Inventiones math. 28, 245 – 275 (1975)

On ℓ-Adic Representations Attached to Modular Forms

Kenneth A. Ribet (Princeton)

Introduction

This paper generalizes some results of Serre and Swinnerton-Dyer [9, 11] concerning Deligne's ℓ-adic representations attached to modular forms. Let $k_1, \ldots, k_r$ be distinct positive even integers, and for each i let ρ_{ℓ,k_i} be the ℓ-adic representation attached to cusp forms of weight k_i for $\mathbf{SL}(2, \mathbf{Z})$. If H_{k_i} is the $\mathbf{Z}$-ring of Hecke operators of weight k_i, then ρ_{ℓ,k_i} may be viewed as a map

$$\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathbf{GL}(2, H_{k_i} \otimes \mathbf{Q}_\ell)$$

satisfying the following two conditions:

(i) ρ_{ℓ,k_i} is unramified at each prime $p \neq \ell$.

(ii) If $F_p \in \rho_{\ell,k_i}(\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}))$ is a Frobenius element for a prime $p \neq \ell$, then F_p has trace (resp. determinant) equal to T_p (resp. p^{k_i-1}).

Note that the condition involving the determinants of Frobenius elements just means that the determinant of ρ_{ℓ,k_i}, *a priori* a character

$$\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to (H_{k_i} \otimes \mathbf{Q}_\ell)^*,$$

is in fact the $(k_i-1)^{\text{st}}$ power of the cyclotomic map obtained by composing the "standard" cylotomic character

$$\chi_\ell \colon \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathbf{Z}_\ell^*$$

with the canonical inclusion $\mathbf{Z}_\ell^* \hookrightarrow (H_{k_i} \otimes \mathbf{Q}_\ell)^*$.

For each ℓ, let ρ_ℓ be the product representation

$$\rho_{\ell_1} \times \cdots \times \rho_{\ell_r}.$$

Then the main theorem (see below) may be paraphrased as follows: for each prime ℓ, the ℓ-adic Lie algebra of ρ_ℓ is "as large as possible," and for almost all primes ℓ (i.e., all but a finite number), the image of ρ_ℓ is exactly as large as possible. This is exactly what Serre and Swinnerton-Dyer proved in the special case where $r=1$ and where $k=k_1$ is one of the integers for which $H_k = \mathbf{Z}$, namely 12, 16, 18, 20, 22, and 26.

Let $\mathscr{H}$ be the product $H_{k_1} \times \cdots \times H_{k_r}$, and let $\mathscr{E}$ be the $\mathbf{Q}$-algebra $\mathscr{H} \otimes \mathbf{Q}$. It follows from the Hecke-Petersson theory that $\mathscr{E}$ is a product of totally real fields and that $\mathscr{H}$ is an order in $\mathscr{E}$, i.e., a subring of finite index in the "ring of integers" $\mathscr{O}$ of $\mathscr{E}$ obtained by taking the product of the intger rings of the factors of $\mathscr{E}$. Since

the image of ρ_ℓ is compact, we may assume that it is contained in $\mathbf{GL}(2, \mathcal{O} \otimes \mathbf{Z}_\ell)$ for each ℓ. Now let $(\mathbf{Z}_\ell^*)^{(k-1)}$ be the subgroup of $(\mathcal{O} \otimes \mathbf{Z}_\ell)^*$ consisting of those tuples

$$(a_1, \ldots, a_r) \in (H_{k_1} \otimes \mathbf{Q}_\ell) \times \cdots \times (H_{k_r} \otimes \mathbf{Q}_\ell)$$

which are of the form

$$(b^{k_1-1}, \ldots, b^{k_r-1})$$

for some $b \in \mathbf{Z}_\ell^*$. Let

$$\mathscr{A}_\ell = \{M \in \mathbf{GL}(2, \mathcal{O} \otimes \mathbf{Z}_\ell) : \det M \in (\mathbf{Z}_\ell^*)^{(k-1)}\}.$$

Then (because of the determinant condition on the ρ_{ℓ, k_i}) for each ℓ the image of ρ_ℓ is contained in $\mathscr{A}_\ell$.

Main Theorem (0.1). 1. *For each ℓ, the image of ρ_ℓ is an open subgroup of $\mathscr{A}_\ell$.*

2. *For almost all ℓ, the image of ρ_ℓ is exactly $\mathscr{A}_\ell$.*

We prove these results by following the general method of Serre and Swinnerton-Dyer, using some group-theoretic results from [6]. The main idea is that whenever the image of ρ_ℓ is small, the group theory of $\mathbf{GL}(2)$ forces a congruence "mod ℓ" on the Hecke operators T_n. This congruence may be interpreted as an identity of modular forms over $\overline{\mathbf{F}}_\ell$, and the theory of such modular forms then enables us to get a bound on ℓ.

Instead of working with the representations ρ_ℓ, however, we have found it more convenient to work with "pieces" of these representations obtained from complex eigenforms. Namely, if

$$f = q + a_2 q^2 + \cdots$$

is a cusp form of weight k for $\mathbf{SL}(2, \mathbf{Z})$ which is an eigenform for all Hecke operators T_n, then the map $T_n \mapsto a_n$ induces a homomorphism $H_k \to \mathbf{C}$ whose image is an order in some number field $E_f \subset \mathbf{C}$. This homomorphism gives rise to a family of ℓ-adic representations

$$\rho_{\ell, f} : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathbf{GL}(2, E_f \otimes \mathbf{Q}_\ell),$$

where $\rho_{\ell, f}$ is a direct summand of the ℓ-adic representation $\rho_{\ell, k}$ associated to cusp forms of weight k. (Since $H_k \otimes \mathbf{Q}$ is a product of fields, E_f is a direct factor of $H_k \otimes \mathbf{Q}$.)

We study these representations in § 5 and prove that their images are as large as possible for almost all ℓ (5.1) and also that their Lie algebras are as large as possible for all ℓ (5.5). In § 6 we study the representations

$$\rho_{\ell, f} \times \rho_{\ell, f'}$$

obtained by taking two eigenforms f and f' which correspond to different factors of the algebra $\mathscr{E}$ and prove again that these representations have large images. In § 7 we finally deduce the main theorem, piecing together the results of the fifth and sixth sections by means of the group-theoretic "two principle" (3.3).

§ 8 studies the representations $\rho_{\ell, 24}$ attached to the space of cusp forms of weight 24: this is the smallest weight for which the theory of Serre and Swinnerton-

Dyer does not apply. By combining our general theory with some precise computational devices introduced in [11], we compute the set of "exceptional" primes ℓ for which $\rho_{\ell,24}$ does not map $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ onto $\mathscr{A}_\ell$.

The first four sections contain preliminary material on such subjects as λ-adic representations, subgroups of $\mathbf{GL}(2)$, and modular forms "mod ℓ." As a corollary to one of the group-theoretic lemmas (the profinite version of the "two principle" mentioned above), we obtain a generalization of Serre's theorem about the ℓ-adic representations attached to a product of elliptic curves (3.5).

Some of the material in the early sections of this paper was abstracted from the author's Harvard thesis [6]. The author wishes again to thank his advisor John Tate for his help and encouragement. The author also wishes to thank J-P. Serre, who suggested the problems studied in this paper, and N. Katz, who provided help with modular forms.

§ 1. Compatible Systems of λ-Adic Representations

This section contains some preliminary results concerning λ-adic representations. Much of the material is due to Serre [7], who essentially left the theory as an "exercise." Complete details can be found in [6], from which (1.2) has been abstracted.

We fix a number field E and set $d=[E:\mathbf{Q}]$. The residue characteristic of a (non-archimedian) prime λ of E is a prime number $\ell(\lambda)$, and we write $\lambda|\ell$ (and say that λ divides ℓ) if $\ell=\ell(\lambda)$. We let E_λ be the completion of E at λ.

Let K be a field, and let K_s be a separable closure for K. Let G be the Galois group $\mathrm{Gal}(K_s/K)$. A *λ-adic representation* of G (or, by abuse, of K) is a continuous homomorphism

$$\rho\colon G\to \mathrm{Aut}_{E_\lambda} V,$$

where V is a finite-dimensional E_λ-vector space. The *dimension* of ρ is the dimension of the representation space V. Since

$$\mathrm{Aut}_{E_\lambda} V\subset \mathrm{Aut}_{\mathbf{Q}_\ell} V,$$

a λ-adic representation of dimension n may be regarded as an ℓ-adic representation of dimension $n\cdot[E_\lambda:\mathbf{Q}_\ell]$ if $\ell=\ell(\lambda)$.

Suppose, on the other hand, that

$$\rho\colon G\to \mathrm{Aut}_{\mathbf{Q}_\ell} W$$

is an ℓ-adic representation. Then if $\lambda|\ell$ we get a λ-adic representation P/λ by making G act on the E_λ-vector space $V=W\otimes_{\mathbf{Q}_\ell} E_\lambda$. In particular, if $\mathrm{ch}\, K\neq\ell$, let

$$\chi_\ell\colon G\to \mathrm{Aut}(V_\ell)=\mathbf{Q}_\ell^*$$

be the 1-dimensional ℓ-adic representation giving the action of G on the ℓ-power roots of unity in K_s [7, I-3]. Then we get a λ-adic representation

$$\chi_\ell=\chi_{\ell/\lambda}\colon G\to \mathrm{Aut}_{E_\lambda}(V_\ell\otimes E_\lambda)=E_\lambda^*,$$

called the *cyclotomic character*. It may also be described as the composition

$$G \xrightarrow{\chi_\ell} \mathbf{Q}_\ell^* \subset E_\lambda^*.$$

We now suppose that K is a number field.

Let ρ be a λ-adic representation of G. We say that ρ is *unramified* at a place v of K if $\rho(I) = \{1\}$ for each inertia group $I \subset G$ attached to v. When this is the case we can define in the usual way a *Frobenius element* $F_v \in \rho(G)$, unique up to conjugation by elements of $\rho(G)$. The characteristic polynomial

$$P_{v,\rho}(t) = \det(1 - tF_v) \in E_\lambda[t]$$

is then independent of the choice of F_v.

One says that ρ is *rational* (or "*E-rational*") if ρ is unramified at almost all v (i.e., all aside from a finite number) and if for almost all v at which ρ is unramified the polynomial $P_{v,\rho}(t)$ has coefficients in E. If λ' is a prime of E (perhaps equal to λ) and ρ' is a λ'-adic representation of G, then ρ' is said to be *compatible* with ρ if both are rational and if for almost all v we have

$$P_{v,\rho} = P_{v,\rho'}$$

if v is such that both polynomials are defined.

For example, if

$$\rho\colon G \to \mathrm{Aut}\, V$$

is a rational λ-adic representation and ρ' is the *semi-simplification* of ρ (cf. [7], I-10), then ρ' is rational and compatible with ρ.

A *system (ρ_λ) of λ-adic representations* is a collection of λ-adic representations, one for each prime λ of E. We say that (ρ_λ) is *strictly compatible* if there is a finite set S of places of K and a collection of polynomials $\{P_v(t) \in E[t],\ v \notin S\}$ such that each ρ_λ satisfies:

If $v \notin S$ is a place of K with residue characteristic different from that of λ, then ρ_λ is unramified at v and

$$P_{v,\rho_\lambda} = P_v.$$

Remark. If L is an extension of K contained in $\overline{K} = K_s$, then the restriction map

$$\rho \xrightarrow{\mathrm{res}_L} \rho | \mathrm{Gal}(\overline{K}/L)$$

takes λ-adic representations of K to λ-adic representations of L. If L/K is finite, then res_L takes rational representations to rational representations, compatible pairs of representations to compatible pairs of representations, and compatible systems to compatible systems. This follows from the fact that the characteristic polynomial of any power of a Frobenius element F_v may be expressed in terms of the characteristic polynomial of F_v itself by a universal formula.

Theorem (1.1). *Suppose that ρ is a λ-adic representation of K and that ρ' is a λ'-adic representation of K which is compatible with ρ. Suppose that K is either* $\mathbf{Q}$ *or a compositum of quadratic extensions of* $\mathbf{Q}$. *Assume that the semi-simplification of ρ is an abelian representation* (i.e., has an abelian image). *Then the semi-simplification of ρ' is also abelian.*

Proof. (We present the proof "modulo" the theory of locally algebraic λ-adic representations. The reader can consult [7] for a treatment of locally algebraic ℓ-adic representations and a statement of the λ-adic results, or he can read [6] if he wants all the details.) We can assume that ρ and ρ' are semi-simple by replacing them by their semi-simplifications. Given the hypothesis on K it follows from the theorem of Lang-Siegel ([7], Remark 2, p. III-20) that ρ is a locally algebraic abelian λ-adic representation. By Serre's theorem on locally algebraic representations ([7], § 2.4) there exists for each prime λ'' of E a unique (up to isomorphism) semi-simple λ''-adic representation compatible with ρ: this λ''-adic representation is by construction abelian. In particular we get that ρ' is abelian.

