PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 125, Number 11, November 1997, Pages 3209–3212
S 0002-9939(97)04085-9

GALOIS REPRESENTATIONS AND HECKE OPERATORS ASSOCIATED WITH THE MOD p COHOMOLOGY OF $GL(1,\mathbb{Z})$ AND $GL(2,\mathbb{Z})$

AVNER ASH

(Communicated by William W. Adams)

ABSTRACT. We prove that any Hecke eigenclass in the mod p cohomology of a congruence subgroup of $GL(1,\mathbb{Z})$ or $GL(2,\mathbb{Z})$ has attached to it a mod p Galois representation such that the characteristic polynomial of a Frobenius element at a prime l equals the Hecke polynomial at l.

0. INTRODUCTION

The aim of this paper is to prove a conjecture about Galois representations attached to cohomology of a congruence subgroup Γ of $GL(n,\mathbb{Z})$ when $n = 1$ or 2. This conjecture was first stated in [A] as "conjecture B" , although there n was taken to be at least 2.

In brief, the conjecture states that to any Hecke eigenclass in the mod p cohomology of Γ there is attached a mod p representation of the absolute Galois group $G_{\mathbb{Q}}$ of $\mathbb{Q}$ such that for almost all primes l, the Hecke polynomial at l equals the characteristic polynomial of a Frobenius element at l. The exact conjecture is given below. It should be thought of as giving mod p nonabelian reciprocity laws.

In a number of lectures I have given on this material, I have asserted that the conjecture "obviously" holds when $n = 1$ or 2 and there have always been questions from the audience as to why. Hence this note. The answer in short: "because of some simple reductions (section 1), plus class field theory for $\mathbb{Q}$ when $n = 1$ (section 2), and Eichler-Shimura theory when $n = 2$ (section 3). "

Thus even when $n = 1$ the statement of the conjecture has nontrivial content, although the arithmetic groups in question have only 1 or 2 elements. When $n = 2$ the proof involves lifting the cohomology to characteristic 0. This could create complications when Γ has torsion, but these are avoided by the lemmas in section 1.

To state the conjecture and establish the notation that will be used throughout this note, let p be a prime number and $\mathbb{F}$ a field of characteristic p. Let n and N be positive integers, and $\mathbb{Q}_{(N)}$ the ring of rational numbers with denominators prime to N.

Received by the editors June 23, 1996.
1991 *Mathematics Subject Classification.* Primary 11F75.
Research partially supported by NSA grant MDA-904-94-2030. This manuscript is submitted for publication with the understanding that the United States government is authorized to reproduce and distribute reprints.

Recall that a Hecke pair (Γ, S) consists of a congruence subgroup Γ of $GL(n,\mathbb{Z})$ and a subsemigroup S of $GL(n,\mathbb{Q})$ that contains Γ . Then to say (Γ, S) is a congruence Hecke pair of level N means that Γ contains the principal congruence subgroup $\Gamma(N)$ of $SL(n,\mathbb{Z})$ of level N and S contains $S_N(N)$. Here $S_R(N)$ denotes the semigroup of integral matrices with positive determinant prime to R and congruent to $diag(1,1,\dots,1,*)$ modulo N. We also require that S be contained in $GL(n,\mathbb{Q}_{(N)})$.

An admissible $\mathbb{F}S$-module M is a right $\mathbb{F}S$-module, finite dimensional over $\mathbb{F}$, on which the elements of S with positive determinant act via their reductions mod N. For generalities about Hecke algebras and their action on cohomology see [Sh], [AS] and [A].

If $D(l,k)$ denotes the diagonal matrix $diag(1,\dots,1,l,\dots,l)$ (with k l's and $n-k$ 1's), let $T(l,k)$ be the Hecke operator corresponding to the double coset $\Gamma D(l,k)\Gamma$. Given a Hecke eigenelement in cohomology, we will let $a(l,k)$ denote its eigenvalue under $T(l,k)$.

Conjecture. *Let (Γ, S) be a congruence Hecke pair of level N. Let M be an admissible $\mathbb{F}S$-module. Suppose $\beta \in H^*(\Gamma, M)$ is an eigenclass for the action of the Hecke algebra $\mathcal{H}(pN)$ (which is a subalgebra of $\mathcal{H}(\Gamma, S)$) with eigenvalues $a(l,k) \in \mathbb{F}$.*

Then there exists a continuous semisimple representation $\rho : G_{\mathbb{Q}} \to GL(n,\mathbb{F})$ unramified outside pN such that

$$\sum_{k=0}^{n}(-1)^k l^{k(k-1)/2} a(l,k)X^k = \det(I - \rho(\mathrm{Frob}_l)^{-1}X)$$

for all l not dividing pN.

