**, 33–186 (1977)
- [6] Ribet, K. Congruence relations between modular forms. Proc. International Congress of Mathematicians 1983, 503–514
- [7] Ribet, K. On modular representations of  $\text{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$  arising from modular forms. Preprint
- [8] Ribet, K. On the component groups and the Shimura subgroup of  $J_o(N)$ . Séminaire de Théorie des Nombres, Université de Bordeaux, 1987/88

K. A. Ribet  
Mathematics Department  
University of California  
Berkeley CA 94720  
U.S.A.