Theorem (1.2). *Let (ρ_λ) be a strictly compatible system of 2-dimensional λ-adic representations of K. Assume for each finite extension L of K in $\overline{K}$ and each λ that the semi-simplification of the λ-adic representation $\mathrm{res}_L(\rho_\lambda)$ is non-abelian. For each prime number ℓ, let ρ_ℓ be the direct sum of the representations ρ_λ for $\lambda|\ell$, so ρ_ℓ is a continuous map*

$$G \to \mathrm{Aut}_{E\otimes \mathbf{Q}_\ell} V_\ell,$$

where V_ℓ is a free $E\otimes \mathbf{Q}_\ell$-module of rank 2. Suppose that there is a positive integer t *so that for each ℓ the determinant of ρ_ℓ* (taken relative to $E\otimes \mathbf{Q}_\ell$) *is the* t*-th power of the cyclotomic character*

$$\chi_\ell \colon G \to (E\otimes \mathbf{Q}_\ell)^*.$$

Then for each ℓ we have an inclusion

$$\mathscr{G}_\ell \overset{\text{def}}{=} \rho_\ell(G) \subseteq \{u \in \mathrm{Aut}_{E\otimes \mathbf{Q}_\ell} V_\ell \colon \det u \in \mathbf{Q}_\ell^*\} \overset{\text{def}}{=} \mathscr{B}_\ell.$$

Furthermore, if $\mathscr{G}_\ell$ is open in $\mathscr{B}_\ell$ for one ℓ, then $\mathscr{G}_\ell$ is open in $\mathscr{B}_\ell$ for all ℓ.

Proof. The asserted inclusion follows directly from the fact that $\det \rho_\ell = \chi_\ell^t$. We note that $\mathscr{G}_\ell$ and $\mathscr{B}_\ell$ are ℓ-adic Lie groups, so that $\mathscr{G}_\ell$ will be open in $\mathscr{B}_\ell$ precisely when the Lie algebras $\mathfrak{g}_\ell$ and $\mathfrak{b}_\ell$ of these groups are equal. One can show using the hypothesis concerning "non-abelian semi-simplifications" and the fact that χ_ℓ is a character of infinite order that the equality $\mathfrak{g}_\ell = \mathfrak{b}_\ell$ is equivalent to the statement that the $\overline{\mathbf{Q}}_\ell$-vector spaces

$$\overline{V}_\sigma = V_\ell \otimes_{(E\otimes \mathbf{Q}_\ell)} \overline{\mathbf{Q}}_\ell$$

of dimension 2 obtained from the various $\mathbf{Q}_\ell$-linear maps

$$\sigma \colon E\otimes \mathbf{Q}_\ell \to \overline{\mathbf{Q}}_\ell$$

are pairwise non-isomorphic as $\mathfrak{g}_\ell \otimes \overline{\mathbf{Q}}_\ell$-modules. (See Ch. IV of [6], especially (4.4.9) and (4.4.10).) In other words, the statement that $\mathscr{G}_\ell$ is open in $\mathscr{B}_\ell$ may be understood via a direct Lie algebra analysis as the following statement: for each finite extension L/K of K in $\overline{K}$ the (semi-simple) representations

$$\rho_{\ell,\sigma,L} \colon \mathrm{Gal}(\overline{K}/L) \to \mathrm{Aut}_{E\otimes \mathbf{Q}_\ell} V_\ell \to \mathrm{Aut}_{\overline{\mathbf{Q}}_\ell}(\overline{V}_\sigma)$$

are pairwise non-isomorphic as $\overline{\mathbf{Q}}_\ell$-representations of $\mathrm{Gal}(\overline{K}/L)$.

With this said, we are left only with the question of deciding that this non-isomorphism condition does not depend on ℓ. We can check this just when $L=K$, since the hypotheses of the theorem remain true if we replace K by a finite extension L. For convenience we write

$$\rho_{\ell,\sigma}=\rho_{\ell,\sigma,K}$$

for each σ. Let S be a finite set of places of K chosen for (ρ_λ) as in the definition of "strictly compatible." For each $v\notin S$, $v\nmid\ell$, let $a_{v,\ell}$ be the trace of a Frobenius element for v in $\mathcal{G}_\ell$, regarded as the trace of an endomorphism of a free $E\otimes\mathbf{Q}_\ell$-module. Thus $a_{v,\ell}$ is an element of $E\otimes\mathbf{Q}_\ell$ which in fact lies in E by strict compatibility. Let F be the subfield of E generated over $\mathbf{Q}$ by the $a_{v,\ell}$ for varying v. From the Čebotarev Density Theorem and the lemma on page I-11 of [7] it follows that two representations $\rho_{\ell,\sigma}$ and $\rho_{\ell,\tau}$ are isomorphic precisely when σ and τ coincide on F. This shows in particular that the field F does not change if S is enlarged. Thus by the strict compatibility – more precisely the fact that for two primes ℓ,ℓ' we have

$$a_{v,\ell}=a_{v,\ell'}$$

whenever both terms are defined – it is clear that F does not depend on ℓ. Since for a given ℓ the $\rho_{\ell,\sigma}$ will be pairwise non-isomorphic exactly when $E=F$ we get what we want.

§ 2. Group Theory

In this section, k is a positive even integer. If R is a ring, R^{*k-1} is the group of $(k-1)^{\text{st}}$ powers in R^*. Also, if K is a field, we say that a subgroup $\mathcal{G}$ of $\mathbf{GL}(2,K)$ is *semi-simple* if the inclusion

$$\mathcal{G}\hookrightarrow\mathbf{GL}(2,K)$$

is a semi-simple representation of $\mathcal{G}$ over K.

Theorem (2.1). *Let $K_1,\ldots,K_t$ be finite extensions of $\mathbf{Q}_\ell$ ($\ell\geqq 5$), and let $O_1,\ldots,O_t$ be their integer rings. Suppose that $\mathcal{G}$ is a closed subgroup of*

$$\mathbf{GL}(2,O_1)\times\cdots\times\mathbf{GL}(2,O_t)$$

whose image "mod ℓ" contains

$$S=\mathbf{SL}(2,O_1/\ell O_1)\times\cdots\times\mathbf{SL}(2,O_t/\ell O_t).$$

Then $\mathcal{G}$ contains

$$\mathcal{S}=\mathbf{SL}(2,O_1)\times\cdots\times\mathbf{SL}(2,O_t).$$

Proof. Let $\mathcal{H}$ be the closure of the commutator subgroup of $\mathcal{G}$. This is a closed subgroup of $\mathcal{S}$ mapping onto the commutator subgroup of S, which is S itself (see below). It follows from an argument of Serre ([7], Lemma 3, p. IV-23) that $\mathcal{H}$ is all of $\mathcal{S}$, and this gives the required result.

It remains to show that if O is the integer ring of an ℓ-adic field, then $\mathbf{SL}(2,O/\ell O)$ is its own commutator subgroup. Let λ be a uniformizing parameter in O, and let e be the absolute ramification index. We will show that $\mathbf{SL}(2,O/\lambda^n O)$ is its own

commutator group for all $n \leqq e$. This is well known for $n=1$ [2]. Let us assume inductively that n is greater than 1 and that the result is known for $n-1$.

By induction, it suffices to show that the commutator subgroup of $\mathbf{SL}(2, O/\lambda^n O)$ contains the kernel of the surjection

$$\mathbf{SL}(2, O/\lambda^n O) \to \mathbf{SL}(2, O/\lambda^{n-1} O).$$

This kernel is naturally isomorphic to the additive group

$$\mathbf{sl}\,(2, O/\lambda O) = \{u \in \mathbf{M}(2, O/\lambda O) : \operatorname{tr} u = 0\}.$$

Moreover, if $u \in \mathbf{sl}\,(2, O/\lambda O)$ and $S \in \mathbf{SL}(2, O/\lambda^n O)$, then the commutator of S and u in $\mathbf{SL}(2, O/\lambda^n O)$ is the element

$$sus^{-1} - u$$

of $\mathbf{sl}\,(2, O/\lambda O)$, where s is the image of S in $\mathbf{SL}(2, O/\lambda O)$. Therefore it suffices to prove that $\mathbf{sl}\,(2, O/\lambda O)$ is generated by elements of this type.

More generally, if F is any field with four or more elements, then the analogous group $\mathbf{sl}\,(2, F)$ is generated by elements of the form $sus^{-1} - u$ with $s \in \mathbf{SL}(2, F)$, $u \in \mathbf{s}1(2, F)$. To see this, we note that any element of $\mathbf{sl}\,(2, F)$ is the sum of matrices with square zero. Given any such matrix v, we may write it in the form $\begin{pmatrix} 0 & x \\ 0 & 0 \end{pmatrix}$ after a change of basis. Since F has at least four elements, we may choose $a \in F$ such that $a^2 \neq 0, 1$. Put $b = x/(a^2 - 1)$,

$$s = \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}, \qquad u = \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix}.$$

Then we have $sus^{-1} - u = v$ as required.

Corollary (2.2). *Suppose that $\mathscr{G}$ is a closed subgroup of*

$$\mathscr{A} = \left\{ (u_1, \ldots, u_t) \in \prod_{i=1}^{t} \mathbf{GL}(2, O_i) : \det u_1 = \cdots = \det u_t \in \mathbf{Z}_\ell^{*k-1} \right\}$$

which satisfies:

(i) $\det \mathscr{G} = \mathbf{Z}_\ell^{*k-1}$.

(ii) *The image of $\mathscr{G}$ "mod ℓ" contains $\prod_{i=1}^{t} \mathbf{SL}(2, O_i/\ell O_i)$.*

Then $\mathscr{G} = \mathscr{A}$.

Proof. Clear.

Theorem (2.3). *Let $\mathscr{G}$ be a compact semi-simple subgroup of $\mathbf{GL}(2, K)$, where K is a finite extension of $\mathbf{Q}_\ell$. Suppose that G has an open abelian subgroup $\mathscr{N}$, but that $(\mathscr{G} : \mathscr{G} \cap K^*) = \infty$. Then G has an open abelian subgroup of index 1 or 2.*

Proof. By replacing $\mathscr{N}$ be the intersection of its (finitely many) conjugates in $\mathscr{G}$, we can assume that $\mathscr{N}$ is normal. One sees that $\mathscr{N}$ is semi-simple because $\mathscr{G}$ is, so $\mathscr{N}$ consists of diagonalizable elements. Moreover $\mathscr{N} \not\subset K^*$ because $\mathscr{N}$ is of finite index in $\mathscr{G}$. Thus there exists a diagonalizable $n \in \mathscr{N}$ with distinct eigenvalues. Since $\mathscr{N}$ is abelian and normal in $\mathscr{G}$, n commutes with gng^{-1} for every $g \in \mathscr{G}$. From this one sees directly by a matrix calculation in $\mathbf{GL}(2, \bar{K})$ that the inter-

section of $\mathcal{G}$ with the centralizer of n in $\mathbf{GL}(2, K)$ has index 1 or 2 in $\mathcal{G}$ and also that the centralizer is abelian. This gives what we want.

§ 3. Group Theory (bis.)

We fix a positive even integer k as in the previous section. We write $\mathbf{GL}(2, q)$ for $\mathbf{GL}(2, \mathbf{F}_q)$ if q is a prime power; similar conventions will be in force for $\mathbf{PGL}(2)$, $\mathbf{PSL}(2)$, etc. In analogy with our terminology concerning "semi-simple subgroups," we will say that a subgroup G of $\mathbf{GL}(2, q)$ is *irreducible* if the inclusion $G \hookrightarrow \mathbf{GL}(2, q)$ is an irreducible representation of G over $\mathbf{F}_q$. This means that G leaves invariant no 1-dimensional subspace of the $\mathbf{F}_q$-vector space $\mathbf{F}_q \times \mathbf{F}_q$.