For commentary and basic results on the conjecture see [A] and [A1]. For a converse conjecture when $n = 2$ we have Serre's conjecture [Se]. See [AMc] for some numerical evidence when $n = 3$, and [AMa] for some results when $n =$ a multiple of $p - 1$.

1. Logical reductions

With notation as in the conjecture, it follows from Theorem 3.1 of [A] that it suffices to consider the case where Γ equals $\Gamma(N)$ and S is the corresponding semigroup $S_N(N)$.

Let ε denote a character from $(\mathbb{Z}/N)^\times$ to $\mathbb{F}^\times$. Let $\mathbb{F}(\varepsilon)$ denote the one-dimensional admissible module on which $S_N(N)$ acts via determinant mod N composed with ε. Then again by Theorem 3.1 of [A] we can further assume that $M = \mathbb{F}(\varepsilon)$.

(1.1) Lemma. *For a fixed integer j, the conjecture holds for $H^j(\Gamma(N), \mathbb{F}(\varepsilon))$ if and only if it also holds for $H^j(\Gamma(N), \mathbb{F})$.*

Proof. Identify ε with the character of $G_{\mathbb{Q}}$ corresponding to it by class field theory. As far as $\Gamma(N)$ is concerned, $\mathbb{F}(\varepsilon)$ and $\mathbb{F}$ are the same trivial module. So the only effect of twisting by ε is to multiply the Hecke eigenvalue $a(l,k)$ by $\varepsilon(l^k)$. This can be mirrored on the Galois side by tensoring ρ with ε.

(1.2) Lemma. *Let i be a fixed integer. If the conjecture holds for $H^j(\Gamma(N_1), \mathbb{F})$ and $H^j(\Gamma(N_2), \mathbb{F})$ for all $j \le i$, then it also holds for $H^i(\Gamma(N), \mathbb{F})$, where N is the greatest common divisor of N_1 and N_2.*

Proof. Since N is a divisor of N_1, we can consider the Hecke pair $(\Gamma(N), S_{N_1}(N))$ as a congruence Hecke pair of level N_1. By Theorem 3.1 of [A] we see that any system of Hecke eigenvalues (as long as we ignore eigenvalues at primes l that divide N_1) that occurs in $H^i(\Gamma(N), \mathbb{F})$ also occurs in $H^j(\Gamma(N_1), \mathbb{F}(\varepsilon))$ for some ε and some $j \leq i$. By the hypothesis and Lemma 1.1, we conclude the existence of a Galois representation ρ_1 unramified outside pN_1 and whose characteristic polynomial at l equals the Hecke polynomial for β at l for all primes l not dividing pN_1.

Repeating this argument for N_2, we get a representation ρ_2 unramified outside pN_2 with the same property for all l not dividing pN_2. By the Tchebotarev density theorem, ρ_1 and ρ_2 must have the same fixed field and be isomorphic representations. Therefore they are unramified outside pN and have the same characteristic polynomials. Hence either of them has the desired property for all primes l not dividing pN.

(1.3) Lemma. *Let i be a fixed integer. If the conjecture holds for $H^j(\Gamma(N), \mathbb{F})$ for all N greater than 2, and for all $j \leq i$, then it also holds for $H^i(\Gamma(N), \mathbb{F})$, where N equals 1 or 2.*

Proof. Apply the previous lemma.

2. The case $n = 1$

By Lemma 1.3, we may assume that $N \geq 3$ so that Γ is the trivial group. If we denote the degree of the cohomology class β by $*$, then the only nontrivial case is when $* = 0$. We may also assume that M is the trivial module $\mathbb{F}$. So the cohomology is just $\mathbb{F}$ on which the Hecke algebra acts trivially. That is, for each prime l not dividing pN the eigenvalue $a(l, 1) = 1$. Thus the Hecke polynomial at l is $1 - X$. The corresponding ρ is just the trivial Galois representation.

Note that the class field theory for $\mathbb{Q}$ came into the proof of Lemma 1.1.

3. The case $n = 2$

Again we may assume that $N \geq 3$ and that $\Gamma = \Gamma(N)$. In particular Γ is torsion free, in fact a free group, so that we need only look at $* \leq 1$. We may also assume that M is the trivial module $\mathbb{F}$.