We now let ℓ be a prime $\geqq 5$, and let $q_1, \ldots, q_t$ be powers of ℓ. We remark that the product

$$M = \mathbf{F}_{q_1} \times \cdots \times \mathbf{F}_{q_t}$$

is an $\mathbf{F}_\ell$-algebra, so we have a canonical injection $\mathbf{F}_\ell \hookrightarrow M$. This injection allows us say that a given element of M *belongs to* $\mathbf{F}_\ell$. Note that if $x \in \mathbf{F}_\ell$ and

$$y = (c_1, \ldots, c_t) \in M,$$

then the statement that y *equals* x means that

$$c_1 = c_2 = \cdots = c_t = x.$$

Theorem (3.1). *Suppose that G is a subgroup of*

$$A = \{(u_1, \ldots, u_t) \in \mathbf{GL}(2, q_1) \times \cdots \times \mathbf{GL}(2, q_t) : \det((u_1, \ldots, u_t)) \in \mathbf{F}_\ell^{*k-1}\}$$

which satisfies

(i) $\det: G \to \mathbf{F}_\ell^{*k-1}$ *is surjective.*

(ii) *G contains an element x such that $(\mathrm{tr}\, x)^2$ generates the $\mathbf{F}_\ell$-algebra M.*

(iii) *The image of each projection $p_i: G \to \mathbf{GL}(2, q_i)$ is an irreducible subgroup of $\mathbf{GL}(2, q_i)$ whose order is divisible by ℓ.*

Then $G = A$.

The proof of the theorem will be given after a series of preliminary results.

First suppose that B and B' are groups and that A is a subgroup of $B \times B'$ for which the two projections $p: A \to B$, $p': A \to B'$ are *surjective*. Let N be the kernel of p' and N' be the kernel of p, so that N "is" a normal subgroup of B and N' "is" a normal subgroup of B'. The following result appears as an exercise in Bourbaki (*Algebra*, Ch I, p. 124).

Lemma (3.2) ("Goursat's Lemma"). *The image of A in $B/N \times B'/N'$ is the graph of an isomorphism*

$$B/N \xrightarrow{\sim} B'/N'.$$

Lemma (3.3). *Let $S_1, S_2, \ldots, S_t$ $(t > 1)$ be finite groups with no non-trivial abelian quotients. Let G be a subgroup of*

$$S = S_1 \times \cdots \times S_t$$

such that each projection

$$G \to S_i \times S_j$$

$(1 \leqq i < j \leqq t)$ *is surjective. Then* $G = S$.

Proof (Serre). The lemma is clearly true if $t = 2$. We assume inductively that $t > 2$ and that the lemma is true for $t - 1$. By symmetry it is enough to prove that G contains S_1, i.e., $S_1 \times \{1\}$. For this, by hypothesis, it is enough to prove that G contains all commutators $aba^{-1}b^{-1}$ with $a, b \in S_1$. Given a and b, by using the induction assumption we may choose elements c of S_2 and d of S_3 such that

$$(a, c, 1, \ldots, 1)$$

and

$$(b, 1, d, 1, \ldots, 1)$$

belong to G. Then the commutator of these elements, namely

$$(aba^{-1}b^{-1}, 1, \ldots, 1)$$

also belongs to G.

Using the same argument we get a profinite variant of the above "two principle":

Lemma (3.4). *Let* $\mathscr{S}_1, \ldots, \mathscr{S}_t$ $(t > 1)$ *be profinite groups. Assume for each* i *that the following condition is satisfied: for each open subgroup* $\mathscr{U}$ *of* $\mathscr{S}_i$, *the closure of the commutator subgroup of* $\mathscr{U}$ *is open in* $\mathscr{S}_i$. *Let* $\mathscr{G}$ *be a closed subgroup of*

$$\mathscr{S} = \mathscr{S}_1 \times \cdots \times \mathscr{S}_t$$

which maps to an open subgroup of each group $\mathscr{S}_i \times \mathscr{S}_j (i \neq j)$. *Then* $\mathscr{G}$ *is open in* $\mathscr{S}$.

Remarks

1. In (3.3), it is not quite necessary to assume that every group S_i is its own commutator subgroup. It suffices to assume that the condition holds for all but two of the groups. Similarly for (3.4).

2. In the profinite version, the condition on commutator subgroups will hold for $\mathscr{S}_i$ if $\mathscr{S}_i$ is an ℓ-adic Lie group whose Lie algebra is its own derived algebra.

3. Similarly, the condition on commutator subgroups holds if $\mathscr{S}_i$ is a product $\prod_\alpha \mathscr{S}_\alpha$, where each S_α satisfies the commutator subgroup condition, provided that for all but finitely many $\mathscr{S}_\alpha$ the commutator subgroup $[\mathscr{S}_\alpha, \mathscr{S}_\alpha]$ is dense in $\mathscr{S}_\alpha$. In particular, the condition is satisfied by $\prod_\ell \mathbf{SL}(2, \mathbf{Z}_\ell)$. Thus by combining (3.4) with Theorem 6 of [8] we may extend that theorem (which concerns a product of two elliptic curves) to the case of a product of two *or more* elliptic curves.

More precisely, let $E_1, \ldots, E_t$ $(t > 1)$ be elliptic curves over a number field K. For each i and each prime ℓ, let

$$\rho_{\ell,i}\colon \mathrm{Gal}(\bar{K}/K) \to \mathrm{Aut}(T_{\ell,i})$$

be the ℓ-adic representation attached to E_i. Let

$$\mathscr{A}_\ell = \left\{(M_1, \ldots, M_t) \in \prod_{i=1}^{t} \mathrm{Aut}(T_{\ell,i}) : \det M_1 = \cdots = \det M_t\right\}$$

for each ℓ, and let

$$\mathscr{A}_\infty = \prod_\ell \mathscr{A}_\ell,$$

the product being extended over all primes. Let

$$\psi : \mathrm{Gal}(\bar{K}/K) \to \mathscr{A}_\infty$$

be the map giving the action of $\mathrm{Gal}(\bar{K}/K)$ on

$$\prod_{i=1}^{t} \prod_\ell T_{\ell,i}.$$

Theorem (3.5). *Assume for each distinct pair of integers i, j that the systems of ℓ-adic representations $(\rho_{\ell,i})$ and $(\rho_{\ell,j})$ associated to E_i and E_j become isomorphic over no finite extension of K. Assume also that no elliptic curve E_i has complex multiplication over $\bar{K}$. Then the image of φ is open in $\mathscr{A}_\infty$.*

Proof. As usual, it suffices to prove that the image of ψ contains the group

$$\mathscr{S} = \prod_{i=1}^{t} \prod_\ell \mathbf{SL}(T_{\ell,i})$$

consisting of elements of $\mathscr{A}_\infty$ with determinant 1. For this, we apply (3.4) to the intersection $\mathscr{G} = \mathscr{S} \cap \psi(\mathrm{Gal}(\bar{K}/K))$, using ([8], Th. 6) to verify the hypothesis on $\mathscr{G}$.

In addition, we will use the following two results in our proof of (3.1):

Proposition (3.6) (Dickson, [2]). *Let p be a prime $\geqq 5$ and let $q = p^n$. Suppose that G is a subgroup of* **PSL**$(2, q)$ *which has order divisible by p and which is "irreducible" in the sense that it acts without fixed points on* $\mathbf{P}^1(\mathbf{F}_q)$. *Then there is a subfield K of $\mathbf{F}_q$ such that G is conjugate in* **PGL**$(2, q)$ *either to* **PGL**$(2, K)$ *or to* **PSL**$(2, K)$.

Proposition (3.7) (Dieudonné-Hua). *Let K be a field of characteristic different from 2, and let φ be an automorphism of the group* **PGL**$(2, K)$ (resp., **PSL**$(2, K)$). *Then φ is the composition of an inner automorphism of* **PGL**$(2, K)$ (resp., the restriction to **PSL**$(2, K)$ of an inner automorphism of **PGL**$(2, K)$) *with the automorphism of* **PGL**$(2, K)$ (resp., **PSL**$(2, K)$) *induced by a field automorphism of K.*

The statement relative to **PGL**$(2, K)$ is proved in [4]. The statement relative to **PSL**$(2, K)$ is proved in [3] – see p. 91 and 98, especially.

Example. The automorphism $u \mapsto (u^{-1})^t$ is obtained by conjugating by

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

Proof of (3.1)

The Case $t=1$. Let $q=q_1$, and let $\bar{G}$ (resp., $\bar{A}$) be the image of G (resp., A) in $\mathbf{PGL}(2, q)$. We have

$$\bar{G} \subseteq \bar{A} \subseteq \mathbf{PSL}(2, q^2).$$

It follows from (iii) that $\bar{G}$ acts without fixed points on $\mathbf{P}^1(\mathbf{F}_{q^2})$. By (3.6) there is a subfield K of $\mathbf{F}_{q^2}$ such that $\bar{G}$ is conjugate in $\mathbf{PGL}(2, q^2)$ either to $\mathbf{PSL}(2, K)$ or to $\mathbf{PGL}(2, K)$. By (ii), $K \supseteq \mathbf{F}_q$. (The point is that, with x as in (ii), the element $(\operatorname{tr} x)^2/(\det x)$ generates $\mathbf{F}_q$ and depends only on the conjugacy class of the image of x in $\mathbf{PGL}(2, q^2)$.) Thus a conjugate of $\bar{G}$ in $\mathbf{PGL}(2, q^2)$ contains $\mathbf{PSL}(2, q)$. Accordingly, there is a conjugate G' of G in $\mathbf{GL}(2, q^2)$ such that

$$\mathbf{F}_{q^2}^* \cdot G' \supseteq \mathbf{SL}(2, q).$$

Since $\mathbf{SL}(2, q)$ has no non-trivial abelian quotients, it follows that $G' \supseteq \mathbf{SL}(2, q)$. Hence

$$G' \cap \mathbf{SL}(2, q^2) \supseteq \mathbf{SL}(2, q) = A \cap \mathbf{SL}(2, q^2) \supseteq G \cap \mathbf{SL}(2, q^2).$$

Since the order of the first term equals the order of the last we get $G \supseteq \mathbf{SL}(2, q)$. It now follows from (i) that $G = A$.

The Case $t=2$. Let $q_1=\ell^n$, $q_2=\ell^m$. Let B (resp., B') be the image of A in $\mathbf{GL}(2, \ell^n)$ (resp., $\mathbf{GL}(2, \ell^m)$). By the argument just given, the two projections $G \to B$, $G \to B'$ are surjective. Let N' and N be their respective kernels. We shall obtain a contradiction from the assumption $G < A$.

In fact, under this assumption we clearly have $N \subseteq \{\pm 1\}$ and $N' \subseteq \{\pm 1\}$, since N (for example) is a normal subgroup of $\mathbf{SL}(2, \ell^n)$ which cannot be equal to all of $\mathbf{SL}(2, \ell^n)$. By (3.2) the image of G in $B/N \times B'/N'$ is the graph of an isomorphism

$$\alpha\colon\ B/N \xrightarrow{\sim} B'/N'.$$

Since α maps the center of B/N onto the center of B'/N', α induces an isomorphism

$$\bar{\alpha}\colon\ B/C \xrightarrow{\sim} B'/C',$$

where C and C' are the respective centers of B and B'. Now B/C is isomorphic either to $\mathbf{PSL}(2, \ell^n)$ or to $\mathbf{PGL}(2, \ell^n)$, depending on the parity of n, and a similar statement holds for B'/C'. This imples first of all that $n=m$. (Look at orders.) Then by (3.7) there exist elements $S \in \mathbf{GL}(2, \ell^n)$ and $\sigma \in \mathrm{Gal}(\mathbf{F}_{\ell^n}/\mathbf{F}_\ell)$ so that for each (u, u') in G we have

$$u' = \varepsilon \cdot (SuS^{-1})^\sigma,$$

where ε is a scalar (which depends on u and u'). Now

$$\det u = \det u' \in \mathbf{F}_\ell^*$$

from the definition of A, so we get $\varepsilon^2 = 1$. Thus: if $(u, u') \in G$, then

$$(\operatorname{tr} u')^2 = [(\operatorname{tr} u)^2]^\sigma.$$

This contradicts (ii).

The General Case. We may suppose that $t>1$. By (i) it suffices to show that the intersection H of G with

$$\mathbf{SL}(2, q_1)\times\cdots\times\mathbf{SL}(2, q_t)$$

is equal to this product. The case treated immediately above shows that each projection

$$H\to\mathbf{SL}(2, q_i)\times\mathbf{SL}(2, q_j)\qquad(i\neq j)$$

is surjective. Now by (3.3) we get the desired equality.

The final result of this section is a "corollary" of the argument given above for the case $t=2$. Here again ℓ is a prime $\geqq 5$, and q and q' are powers of ℓ. Also, k' is a positive even integer, which may or may not be equal to k. We let A be the subgroup of

$$\mathbf{GL}(2, q)\times\mathbf{GL}(2, q')$$

consisting of pairs (u, u') which satisfy the following condition:

There exists a $v\in\mathbf{F}_\ell^*$ *for which*

$$\det u = v^{k-1}$$

and

$$\det u' = v^{k'-1}.$$

Theorem (3.8). *Suppose that G is a subgroup of A whose projections B and B' onto* $\mathbf{GL}(2, q)$ *and* $\mathbf{GL}(2, q')$ *are the same as those of A. Suppose also that $G\neq A$. Then $q=q'$, and there exists an element*

$$\sigma\in\mathrm{Gal}(\mathbf{F}_q/\mathbf{F}_\ell)$$

and a character

$$\varepsilon\colon\ G\to\mathbf{F}_q^*$$

such that, for each (u, u') in G, we have

$$\mathrm{tr}\,u' = \varepsilon(u, u')\cdot(\mathrm{tr}\,u)^\sigma,$$

$$\det u' = [\varepsilon(u, u')]^2\cdot(\det u).$$

Proof. Let N' and N be the kernels of the projections of G onto B and B' respectively. Since N is normal in $B\supseteq\mathbf{SL}(2, q)$, either $N\subseteq\{\pm 1\}$ or else $N\supseteq\mathbf{SL}(2, q)$. The latter case can be ruled out by Goursat's Lemma. Indeed, let N_A' and N_A be the kernels of the projections of A onto B and B' respectively. One checks easily that the indices $(N_A:\mathbf{SL}(2, q))$ and $(N_A':\mathbf{SL}(2, q'))$ are relatively prime. By Goursat's Lemma we have isomorphisms

$$B/N\simeq B'/N',$$

$$B/N_A\simeq B'/N_A'.$$

Under the assumption that we are in the latter case, the first isomorphism gives $N'\supseteq\mathbf{SL}(2, q')$; and the two together give

$$(N_A:N)=(N_A':N').$$

By the relative primality we then get $N=N_A$ and $N'=N'_A$, contradicting the assumption that G is a proper subgroup of A. Thus we do have $N\subseteq\{\pm 1\}$, and similarly $N'\subseteq\{\pm 1\}$.

We can now argue as above to deduce that $q=q'$ and that there are elements $\sigma\in\mathrm{Gal}(\mathbf{F}_q/\mathbf{F}_\ell)$, $S\in GL(2,q)$ such that for each (u,u') in G there is a scalar ε such that

$$u'=\varepsilon\cdot(SuS^{-1})^\sigma.$$

The conclusions can be read off from this.

§ 4. Modular Forms "mod ℓ"

We first review the Serre/Swinnerton-Dyer theory of modular forms "mod ℓ" [9, 11], working with modular forms over $\bar{\mathbf{F}}_\ell$, rather than over $\mathbf{F}_\ell$.

If R is a ring we let $M_k(R)$ be the R-module of modular forms of weight k for $SL(2,\mathbf{Z})$ over R; this is written $M(R,1,k)$ in [5]. A modular form $f\in M_k(R)$ has a *q-expansion*

$$\sum_{n=0}^{\infty} a_n(f)\,q^n\in R[[q]],$$

and by abuse we often identify a modular form with its q-expansion. (There is at most one modular form with given q-expansion *and of given weight.*)

Given any homomorphism $\varphi\colon R\to R'$, there is a natural map

$$M_k(R)\otimes_R R'\to M_k(R')$$

taking

$$\left(\sum a_n q^n\right)\otimes b\mapsto\sum b\cdot\varphi(a_n)\,q^n.$$

This map is an isomorphism in the special case where $R=\mathbf{Z}$ and 6 is invertible in R' ([5], (1.8.2)). For example, if ℓ is a prime at least 5, then $M_k(\mathbf{F}_\ell)$ is the vector space

$$M_k(\mathbf{Z})\otimes\mathbf{F}_\ell$$

of reductions "mod ℓ" of ordinary modular forms of weight k with integral q-expansions. We also have the *q-expansion principle*: if R is a subring of R' and $f\in M_k(R')$ has a q-expansion which lies in $R[[q]]$, then f *is* a modular form over R ([5], (1.9.1)).

For the remainder of the section we fix a prime number ℓ greater than 3. For each k, we let

$$\bar{M}_k=M_k(\bar{\mathbf{F}}_\ell)=M_k(\mathbf{F}_\ell)\otimes_{\mathbf{F}_\ell}\bar{\mathbf{F}}_\ell.$$

Let $A\in\bar{M}_{\ell-1}$ be the Hasse invariant, i.e., the image in $\bar{M}_{\ell-1}$ of the normalized Eisenstein series $E_{\ell-1}$ of weight $\ell-1$. Multiplication by A defines for each k an injection

$$\text{"}A\text{"}\colon\ \bar{M}_k\hookrightarrow\bar{M}_{k+\ell-1}$$

which induces the *identity* map on q-expansions. This shows, by the way, that two modular forms of different weights over $\bar{\mathbf{F}}_\ell$ can have the same q-expansion. The "structure theorem" of Swinnerton-Dyer is the following

Theorem (4.1). *Suppose that $f \in \overline{M}_k$ and $f' \in \overline{M}_{k'}$ have the same q-expansions and suppose that $k \geqq k'$. Then*

$$k \equiv k' \mod(\ell - 1),$$

and

$$f = A^t \cdot f',$$

where $t = (k-k')/(\ell-1)$.

[The theorem is proved essentially in this form by Katz [5], (4.4.2).]

Definition. The *filtration* of a modular form $f \in \overline{M}_k$ is the quantity

$$w(f) = \inf\{k' : \exists\, g \in \overline{M}_{k'} \text{ s.t. } \dot{\sum} a_n(g)\, q^n = \sum a_n(f)\, q^n\}.$$

One checks easily the following:

(i) $w(0) = -\infty$.

(ii) If f and g have the same q-expansions (but not necessarily the same weights) then $w(f) = w(g)$.

(iii) If $0 \neq f \in \overline{M}_k$, then $w(f)$ is an integer congruent to $k \bmod (\ell - 1)$.

We will use repreatedly the following result [9].

Theorem (4.2). *For each k there exists a unique map*

$$\theta : \overline{M}_k \to \overline{M}_{k+\ell+1}$$

which induces the map

$$q \frac{d}{dq} : \sum a_n q^n \mapsto \sum n a_n q^n$$

on q-expansions. If f has filtration k and $\ell \nmid k$, then θf has filtration $k + \ell + 1$.

Corollary (4.3). *If $\ell \nmid k$, then θ is injective on $\overline{M}_k$.*

Lemma (4.4). *Let $f \in \overline{M}_k$ and $g \in \overline{M}_{k'}$ be non-zero modular forms with $k \geqq k'$. Suppose that t is a non-negative integer such that*

$$a_n(f) = n^t\, a_n(g)$$

for all n prime to ℓ. Then t is congruent $\bmod(\ell - 1)$ either to $(k-k')/2$ or else to $(k'-k+\ell-1)/2$. Moreover, if $\ell \geqq k + k'$, then $k = k', f = g$, and t is a multiple of $(\ell - 1)$.

Proof. The hypothesis says precisely that θf and $\theta^{t+1} g$ have the same q-expansions. Their weights must then be congruent mod $(\ell - 1)$ because of (4.1); thus

$$2t \equiv k - k' \mod(\ell - 1),$$

leading to the two possibilities given above.

We now suppose that $\ell \geqq k + k'$. If we assume that the first possibility is the case, i.e., that θf and $\theta^{1+(k-k')/2} g$ have the same q-expansions, then (4.2) gives the equality between filtrations

$$k + \ell + 1 = k' + \ell + 1 + (k - k') \cdot (\ell + 1)/2,$$

which forces $k = k'$. We then have $\theta f = \theta g$, and by (4.3) this gives $f = g$. On the other hand, the second possibility leads to an equation that is never true.

Corollary (4.5). *Let f be a non-zero element of $\overline{M}_k$ such that $a_n(f)=0$ whenever $\left(\frac{n}{\ell}\right)=-1$. Then $2k>\ell$.*

Proof. We have

$$a_n(f)=n^{(\ell-1)/2}\cdot a_n(f)$$

whenever n is prime to ℓ.

Remark. For numerical work, it is useful to improve the result as follows: under the hypothesis of (4.5), ℓ is either $2k-1$ or $2k-3$ or else is less than k. This follows from the filtration argument beginning near the bottom of p. 29 of [11]. (But note that there should be an extra "$\ell+1$" on the right-hand side of the first displayed equation in the argument.)

Lemma (4.6). *Let $f=\sum a_n q^n$ be a non-zero element of $\overline{M}_k$ which is a "cusp form," i.e., satisfies $a_0(f)=0$. Suppose that there exist integers m and m' mod$(\ell-1)$ such that*

$$m+m'\equiv k-1 \quad \text{mod}(\ell-1)$$

and such that for all n prime to ℓ we have

$$a_n=n^m\,\sigma_{m'-m}(n),$$

where as usual

$$\sigma_t(n)=\sum_{d\mid n} d^t$$

for any t. Then either $\ell\leqq k+1$ or ℓ divides the numerator of b_k/k, where b_k is the k-th Bernoulli number [9].

Proof. Since f is non-zero, k is an even positive integer. Thus $m+m'$ is an odd number mod$(\ell-1)$, so we can choose m and m' to be (represented by) integers satisfying

$$0\leqq m<m'<\ell-1.$$

We will treat only the case where

$$1<m'-m<\ell-2;$$

the two remaining cases $m'-m=1$, $\ell-2$ are similar [11]. Let g be the image in $\overline{M}_{m'-m+1}$ of the Eisenstein series $G_{m'-m+1}$ of weight $m'-m+1$ and q-expansion

$$-b_k/2k+\sum_{n=1}^{\infty}\sigma_{m'-m}(n)\,q^n\in\mathbf{Q}[[q]].$$

(The q-expansion is "ℓ-integral," so it does make sense to reduce $G_{m'-m+1}$ "mod ℓ,") It follows directly from the hypothesis that θf and $\theta^{m+1}g$ have the same q-expansions. One sees from (4.2) that the latter modular form has filtration

$$m'-m+1+(m+1)(\ell+1)$$

and that the former has filtration $k+\ell+1$ provided that $\ell>k+1$. These numbers must be equal, so we get $m=0$, $m'=k-1$. Thus we have

$$\theta f=\theta g$$

since these modular forms have the same weights and q-expansions. By (4.3) we get $f=g$, which gives in particular $a_0(g)=a_0(f)=0$, as required.

§ 5. Theorems for One Modular Form

In this section we begin our study of ℓ-adic representations attached to modular forms. First, let k be an even integer such that the complex vector space S_k of cusp forms of weight k on $\mathbf{SL}(2, \mathbf{Z})$ has positive dimension. (In other words, k must be even, at least 12, but not 14.) Let H_k be the $\mathbf{Z}$-subring of End S_k generated by all Hecke operators T_n, and let $E_k = H_k \otimes \mathbf{Q}$ be the corresponding $\mathbf{Q}$-algebra. For each ℓ, let $\rho_{\ell,k}$ be the ℓ-adic representation attached to cusp forms of weight k. By construction, this is a map

$$\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{Aut}\, T_{\ell,k},$$

where $T_{\ell,k}$ is a certain free $\mathbf{Z}_\ell$-module of rank $2 \cdot \dim S_k$ on which $H_k \otimes \mathbf{Z}_\ell$ acts $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$-linearly. The vector space

$$V_{\ell,k} = T_{\ell,k} \otimes_{\mathbf{Z}_\ell} \mathbf{Q}_\ell$$

is a *free* $E_k \otimes \mathbf{Q}_\ell$-module of rank 2 under this action.

Now let f be a cusp form of weight k which is a normalized eigenform for the Hecke operators. This means that f is an element

$$q + a_2 q^2 + \cdots$$

of S_k which satisfies

$$f | T_n = a_n \cdot f$$

for all $n \geqq 1$. Let E_f (resp. H_f) be the field (resp. ring) generated by all the complex numbers a_n; then E_f is a totally real number field, and H_f is an order in the ring of integers O_f of E_f. Also, E_f (resp. H_f) is the image of E_k (resp. H_k) under the natural map

$$E_k \to \mathbf{C}$$

for which $T_n \mapsto a_n$ for all n. For each prime ℓ, put

$$V_{\ell,f} = V_{\ell,k} \otimes_{(E_k \otimes \mathbf{Q}_\ell)} (E_f \otimes \mathbf{Q}_\ell),$$

and let $T_{\ell,f}$ be the image of $T_{\ell,k}$ in $V_{\ell,f}$. Let $\rho_{\ell,f}$ be the ℓ-adic representation

$$\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{Aut}\, T_{\ell,f} \subset \mathrm{Aut}\, V_{\ell,f},$$

the *ℓ-adic representation attached to f*. In this section we shall simply write ρ_ℓ instead of $\rho_{\ell,f}$, reserving the full notation for § 7 (when we have several modular forms). Analogously, we simplify notation by writing T_ℓ for $T_{\ell,f}$, O for O_f, H for H_f, etc.