First note that if $* = 0$, the conjecture follows from Lemma 4.1.2 and Theorem 4.1.4 of [A], which handle the case $* = 0$ for all n. In fact we could have appealed directly to these results in section 2.

Now let $* = 1$. Let A denote the ring of integers in a finite Galois extension of $\mathbb{Q}$ such that A has $\mathbb{F}$ as a quotient. Let P be a prime ideal in A over p and identify A/P with $\mathbb{F}$. Let π be a uniformizer in the local ring A_P of A localized at P.

From the short exact sequence of multiplication by π, namely $0 \to A_P \to A_P \to \mathbb{F} \to 0$, we get the long exact sequence of cohomology groups:

$$0 \to H^1(\Gamma, A_P) \to H^1(\Gamma, A_P) \to H^1(\Gamma, \mathbb{F}) \to 0.$$

(We use the injectivity of multiplication by π on $H^0(\Gamma, A_P)$ and the fact that Γ has cohomological dimension 1.)

It follows from [AS] that the given system of Hecke eigenvalues on $\beta \in H^1(\Gamma, \mathbb{F})$ can be lifted to $H^1(\Gamma, A_P)$. That is, there exists a Hecke eigenclass $\Delta \in H^1(\Gamma, A_P)$ with Hecke eigenvalues $A(l, k)$ in A_P such that $a(l, k) = A(l, k) \bmod \pi$.

We now choose an embedding of A_P into $\mathbb{C}$ and view Δ as a class in $H^1(\Gamma, \mathbb{C})$. After conjugating the pair (Γ, S) by an appropriate matrix in $GL(2, \mathbb{Q})$, we may

move Δ to be a Hecke eigenclass in $H^1(\Gamma_1(N^2), \mathbb{C})$. Replacing the level N^2 by a divisor m if necessary we may assume that $\Delta \in H^1(\Gamma_1(m), \mathbb{C})$ corresponds to a newform of weight 2 under the Eichler-Shimura map (chap. 8 in [Sh]). In particular, there is attached to this newform a Dirichlet character of level m, its "nebentype". Without loss of generality, we can enlarge A so that it contains the values of this nebentype character. Let A_π denote the completion of A_P.

It now follows that there exists a continuous semisimple representation $\Phi : G_{\mathbb{Q}} \to GL(n, A_\pi)$ unramified outside pN such that

$$\sum_{k=0}^{n} (-1)^k l^{k(k-1)/2} A(l,k) X^k = \det(I - \Phi(\mathrm{Frob}_l)^{-1} X)$$

for all l not dividing pN. This is essentially due to Eichler and Shimura. For the statement for any positive integral weight see for example section 6 of [DS].

We can now take ρ to be Φ mod π.

References

[A] A. Ash, *Galois representations attached to mod p cohomology of $GL(n, \mathbb{Z})$*, Duke Math. J. vol. 65, no.2, (1992), 235-255. MR **93c:**11036

[A1] A. Ash, *Galois representations and cohomology of $GL(n, \mathbb{Z})$*, Seminaire de Theorie des Nombres, Paris, 1989-90, (S. David, ed.), Birkhauser, Boston (1992), 9-22.

[AMa] A. Ash and R. Manjrekar, *Galois Representations and Hecke Operators associated with the mod-p cohomology of $GL(m(p-1), \mathbb{Z})$*, to appear in Math. Zeit.

[AMc] A. Ash and M. McConnell, *Experimental indications of three-dimensional Galois representations from the cohomology of $SL(3, \mathbb{Z})$*, Experimental Math. 1(1992), 209-223. MR **94b:**11045

[AS] A. Ash and G. Stevens, *Cohomology of arithmetic groups and congruences between systems of Hecke eigenvalues*, J. Reine Angew. Math. 365 (1986), 192-220. MR **87i:**11069

[DS] P. Deligne and J.-P. Serre, *Formes modulaires de poids 1*, Ann. Sci. Ec. Norm. Sup. 7 , (1974), 507-530. MR **52:**284

[Se] J.-P. Serre, *Sur les representations modulaires de degre 2 de Gal $(\bar{Q}/Q)$*, Duke J. 54 , (1987), 179-230. MR **88g:**11022

[Sh] G. Shimura, Introduction to the Arithmetic Theory of Automorphic Functions, Princeton U. Press, Princeton, 1971. MR **47:**3318

The Ohio State University, Department of Mathematics, 231 W. 18th Ave, Columbus, Ohio 43210

E-mail address: ash@math.ohio-state.edu