From the properties of the representations $\rho_{\ell,k}$ given above and in the introduction, we easily deduce:

(i) ρ_ℓ is unramified at each prime $p \neq \ell$.

(ii) The action of $H \otimes_{\mathbf{Z}} \mathbf{Q}_\ell = E \otimes_{\mathbf{Q}} \mathbf{Q}_\ell$ on V_ℓ makes V_ℓ into a free module of rank 2 over $E \otimes_{\mathbf{Q}} \mathbf{Q}_\ell$.

(iii) The action of $H \otimes_{\mathbf{Z}} \mathbf{Z}_\ell$ on T_ℓ makes T_ℓ into a free $H \otimes \mathbf{Z}_\ell$-module of rank 2 provided that $\ell \nmid (O:H)$.

(iv) If p is a prime $\neq \ell$ and $F_p \in \rho_\ell(\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}))$ is an ("arithmetic") Frobenius element for p, then the characteristic polynomial $\det(1 - t \cdot F_p)$ giving the action of F_p on the $E \otimes \mathbf{Q}_\ell$-module V_ℓ is

$$1 - a_p t + p^{k-1} t^2,$$

where $a_p = a_p(f)$.

Remarks

1. Let λ be a prime of E and let ℓ be its residue characteristic. Exploiting the canonical projection of $E \otimes \mathbf{Q}_\ell$ onto E_λ we get a λ-adic representation

$$\rho_\lambda \colon \mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}) \xrightarrow{\rho_\ell} \mathrm{Aut}_{(E \otimes \mathbf{Q}_\ell)} V_\ell \to \mathrm{Aut}_{E_\lambda} V_\lambda,$$

where $V_\lambda = V_\ell \otimes_{(E \otimes \mathbf{Q}_\ell)} E_\lambda$. It is immediate that the system (ρ_λ) of λ-adic representations thus constructed is a strictly compatible system with empty "exceptional set" S and Frobenius polynomials

$$P_p(t) = 1 - a_p t + p^{k-1} t^2.$$

Note that a given ρ_ℓ can be recovered from the system (ρ_λ) via the decomposition

$$V_\ell = \prod_{\lambda \mid \ell} V_\lambda.$$

2. By the Čebotarev Density Theorem one deduces from (iv) that the determinant of ρ_ℓ taken relative to $E \otimes \mathbf{Q}_\ell$ is the $(k-1)^{\mathrm{st}}$ power of the cyclotomic character

$$\chi_\ell \colon \mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}) \to \mathbf{Q}_\ell^* \subset (E \otimes \mathbf{Q}_\ell)^*.$$

Since the image of χ_ℓ is $\mathbf{Z}_\ell^*$, we have

$$\det(\rho_\ell \, \mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})) = \mathbf{Z}_\ell^{*\,k-1}.$$

Note that

$$E \otimes \mathbf{Q}_\ell = \prod_{\lambda \mid \ell} E_\lambda;$$

to say that an element $(\ldots, e_\lambda, \ldots)$ of $E \otimes \mathbf{Q}_\ell$ belongs to $\mathbf{Z}_\ell^{*\,k-1}$ means that each entry in the tuple belongs to $\mathbf{Q}_\ell$ and moreover that the entries are all *equal*, the common value being the $(k-1)^{\mathrm{st}}$ power of a unit.

3. Since f is an eigenform for the Hecke operators, the coefficients $a_n = a_n(f)$ of the q-expansion of f are determined by the numbers a_p for p prime. Indeed, as is well known, we have

$$a_n \cdot a_m = a_{nm} \quad \text{if } (n, m) = 1$$

and

$$a_{p^{n+1}} = a_p \cdot a_{p^n} - p^{k-1} a_{p^{n-1}}$$

for p prime and $n \geqq 1$. This fact will be used repeatedly.

4. Because of the theory of the Petersson inner product, E_k is a commutative semi-simple algebra, in fact the product of totally real fields. Hence E_f is isomorphic to a direct factor of E_k. Moreover, every factor of E_k is of this form. That is, there is a set Σ_k of normalized eigenforms of weight k so that

$$E_k \xrightarrow{\sim} \bigoplus_{g \in \Sigma_k} E_g .$$

We will use this decomposition in § 7.

It follows from Remark 2 that the image $\mathscr{G}_\ell$ of ρ_ℓ is contained in

$$\mathscr{A}_\ell = \{u \in \mathrm{Aut}_{(H \otimes \mathbf{Z}_\ell)} T_\ell \colon \det u \in \mathbf{Z}_\ell^{*(k-1)}\} .$$

(Note that this group, more properly written $\mathscr{A}_{\ell,f}$, is the image in Aut T_ℓ of the group we called $\mathscr{A}_\ell$ in the introduction.)

Theorem (5.1). *For almost all primes ℓ we have $\mathscr{G}_\ell = \mathscr{A}_\ell$.*

Proof. Let us say that a prime ℓ is good (for f) if $\ell \geqq 5$, $\ell \nmid (O:H)$, and ℓ is unramified in E. It is clear that almost all primes are good, so that we may ignore the "bad" primes in proving the theorem. If ℓ is good, then T_ℓ is free of rank 2 over $H \otimes \mathbf{Z}_\ell$ because of (iii). We choose for each such ℓ an $H \otimes \mathbf{Z}_\ell$-basis of T_ℓ; then $\mathscr{G}_\ell$ and $\mathscr{A}_\ell$ may be viewed as subgroups of $\mathbf{GL}(2, H \otimes \mathbf{Z}_\ell)$.

Step 0 (Application of group theory). If ℓ is good, let G_ℓ (resp. A_ℓ) be the image of $\mathscr{G}_\ell$ (resp., $\mathscr{A}_\ell$) "mod ℓ," i.e., in $\mathbf{GL}(2, H/\ell H)$. Thus

$$G_\ell \subseteq A_\ell = \{u \in \mathbf{GL}(2, H/\ell H) \colon \det u \in \mathbf{F}_\ell^{*k-1}\} .$$

We have an *a priori* equivalence

$$G_\ell = A_\ell \quad \text{if and only if} \quad \mathscr{G}_\ell = \mathscr{A}_\ell .$$

In fact, if $G_\ell = A_\ell$, then the equality $\mathscr{G}_\ell = \mathscr{A}_\ell$ follows easily from (2.2) together with Remark 2.

On the other hand, the results of § 3 give conditions sufficient for the equality $G_\ell = A_\ell$. For $\lambda | \ell$ let G_λ be the image of G_ℓ in $\mathbf{GL}(2, H/\lambda)$. Then

$$G_\ell \subseteq \prod_{\lambda | \ell} G_\lambda \subseteq \prod_{\lambda | \ell} \mathbf{GL}(2, H/\lambda) = \mathbf{GL}(2, H/\ell H).$$

Using (3.1) we see that $G_\ell = A_\ell$ whenever the following two conditions are satisfied:

I. For each $\lambda | \ell$, the group G_λ has order divisible by ℓ and acts H/λ-irreducibly on $H/\lambda \times H/\lambda$.

II. There exists an element $u \in G_\ell$ such that $(\mathrm{tr}\, u)^2$ generates the $\mathbf{F}_\ell$-algebra $H/\ell H$.

Step 1 (Proof of I for almost all ℓ). Here we must prove for almost all good ℓ an assertion concerning the primes λ dividing ℓ. We shall say that a prime λ of E is good if its residue characteristic ℓ is good. Then the object is to show for almost all good λ that G_λ is irreducible (in the sense of § 3) and has order divisible by the residue characteristic of λ.

Our main tool will be the modular form f_λ obtained by reducing f mod λ. Formally, we regard f as an element of $M_k(H)$ (which is permissible by the "q-

expansion principle") and let f_λ be the image of f under the canonical map

$$M_k(H) \to M_k(H/\lambda).$$

Since

$$M_k(H/\lambda) \subseteq M_k(\overline{H/\lambda}) \text{ "}=\text{" } M_k(\bar{\mathbf{F}}_\ell),$$

the lemmas at the end of § 4 apply to f_λ. We note that the coefficients $a_n(f_\lambda)$ of the q-expansion of f_λ are given by the rule: $a_n(f_\lambda)$ is the image of $a_n \pmod{\lambda}$.

Lemma (5.2). *For almost all good λ the group G_λ acts irreducibly.*

Proof. Let λ be a good prime such that G_λ acts *reducibly*. We shall show that the residue characteristic ℓ of λ satisfies: either $\ell \leqq k+1$ or ℓ divides the numerator of $b_k/2k$. To see this, let ρ be the representation

$$\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}) \xrightarrow{\rho_\ell} \mathbf{GL}(2, H \otimes \mathbf{Z}_\ell) \to \mathbf{GL}(2, H/\lambda)$$

whose image is G_λ. Since ρ is (by assumption) reducible, there are characters

$$\varphi, \varphi' \colon \mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}) \to (H/\lambda)^*$$

so that ρ may be represented in matrix form as

$$\begin{pmatrix} \varphi & * \\ 0 & \varphi' \end{pmatrix}.$$

Since ρ is unramified at primes different from ℓ, and since $(H/\lambda)^*$ has order prime to ℓ, φ and φ' are each powers of the cyclotomic character "mod ℓ," i.e., the character

$$\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}) \xrightarrow{\chi_\ell} \mathbf{Z}_\ell^* \to \mathbf{F}_\ell^*.$$

There are thus integers m and m' (defined mod $(\ell-1)$) such that for each $p \neq \ell$ we have

$$\det(1 - F \cdot t) = 1 - (p^m + p^{m'})\, t + p^{m+m'} t^2,$$

where F is a Frobenius element for p in $\rho(\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}))$. Comparing this with "axiom" (iv), we get congruences (mod λ)

$$a_p \equiv p^m + p^{m'},$$
$$p^{k-1} \equiv p^{m+m'}$$

for each $p \neq \ell$. The second gives

$$m + m' \equiv k - 1 \pmod{(\ell-1)}.$$

The first gives us for *all* n prime to ℓ

$$a_n(f_\lambda) \equiv n^m \sigma_{m'-m}(n) = n^m \sum_{d \mid n} d^{m'-m},$$

since f is an eigenfunction. The desired conclusion now follows from (4.6).

Lemma (5.3). *For almost all good λ the group G_λ has order divisible by ℓ, the residue characteristic of λ.*

Proof. If G_λ has order prime to ℓ, then one of the following must hold ([8], Prop. 16):

(i) G_λ is abelian.

(ii) The image $\bar{G}_\lambda$ of G_λ in $\mathbf{PGL}(2, H/\lambda)$ is dihedral.

(iii) The group $\bar{G}_\lambda$ as above is isomorphic to one of the following "exceptional" groups: $\mathbf{S}_4, \mathbf{A}_4, \mathbf{A}_5$.

We shall show that each of these cases can appear only a finite number of times.

In case (i), G_λ must act reducibly, since a simple abelian subgroup of $\mathbf{GL}(2, H/\lambda)$ could not contain the element of G_λ with eigenvalues $+1$, -1 provided by a "complex conjugation" in $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$. Thus (5.2) already shows that this case occurs only a finite number of times.

In case (ii), $\bar{G}_\lambda$ is an extension of $\{\pm 1\}$ by a cyclic group C, and every element of $\bar{G}_\lambda$ not in C has order 2. Thus every element of G_λ which does not map to C has trace 0. On the other hand, the map

$$\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}) \to G_\lambda \to \bar{G}_\lambda \to \{\pm 1\}$$

is surjective and unramified at primes other than ℓ, and must therefore be the quadratic character $\left(\frac{-}{\ell}\right)$. These two facts together give

$$a_p(f_\lambda) = 0 \quad \text{if } \left(\frac{p}{\ell}\right) = -1.$$

It follows that $a_n(f_\lambda) = 0$ for each non-residue $n \bmod \ell$. By (4.5) we get $\ell < 2k$.

Case (iii) is more complicated. We use the fact that every element of $\bar{G}_\lambda$ has order $1, 2, 3, 4$, or 5. From this it follows that for each $u \in G_\lambda$ the quantity $(\mathrm{tr}\, u)^2/(\det u)$ is $4, 0, 1, 2$, or else a root of $x^2 - 3x + 1 = 0$. Thus for each $p \neq \ell$, one of the following elements of H will be congruent to 0 (mod λ):

$$a_p^2 - 4p^{k-1},\ a_p^2,\ a_p^2 - p^{k-1},\ a_p^2 - 2p^{k-1},\ a_p^4 - 3p^{k-1}a_p^2 + p^{2(k-1)}.$$

Now let us assume that there are *infinitely* many good λ which fall into case (iii). Then for each prime p one of the five elements listed above must be 0. Choose one good λ with residue characteristic $\ell \geqq 7$ such that λ falls into case (iii). Applying the Čebotarev Density Theorem in $\bar{G}_\lambda$ we see that there are infinitely many $p \neq \ell$ whose Frobenius elements in $\bar{G}_\lambda$ are the identity. For those p we have $a_p^2 \equiv 4p^{k-1}$ (mod λ); looking at the above list we see that this implies $a_p^2 = 4p^{k-1}$ (equality in H) because $\ell \geqq 7$. Since k is even (being the weight of a non-zero modular form for $\mathbf{SL}(2, \mathbf{Z})$), this equation can hold only if p ramifies in the field E. But only finitely many primes can ramify in a number field, so this gives a contradiction.

Remark 5. Suppose that λ is a good prime which falls into case (iii) and which is of degree 1 (i.e., $H/\lambda = \mathbf{F}_\ell$). Then, following [11], we can show that λ satisfies some restrictive criteria. First of all, the group $\bar{G}_\lambda$ must be $\mathbf{S}_4$ (rather than $\mathbf{A}_4$ or $\mathbf{A}_5$) because it has a subgroup of index 2 ([11], p. 16). Further, since the quadratic character of $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ obtained by mapping $\bar{G}_\lambda$ to its quotient of order 2 is unramified except at ℓ, it follows that any prime $p \neq \ell$ whose Frobenius elements in $\mathbf{S}_4$ do not lie in the subgroup $\mathbf{A}_4$ must in fact be a non-residue (mod ℓ). By the

Čebotarev Density Theorem, there exist primes p whose Frobenii are the 4-cycles in $\mathbf{S}_4$; such primes are non-residues (mod ℓ) for which we have

$$a_p^2 - 2p^{k-1} \equiv 0 \pmod{\lambda}.$$

We deduce that 2 is not a square in H/λ, or in other words that

$$\ell \equiv \pm 3 \pmod 8.$$

Using the fact that 2 is not a square in H/λ, one can show that λ divides one of the three numbers

$$a_2,\ a_2 - 2^{k/2},\ a_2 + 2^{k/2}$$

([11], p. 30). Finally, the argument on pp. 30–31 of [11] shows that 3 divides the class number of the quadratic field which is unramified only at ℓ. These are all *necessary* criteria for a prime of degree 1 to fall into case (iii).

Step 2 (Proof of II for almost all ℓ). In order to prove II for almost all ℓ we must first establish the equality $G_\ell = A_\ell$ for an infinite set of ℓ.

Lemma (5.4). *Suppose that a good ℓ satisfies:*

(a) *All primes $\lambda | \ell$ are of degree* 1 (i.e., ℓ splits completely in E).

(b) *For $\lambda | \ell$, G_λ acts irreducibly and has order divisible by ℓ* (i.e., condition I holds for ℓ).

(c) $\ell \geqq 2k$.

Then $G_\ell = A_\ell$.

(Given Step 1, it is clear that the hypotheses will be satisfied by an infinite set of primes ℓ.)

Proof. Since $\det(G_\ell) = \mathbf{F}_\ell^{*\,k-1}$, it suffices to prove that G_ℓ contains $\mathbf{SL}(2, H/\ell H)$. However, it is easy to see from (a) and (b) that G_λ contains $\mathbf{SL}(2, H/\lambda) = \mathbf{SL}(2, \mathbf{F}_\ell)$ for each $\lambda | \ell$. Thus in particular we are done if $d = 1$.

Let us suppose that $d > 1$. By (3.3) it suffices to show for each pair $\lambda, \lambda' (\lambda \neq \lambda')$ that the image G of G_ℓ in

$$\mathbf{GL}(2, H/\lambda \times H/\lambda')$$

contains

$$\mathbf{SL}(2, H/\lambda \times H/\lambda').$$

We have *a priori* $G \subseteq A$, where A is the image of A_ℓ in

$$\mathbf{GL}(2, H/\lambda \times H/\lambda'),$$

and the point is to show that $G = A$.

Assuming that $G < A$ we get by (3.8) a character

$$\varepsilon\colon G \to \{\pm 1\}$$

such that for each $(u, u') \in G$ we have

$$\operatorname{tr} u' = \varepsilon(u, u') \cdot \operatorname{tr} u.$$

Let φ be the composition of ε with the representation

$$\rho\colon \mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}) \to \mathbf{GL}(2, H/\lambda) \times \mathbf{GL}(2, H/\lambda')$$

with image G. Then φ is unramified at all primes $p \neq \ell$. Thus there are only two possibilities: φ is the unit character (identically 1) or ρ is the quadratic character $\left(\frac{\cdot}{\ell}\right)$. Consider the first possibility. Here we have

$$a_p(f_\lambda) = a_p(f_{\lambda'})$$

for all $p \neq \ell$. (The equation makes sense because H/λ and H/λ' are "the same," being each isomorphic to the prime field $\mathbf{F}_\ell$.) In other words, we have $\theta f_\lambda = \theta f_{\lambda'}$. By (4.3) and (c), $f_\lambda = f_{\lambda'}$ and hence

$$a_n(f_\lambda) = a_n(f_{\lambda'})$$

for all n. This obviously contradicts the fact that

$$H/\ell H = \prod_{\lambda \mid \ell} H/\lambda \simeq \mathbf{F}_\ell \times \cdots \times \mathbf{F}_\ell \quad (d \text{ times}).$$

We now consider the second possibility. This time we get

$$a_n(f_\lambda) = n^{(\ell-1)/2} \cdot a_n(f_{\lambda'})$$

for all n prime to ℓ. We then get a contradiction from (4.4) because of (c). [*Variant:* one could also apply (4.5) to the sum

$$f_\lambda + f_{\lambda'} \in M_k(\mathbf{F}_\ell)$$

to get a contradiction.]

Corollary. *There exist infinitely many primes p such that a_p^2 generates the field E.*

Proof. It is obvious that if $\ell \gg 0$ and ℓ splits completely in E there is a $u \in A_\ell$ such that $(\mathrm{tr}\, u)^2$ generates the $\mathbf{F}_\ell$-algebra $H/\ell H$. By the lemma we can find such good ℓ for which $G_\ell = A_\ell$. Applying the Čebotarev Density Theorem to G_ℓ we see that there exist infinitely many primes p such that the image of a_p^2 in $H/\ell H$ generates $H/\ell H$. This gives us what we want.

Choose one prime p for which a_p^2 generates E. Then the subring of H generated by a_p^2 has finite index in H. Suppose that ℓ is a good prime $\neq p$ which does not divide this index. Then condition II holds for ℓ with u taken to be a Frobenius element for p in G_ℓ. Thus II holds for almost all (good) ℓ. This completes the proof of (5.1).

Remark 6. The proof of the theorem is not effective because the Čebotarev Density Theorem was applied in two places. We needed it just above to provide a prime p for which a_p^2 generates E. Earlier we needed it to show that there exists a prime p for which none of the five quantities

$$a_p^2,\ a_p^2 - 4p^{k-1}, \ldots$$

is zero. In practice, however, these conditions seem to be satisfied by just about "any old p." If 5 is not a square in E, then the second condition can be met by

taking p to be any prime unramified in E for which $a_p \neq 0$. For example, if f is the eigenform

$$E_6^2 \Delta + (1572 + 12\sqrt{144169}) \cdot \Delta^2$$

of weight 24, one can obviously satisfy both conditions by taking $p=2$. For an analysis of the representations in this case, see § 8.

A complement to (5.1) is

Theorem (5.5). *For every prime ℓ, the image $\mathscr{G}_\ell$ of ρ_ℓ is open in $\mathscr{A}_\ell$.*

Proof. We wish to apply (1.2) to the system (ρ_λ) discussed in Remark 1. For this, define $\mathscr{B}_\ell$ as in (1.2); then $\mathscr{G}_\ell$ is open in $\mathscr{A}_\ell$ if and only if $\mathscr{G}_\ell$ is open in $\mathscr{B}_\ell$.

To show that (ρ_λ) satisfies the hypotheses to (1.2), we must prove a statement concerning "non-abelian semi-simplifications." Let λ be a prime of E, and let $\mathscr{G} \subseteq \mathrm{Aut}_{E_\lambda} V_\lambda$ be the image of the semi-simplification of ρ_λ. We first show that the index

$$(\mathscr{G} : \mathscr{G} \cap E_\lambda^*)$$

is infinite. Indeed, if this index were finite the Čebotarev Density Theorem would imply the existence of an infinite number of primes whose Frobenius elements in $\mathscr{G}$ would belong to $\mathscr{G} \cap E_\lambda^*$. For such primes p we would have $a_p^2 = 4p^{k-1}$, contrary to the fact that only finitely many primes can ramify in E.

It now follows that for each finite extension K of $\mathbf{Q}$ (in a fixed $\bar{\mathbf{Q}}$) the semi-simplification of $\mathrm{res}_K(\rho_\lambda)$ is non-abelian. In fact, if any such semi-simplification were abelian, there would be a *quadratic* field K for which the semi-simplification of $\mathrm{res}_K(\rho_\lambda)$ would be abelian, by (2.3). Then, by (1.1), the semi-simplification of $\mathrm{res}_K(\rho_{\lambda'})$ would be abelian for every prime λ' of E. This clearly contradicts (5.1): the image of $\mathrm{res}_K(\rho_{\lambda'})$ will act irreducibly and non-abelianly on $V_{\lambda'}$ whenever the residue characteristic ℓ' of λ' is such that $\mathscr{G}_{\ell'} = \mathscr{A}_{\ell'}$. Our conclusion is that (ρ_λ) does satisfy the hypotheses to (1.2).

Now using (1.2) we see that the assertion that $\mathscr{G}_\ell$ is open in $\mathscr{B}_\ell$ is independent of ℓ: it is true for all ℓ or none at all. But the assertion has already been proven true for almost all good primes ℓ by (5.1) – clearly $\mathscr{A}_\ell$ is open in $\mathscr{B}_\ell$. Hence the assertion is true for all ℓ.

§ 6. Pairs of Modular Forms

Let $f = \sum a_n q^n$ and $f' = \sum a'_n q^n$ be normalized eigenforms as in § 5, with weights $k \geqq k'$ respectively. Define $E, H, \ldots$ (resp., $E', H', \ldots$) as in § 5. Our aim is to show that the ℓ-adic representations attached to f are "as independent as possible" of the ℓ-adic representations attached to f'. In slightly more concrete terms, the object is to prove that the images of the ℓ-adic representations

$$(\rho_\ell, \rho'_\ell) \colon \mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{Aut}(V_\ell \times V'_\ell)$$

are as large as possible. As in the previous section there are two separate problems: to describe the image exactly for almost all ℓ, and to compute the Lie algebra of the image for every ℓ. We will treat only the first problem: the Lie algebra computation is then a corollary which the reader will be spared. (One argues as in (5.5); the point is that (1.2) remains valid if E is replaced by a product of fields.)

For the remainder of this section we shall make the following hypothesis on the pair (f,f'):

If f and f' have the same weight k, then the $\mathbf{Q}$-algebra generated by pairs (a_n, a'_n), $n=1, 2, \ldots$ is equal to $E \times E'$.

The hypothesis means that if f and f' have weight k, then they correspond to *different* factors of the Hecke algebra E_k, which is to say that they are *not* conjugate under the action of $\mathrm{Aut}(\mathbf{C})$ on modular forms.

Let us fix the following notation. We let $\mathbf{T}$ be the $\mathbf{Z}$-subring of $H \times H'$ generated by the pairs (a_n, a'_n). By hypothesis, the index $(H \times H' : \mathbf{T})$ is finite if $k=k'$. (It is automatically finite if $k \neq k'$, but we will not use this.) Also, suppose that ℓ is a good prime both for f and f'. Let $\mathscr{G}_\ell$ and $\mathscr{A}_\ell$ be defined as in § 5 for f, and define $\mathscr{G}'_\ell$ and $\mathscr{A}'_\ell$ similarly for f'. Let $\mathscr{G}''_\ell$ be the image of (ρ_ℓ, ρ'_ℓ). Then $\mathscr{G}''_\ell$ is a subgroup of

$$\mathscr{G}_\ell \times \mathscr{G}'_\ell \subseteq \mathscr{A}_\ell \times \mathscr{A}'_\ell \subseteq (\mathrm{Aut}_{H \otimes \mathbf{Z}_\ell} T_\ell) \times (\mathrm{Aut}_{H' \otimes \mathbf{Z}_\ell} T'_\ell).$$

Since the determinants of ρ_ℓ and ρ'_ℓ are respectively the $(k-1)^{\text{st}}$ and the $(k'-1)^{\text{st}}$ powers of the cyclotomic character χ_ℓ, the image group $\mathscr{G}''_\ell$ is actually contained in

$$\mathscr{A}''_\ell = \{(u, u') \in \mathscr{A}_\ell \times \mathscr{A}'_\ell : \det u = v^{k-1},\ \det u' = v^{k'-1} \text{ for some } v \in \mathbf{Z}_\ell^*\}.$$

Of course, a *necessary* condition that $\mathscr{G}''_\ell = \mathscr{A}''_\ell$ is that $\mathscr{G}_\ell = \mathscr{A}_\ell$ and $\mathscr{G}'_\ell = \mathscr{A}'_\ell$.

Theorem (6.1). *Suppose that ℓ is a good prime for f and f' such that $\mathscr{G}_\ell = \mathscr{A}_\ell$ and $G'_\ell = \mathscr{A}'_\ell$. Suppose further that $\ell \geqq k+k'$. Then if $k \neq k'$ we have $\mathscr{G}''_\ell = \mathscr{A}''_\ell$. If $k=k'$, we have $\mathscr{G}''_\ell = \mathscr{A}''_\ell$ provided that ℓ does not divide the index of $\mathbf{T}$ in $H \times H'$.*

Proof. The first step is to see that it suffices to prove that $\mathscr{G}''_\ell$ and $\mathscr{A}''_\ell$ are equal "mod ℓ." In fact, using (2.1) and the surjectivity of

$$\chi_\ell : \mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}) \to \mathbf{Z}_\ell^*,$$

one proves easily that the equality $\mathscr{G}''_\ell = \mathscr{A}''_\ell$ is a consequence of the equality $G''_\ell = A''_\ell$, where these are the respective images of G''_ℓ and $\mathscr{A}''_\ell$ in

$$\mathrm{Aut}_{H/\ell H}(T_\ell/\ell T_\ell) \times \mathrm{Aut}_{H'/\ell H'}(T'_\ell/\ell T'_\ell).$$

After choosing bases we have

$$G''_\ell \subseteq A''_\ell \subseteq \mathbf{GL}(2, H/\ell H \times H'/\ell H').$$

Given (3.3) and the equalities $G_\ell = A_\ell$, $G'_\ell = A'_\ell$ deduced "mod ℓ" from our supposed equalities, it is enough to show for each prime $\lambda | \ell$ of H and each prime $\lambda' | \ell$ of H' that the projection G of G''_ℓ onto

$$\mathbf{GL}(2, H/\lambda \times H'/\lambda')$$

is the same as the projection A of A''_ℓ onto this group. (I.e., by (3.3), this statement implies $G''_\ell = A''_\ell$.) We have

$$G \subseteq A = \{(u, u') \in \mathbf{GL}(2, H/\lambda \times H'/\lambda') : \det u = v^{k-1},\ \det u' = v^{k'-1} \text{ for some } v \in \mathbf{F}_\ell^*\}.$$

By hypothesis, the projections of G onto $\mathbf{GL}(2, H/\lambda)$ and $\mathbf{GL}(2, H'/\lambda')$ are the same as those of A.

Now suppose that $G<A$ for some λ, λ'. Then by (3.8) there is an isomorphism

$$\sigma\colon H'/\lambda' \xrightarrow{\sim} H/\lambda$$

and a character

$$\varepsilon\colon G \to (H/\lambda)^*$$

such that for each $(u, u') \in G$ we have

$$\operatorname{tr} u = \varepsilon(u, u') \cdot (\operatorname{tr} u')^\sigma,$$
$$\det u = \varepsilon(u, u')^2 \cdot \det u'.$$

(We can regard $\det u'$ as an element of H/λ, since it is in the prime field.) Since all our representations are unramified except possibly at ℓ, the composition

$$\operatorname{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}) \to G \xrightarrow{\varepsilon} (H/\lambda)^*$$

is a power of the cyclotomic character (mod ℓ). Thus there is an integer t (defined mod $(\ell-1)$) such that

$$a_p(f_\lambda) = p^t \cdot (a_p(f'_{\lambda'}))^\sigma,$$
$$p^{k-1} \equiv p^{2t} \cdot p^{k'-1} \pmod{\ell}$$

for all $p \neq \ell$. We thus have

$$\theta f = \theta^{(t+1)}(f'_{\lambda'})^\sigma,$$

where $(f'_{\lambda'})^\sigma$ is the image of $f'_{\lambda'}$ under the map on modular forms induced by σ. Since $\ell \geqq k+k'$, we find from (4.5) that $k=k'$ and that

$$f_\lambda = (f'_{\lambda'})^\sigma.$$

In particular, our assumption $G<A$ is not possible when $k \neq k'$, so we already have the desired conclusion in that case.

We continue by deducing from the above equality of modular forms the equality of their q-expansions: for all $n \geqq 1$ we have

$$a_n (\operatorname{mod} \lambda) = \sigma[a'_n (\operatorname{mod} \lambda')].$$

It follows that the pairs (a_n, a'_n) do not generate $H/\lambda \times H'/\lambda'$; thus they certainly do not generate $H/\ell H \times H'/\ell H'$. This contradicts the fact that ℓ does not divide the index of $\mathbf{T}$ in $H \times H'$, which we assumed in case $k=k'$.

Corollary (6.2). *We have $\mathscr{G}''_\ell = \mathscr{A}''_\ell$ for almost all ℓ.*

§ 7. Proof of the Main Theorem

Here we wish to deduce the main theorem (0.1) from the results in the previous two sections. Since we have already abandoned Lie algebra questions in § 6, we will speak only about assertion 1 of the theorem – the assertion having to do with the exact images of $\operatorname{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$. Just as in the previous section, the result on Lie algebras follows as a corollary.

Recall that we are given r distinct integers k_i and that we wish to consider the ℓ-adic representations

$$\rho_\ell = \rho_{\ell,k_1} \times \cdots \times \rho_{\ell,k_r}.$$

For each ℓ, ρ_ℓ gives the action of $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ on

$$T_\ell = T_{\ell,k_1} \times \cdots \times T_{\ell,k_r},$$

where the latter T's are the modules introduced in § 5. If ℓ is prime to the integer $(\mathcal{O}:\mathcal{H})$ – where $\mathcal{O} = \Pi O_{k_i}$ and $\mathcal{H} = \Pi H_{k_i}$ as in the introduction – then T_ℓ is free of rank 2 over $\mathcal{H} \otimes Z_\ell$, and ρ_ℓ maps $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ into $\mathrm{Aut}_{\mathcal{H}\otimes \mathbf{Z}_\ell} T_\ell$. What is to be proved (for almost all such ℓ) is that the image $\mathcal{G}_\ell$ of $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ is the group

$$\mathcal{A}_\ell = \{u \in \mathrm{Aut}_{\mathcal{H}\otimes \mathbf{Z}_\ell} T_\ell \colon \det u \in \mathbf{Z}_\ell^{*(k-1)}\},$$

where $\mathbf{Z}_\ell^{*(k-1)}$ is the rather complicated group defined in the introduction.

We can reformulate the result so that $\mathbf{Z}_\ell^{*(k-1)}$ does not appear. Namely, the product representation $\rho_\ell \times \chi_\ell$ maps $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ to

$$\mathcal{C}_\ell = \{(u_1, \ldots, u_r; v) \in (\mathrm{Aut}_{H\otimes \mathbf{Z}_\ell} T_\ell) \times \mathbf{Z}_\ell^* \colon \det u_i = v^{k_i - 1} \ (1 \leqq i \leqq r)\}.$$

This is a subgroup of $\mathrm{Aut}_{H\otimes \mathbf{Z}_\ell} T_\ell \times \mathbf{Z}_\ell^*$ whose projection onto the first factor is $\mathcal{A}_\ell$. Thus if the image of $\rho_\ell \times \chi_\ell$ is $\mathcal{C}_\ell$, then the image of ρ_ℓ is $\mathcal{A}_\ell$. Conversely, if ρ_ℓ maps $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ onto $\mathcal{A}_\ell$, then the image of $\rho_\ell \times \chi_\ell$ contains

$$\mathcal{D} \times \{1\},$$

where $\mathcal{D}$ is the closure of the commutator subgroup of $\mathrm{SL}_{H\otimes \mathbf{Z}_\ell} T_\ell$. If $\ell \geqq 5$, $\ell \nmid (\mathcal{O}:\mathcal{H})$, and ℓ is unramified in $\mathcal{O}$ (we shall call such ℓ *good* as in § 5), then $\mathcal{D}$ is all of $\mathrm{SL}_{\mathcal{H}\otimes \mathbf{Z}_\ell} T_\ell$. Consequently, the image of $\rho_\ell \times \chi_\ell$ must be all of $\mathcal{C}_\ell$ because of the surjectivity of χ_ℓ.

Thus the result to be proved is equivalent to

Theorem (7.1). *For almost all ℓ, the image of $\rho_\ell \times \chi_\ell$ is $\mathcal{C}_\ell$.*

Now let $\mathbf{Q}(\mu_{\ell^\infty})$ be the field obtained by adjoining all ℓ-power roots of unity to $\mathbf{Q}$. Then the surjectivity of χ_ℓ implies that the image of $\rho_\ell \times \chi_\ell$ is $\mathcal{C}_\ell$ if and only if

$$\rho_\ell(\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}(\mu_{\ell^\infty}))) = \mathrm{SL}_{\mathcal{H}\otimes \mathbf{Z}_\ell} T_\ell.$$

Theorem (7.2) *(Cyclotomic reformulation). For almost all ℓ, ρ_ℓ maps*

$$\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}(\mu_{\ell^\infty})) \quad \textit{onto} \quad \mathrm{SL}_{\mathcal{H}\otimes \mathbf{Z}_\ell} T_\ell.$$

Proof of (7.2). We may suppose that ℓ is good (see above). Let

$$\mathcal{S} = \rho_\ell(\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}(\mu_{\ell^\infty}))),$$

viewed as a subgroup of $\mathbf{SL}(2, H \otimes \mathbf{Z}_\ell)$. We have a decomposition

$$\mathcal{H} \otimes \mathbf{Z}_\ell \xrightarrow{\sim} \bigoplus_f (H_f \otimes \mathbf{Z}_\ell),$$

where the direct sum is taken over the set of eigenfunctions

$$\Sigma = \bigcup_i \Sigma_{k_i}.$$

(See Remark 4 of § 5.) For each $f \in \Sigma$, let S_f be the image of $\mathscr{S}$ in $\mathbf{SL}(2, H_f \otimes \mathbf{Z}_\ell)$. For each *pair* of distinct eigenfunctions $f, f' \in \Sigma$, let $S_{f,f'}$ be the image of $\mathscr{S}$ in

$$\mathbf{SL}(2, H_f \otimes \mathbf{Z}_\ell) \times \mathbf{SL}(2, H_{f'} \otimes \mathbf{Z}_\ell).$$

By (3.3) and (2.1), $\mathscr{S} = \mathbf{SL}(2, \mathscr{H} \otimes \mathbf{Z}_\ell)$ if the following conditions are satisfied:

(i) For each $f \in \Sigma$, $S_f = \mathbf{SL}(2, H_f \otimes \mathbf{Z}_\ell)$.

(ii) For each distinct pair $f, f' \in \Sigma$,

$$S_{f,f'} = \mathbf{SL}(2, H_f \otimes \mathbf{Z}_\ell) \times \mathbf{SL}(2, H_{f'} \otimes \mathbf{Z}_\ell).$$

These statements are proved for almost all ℓ by (5.1) and (6.1) respectively: one merely has to restate these propositions in the style of (7.2), using the commutator argument above.

One can restate (0.1) as a theorem involving one representation of $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$. Namely, let $\rho_\infty : \mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}) \to \prod_\ell \mathscr{A}_\ell$ be the product of all representations ρ_ℓ as ℓ runs over the set of primes. Since each representation ρ_ℓ is ramified only at ℓ, the image of ρ_∞ is the product $\Pi \mathscr{G}_\ell$, where $\mathscr{G}_\ell$ is the image of ρ_ℓ. (The rational field $\mathbf{Q}$ has no unramified extensions.) Then by the Main Theorem we have

Theorem (7.3). *The image of ρ_∞ is open in $\Pi \mathscr{A}_\ell$.*

Galois Groups over $\mathbf{Q}$

The Main Theorem makes a contribution to the problem of determining which finite simple groups occur as Galois extensions of $\mathbf{Q}$. Let A_ℓ be the image of $\mathscr{A}_\ell$ in $\mathbf{GL}(2, \mathcal{O}/\ell\mathcal{O})$. Then the theorem implies that for almost all ℓ the group A_ℓ occurs as the Galois group of some finite extension $K/\mathbf{Q}$. On the other hand, suppose that ℓ is unramified in $\mathcal{O}$ and at least 5, and let $\mathbf{F}$ be one of the "pieces" of $\mathcal{O}/\ell\mathcal{O}$ in its decomposition as a product of fields. A quick calculation shows that the image of A_ℓ in $\mathbf{PGL}(2, \mathbf{F})$ is a quotient of A_ℓ equal to either $\mathbf{PSL}(2, \mathbf{F})$ or $\mathbf{PGL}(2, \mathbf{F})$ according as the degree of $\mathbf{F}$ over its prime field is even or odd. Therefore:

For almost all maximal ideals λ of $\mathcal{O}$ for which $\mathcal{O}/\lambda$ has even degree over its prime field, the group $\mathbf{PSL}(2, \mathcal{O}/\lambda)$ *may be realized as the Galois group of some extension* $K/\mathbf{Q}$.

In particular, let us consider the representations $\rho_{\ell,24}$ which occur in § 8. For these representations, $\mathcal{O}$ is the integer ring of the quadratic field $\mathbf{Q}(\sqrt{144169})$. Thus:

For all prime numbers $\ell \neq 47$ for which 144169 *is a non-square* (mod ℓ), *the group* $\mathbf{PSL}(2, \mathbf{F}_{\ell^2})$ *occurs as a Galois group over* $\mathbf{Q}$.

The list of finite simple groups which are known to occur as Galois groups over $\mathbf{Q}$ is a very short one. (See the "Queries" section of the A.M.S. *Notices* for November, 1973 and February, 1974.) Aside from the groups provided by results such as the above, the only series of simple Galois groups of the form $\mathbf{PSL}(2, \mathbf{F}_{p^n})$ which has been systematically constructed over $\mathbf{Q}$ consists of the groups $\mathbf{PSL}(2, \mathbf{F}_p)$ for which p is a prime such that 2, 3, or 7 is a non-residue (mod p) [10]. Note that

the groups $\mathbf{PSL}(2, \mathbf{F}_4)$ and $\mathbf{PSL}(2, \mathbf{F}_9)$ occur as well: they are isomorphic to $\mathbf{A}_5$ and $\mathbf{A}_6$ respectively.

§ 8. The Representations $\rho_{\ell, 24}$

This section is a report on the representations attached to the space S of cusp forms of weight 24 for $\mathbf{SL}(2, \mathbf{Z})$. This space is spanned by the forms

$$A = \Delta^2 = q^2 + *q^3 + 1080q^4 + \cdots,$$
$$B = \Delta E_6^2 = q - 1032q^2 + *q^3 + 10965568q^4 + \cdots,$$

where we use "$*$" to denote an unspecified integer.

We find that

$$A|T_2 = B + 2112A,$$
$$B|T_2 = -1032B + 18289152A,$$

so that the characteristic polynomial of T_2 acting on S is

$$X^2 - 1080X - 20468736,$$

which has roots

$$540 \pm 12\sqrt{144169}.$$

(The number 144169 is prime, as was noticed by Hecke.) It follows that the two normalized eigenforms of weight 24 are

$$f = B + (1572 + 12\sqrt{144169})A = \Sigma a_n q^n$$

and its conjugate obtained by changing the sign of the square root. Note especially that

$$a_2 = 540 + 12\sqrt{144169}.$$

As a matter of convenience, we study the family of representations $(\rho_{\ell, f})$ rather than the family $(\rho_{\ell, 24})$; as mentioned in § 5, this just means that we are viewing H_{24} as embedded in $\mathbf{C}$ by means of the map

$$T_n \mapsto a_n.$$

The image of H_{24} in $\mathbf{C}$ is the order of index 24 in the ring of integers of $\mathbf{Q}(\sqrt{144169})$. Let us adopt the notations of §5: G_ℓ, A_ℓ, etc. Then we wish to find a list of the "exceptional" primes ℓ for which $\mathscr{G}_\ell \neq \mathscr{A}_\ell$. We do this by following the proof of (5.1).

Since we want to consider only "good" primes, we must first throw out 2, 3, and 144169. For the remaining primes, we have $\mathscr{G}_\ell = \mathscr{A}_\ell$ whenever I and II hold for ℓ. In fact, II holds for all ℓ except (2, 3, and) 5. This follows immediately from the equation

$$a_2^2 = * + 2^5 \cdot 3^4 \cdot 5\sqrt{144169}.$$

To examine I, let us imagine that we are given a good prime λ with residue characteristic ℓ.

Irreducibility

As in the proof of (5.2), G_λ is irreducible unless $\ell \leqq 25$ *or* ℓ divides the numerator of $b_{24}/48$. The primes dividing this numerator are 103 and 2294797.

Divisibility (Cases i and ii)

In case (i), G_λ acts reducibly, so there are no new primes. For case (ii) we have to worry about all primes $\ell \leqq 24$ and the prime 47 (see the remark after (4.5)).

Divisibility (Case iii)

This is the case with the most computation, but it turns out that there are no new primes to add to the list. It is best to distinguish two subcases:

Subcase: $\lambda = (\ell)$ is of degree 2.

Here we use only the fact that λ must divide one of the numbers

$$x_1 = a_2^2 - 4 \cdot 2^{23},$$
$$x_2 = a_2^2,$$
$$x_3 = a_2^2 - 2 \cdot 2^{23},$$
$$x_4 = a_2^2 - 1 \cdot 2^{23},$$
$$x_5 = a_2^4 - 3 \cdot 2^{23} a_2^2 + 2^{46}.$$

For each i, write

$$x_i = y_i + z_i \sqrt{144169}$$

with $x_i, y_i \in \mathbf{Z}$. Then if λ divides x_i, ℓ divides z_i. Now

$$z_1 = \cdots = z_4 = 2^5 \cdot 3^4 \cdot 5;$$
$$z_5 = 2^{11} 3^5 \cdot 5 \cdot 47 \cdot 1877.$$

Aside from 2, 3, 5, the only primes which occur here are 47 and 1877. But 47 has already been singled out in case (ii), while 1877 splits in $\mathbf{Q}(\sqrt{144169})$.

Subcase: λ is of degree 1.

In this subcase we use the necessary conditions listed at the end of the case (iii) discussion of § 5 (Remark 5). A first condition is that λ must divide one of the numbers

$$a_2, \ a_2 \pm 2^{12},$$

which implies that ℓ divides the norm of one of these numbers. Up to sign, these norms are

$$2^{10} 3^2 \cdot 2221,$$
$$2^{10} \cdot 5 \cdot 11 \cdot 13,$$
$$2^{10} \cdot 5^2 \cdot 317.$$

So the only possible primes ℓ which can trouble us are 317 and 2221. To eliminate these, it suffices to know that the class numbers $h(317)$ and $h(2221)$ are prime to 3. In fact, both of them are 1; the first value is well-known, and the second was supplied to me by Yamamoto.

Summary of the (Possibly) Exceptional Primes

ℓ	*First Source of Difficulty*
2, 3	Less than 5 (group theory fails)
144169	Ramifies in $\mathbf{Q}(\sqrt{144169})$
5	II may not be verified
7, 11, 13, 17, 19, 23	Possibly of type (i) or type (ii)
103, 2294797	"Bernoulli primes": representation reducible
47	Possibly of type (ii)

Comments on These Primes

Two of these primes are not exceptional. First, let λ be the prime of $\mathbf{Q}(\sqrt{144169})$ lying over the rational prime $\ell = 144169$. To see that $\mathscr{G}_\ell = \mathscr{A}_\ell$, it suffices by (2.1) to prove that their images G_ℓ and A_ℓ in $\mathbf{GL}(2, H/\ell H)$ are equal. Now A_ℓ is the semi-direct product of "$A_\ell \bmod \lambda$" $= \mathbf{GL}(2, \mathbf{F}_\ell)$ with the additive group

$$\mathbf{sl}(2, \mathbf{F}_\ell) = \{u \in \mathbf{M}(2, \mathbf{F}_\ell) \colon \operatorname{tr} u = 0\},$$

the former acting (irreducibly) by conjugation on the latter. The arguments of § 5 show that G_ℓ maps surjectively to $\mathbf{GL}(2, \mathbf{F}_\ell)$. On the other hand, G_ℓ contains non-zero elements of $\mathbf{sl}(2, \mathbf{F}_\ell)$, e.g., F_2^{144168}, where F_2 is a Frobenius element in G_ℓ for the prime $p = 2$. The irreducibility of the action of $\mathbf{GL}(2, \mathbf{F}_\ell)$ on $\mathbf{sl}(2, \mathbf{F}_\ell)$ then shows that $G_\ell = A_\ell$. Secondly, one can show that $\rho_{23} \pmod{23}$ maps $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ onto

$$A_{23} = \{u \in \mathbf{GL}(2, \mathbf{F}_{23^2}) \colon \det u \in \mathbf{F}_{23}^*\}.$$

One way to see this is to think of the representation (mod 23) as the representation giving the action of $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ on the 23-division points of the Jacobian variety $J_0(23)$ – some computations based on [6] then give the required result. Then as usual we conclude that $\mathscr{G}_{23} = \mathscr{A}_{23}$.

According to some computations of Serre, the other primes listed above are all in fact exceptional. The representation (mod 47) is like the representation (mod 23) attached to the modular form Δ of weight 12 in that it has a dihedral image (this time of order 10); this fact is essentially equivalent to the congruence for $\Delta^2 \pmod{47}$ (cf. [12], footnote p. 2).

The remaining primes 2, 3, 5, 7, 11, 13, 17, 19, 103, and 2294797 all split in our quadratic field and give rise to two representations of $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ with values in $\mathbf{GL}(2, \mathbf{F}_\ell)$. (If $\ell = 2$ or $\ell = 3$, then ℓ divides $(O\colon H) = 24$; to get representations (mod ℓ) in these cases, one must replace T_ℓ by a $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$-invariant lattice stable under $O \otimes \mathbf{Z}_\ell$.) In each case, one of the representations, at least, is reducible. The other representation is reducible also in case $\ell = 2, 3, 5$, or 7 but is irreducible (and even has large image) in the remaining six cases.

References

1. Deligne, P.: Formes modulaires et représentations ℓ-adiques. Séminaire Bourbaki 355, Février 1969. Lecture Notes in Mathematics **179**. Berlin-Heidelberg-New York: Springer 1971
2. Dickson, L. E.: Linear groups with an exposition of the Galois field theory. Leipzig: Teubner 1901

3. Dieudonné, J.: La géométrie des groupes classiques. Berlin-Heidelberg-Göttingen: Springer 1955
4. Hua, L-K.: Supplement to: On the automorphisms of the classical groups, by J. Dieudonné. AMS Memoirs No. 2. New York: AMS 1951
5. Katz, N.: p-adic properties of modular schemes and modular forms. International Summer School on Modular Functions; Antwerp, 1972. Lecture Notes in Mathematics **350**, 69–190, 1973
6. Ribet, K.: Galois action on division points of abelian varieties with many real multiplications. Harvard thesis, 1971. (To appear in revised form)
7. Serre, J-P.: Abelian ℓ-adic representations and elliptic curves. New York: Benjamin 1968
8. Serre, J-P.: Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. Inventiones math. **15**, 259–331 (1972)
9. Serre, J-P.: Congruences et formes modulaires (d'après H.P.F. Swinnerton-Dyer). Séminaire Bourbaki 416, Juin 1972. Lecture Notes in Mathematics **317**, 319–338, 1973
10. Shih, K.: On the construction of Galois extensions of function fields and number fields. Princeton thesis, 1972
11. Swinnerton-Dyer, H. P. F.: On ℓ-adic representations and congruences for coefficients of modular forms. International Summer School on Modular Functions; Antwerp, 1972. Lecture Notes in Mathematics **350**, 1–55, 1973
12. Wilton, J. R.: Congruence properties of Ramanujan's function $\tau(n)$. Proc. London Math. Soc. **31**, 1–10 (1928)

Kenneth A. Ribet
Princeton University
Department of Mathematics
Fine Hall
Princeton, N.J. 08540, USA

(Received May 29, 1974/January 11, 1975)