ON A CONJECTURE OF ASH

ADRIAN BARBU
THE OHIO STATE UNIVERSITY
2015 NEIL AVE., COLUMBUS, OH 43210, USA

Abstract. In this paper we prove a particular case of a Conjecture of Ash that states the existence of Galois representations associated to Hecke eigenclasses in cohomology.

e-mail: barbu.3@osu.edu

1. Introduction

In 1992, Professor Avner Ash made the following conjecture (see [Ash], p 242, Conjecture B):

Conjecture 1.1. *(Ash, 1992) Let* (Γ, S) *be a congruence Hecke pair of level* N *and* p *be a prime. Let* $\mathbb{F}$ *be a finite field of characteristic* p. *Let* V *be an admissible* $\mathbb{F}S$ *module. Suppose* $\beta \in H^i(\Gamma, V)$ *is an eigenclass for the action of the Hecke operators* $T_{l,k}$ *with eigenvalues* $a(l,k) \in \mathbb{F}$ *for all primes* l *not dividing* N *and all* $k = 1, ..., n$.

Then there exists a continuous semisimple representation $\rho : G_{\mathbb{Q}} \to GL_n(\mathbb{F})$ *unramified ouside* pN *such that*

$$P(\beta, l) = det(I - \rho(Frob_l)X)$$

for all primes l *not dividing* pN.

Recall that $P(\beta, l) = \sum (-1)^k l^{k(k-1)/2} a(l,k) X^k$.

This conjecture is analogous to the Eichler-Shimura theorem that associates a Galois representation to each modular form which is an eigenform for the Hecke operators.

Let $U_n(\mathbb{F}_p)$ be the group consisting of upper triangular matrices of $GL_n(\mathbb{F}_p)$ with 1 on the diagonal. Also let Γ_U be the congruence subgroup defined by $\Gamma_U = \{M \in SL_n(\mathbb{Z}),\ \overline{M} \in U\}$. We will prove that Conjecture 1.1 holds for Hecke eigenclasses in $H^*(\Gamma_U, \mathbb{F}_p)$ that come from $H^*(U_n(\mathbb{F}_p), \mathbb{F}_p)$ via the reduction mod p map. See Cor. 4.4 below for a precise statement.

We prove:

Theorem 1.2. *Let* $\beta \in H^*(U_n(\mathbb{F}_p), \mathbb{F}_p)$ *be an eigenclass for* $T_{l,k}$ *for all primes* $l \neq p$, *and all* $1 \leq k \leq n$. *Then there is an integer* d *such that the representation*

$$\rho = \omega^d \oplus \omega^{d+1} \oplus ... \oplus \omega^{d+n-1} : G_{\mathbb{Q}} \to GL_n(\mathbb{F}_p), \quad (1)$$

where $G_{\mathbb{Q}} = Gal(\overline{\mathbb{Q}}/\mathbb{Q})$, *has the property that*

$$P(\beta, l) = det(I - \rho(Frob_l)X) \text{ for all } l \neq p.$$

Date: September 6, 2000.

Here $\omega : G_{\mathbb{Q}} \to \mathbb{F}^{\times}$ is the cyclotomic character of conductor p. Thus if ζ is a primitive p-th root of unity, then $\zeta^{\sigma} = \zeta^{\omega(\sigma)}$.

This material was part of a Ph.D. thesis at the Ohio State University under the supervision of Professor Avner Ash.

2. Notations

Let $U = U_n(\mathbb{F}_p)$ be the subgroup of $GL_n(\mathbb{F}_p)$ consisting of upper triangular matrices with 1 on the diagonal. Also let

$$U^* = \{A \in GL_n(\mathbb{F}_p), A = \begin{pmatrix} 1 & * & ... & * \\ 0 & 1 & ... & * \\ . & . & . & . \\ 0 & ... & 1 & * \\ 0 & ... & 0 & * \end{pmatrix}\}.$$

Define

$$\Gamma_U = \{M \in SL_n(\mathbb{Z}),\ \overline{M} \in U\},$$
$$S_U = \{M \in M_n(\mathbb{Z}), \det M > 0, (\det M, p) = 1,\ \overline{M} \in U^*\},$$
$$\Gamma(N) = \{M \in SL_n(\mathbb{Z}), M \equiv I_n \mod N\},\ \text{with } \Gamma(1) = SL_n(\mathbb{Z}),$$
$$S_K(N) = \{M \in M_n(\mathbb{Z}), \det M > 0, (\det M, K) = 1, M \equiv diag(1,1,...,1,*) \bmod N\},$$
$$GS_K(N) = \{M \in M_n(\mathbb{Z}), \det M \neq 0, (\det M, K) = 1, M \equiv diag(1,1,...,1,*) \bmod N\}.$$

3. Some functoriality properties

Recall some definitions from [Ash]:

Definition 3.1. A Hecke pair is a pair (Γ, S), where Γ is a subgroup of $GL_n(\mathbb{Z})$ containing $\Gamma(N)$ for some N, and S is a semigroup of $GL_n(\mathbb{Q})$ such that $\Gamma \subset S$.

Definition 3.2. Two Hecke pairs (Γ, S) and (Γ', S') are said to be compatible if
1) $\Gamma \subset \Gamma', S \subset S'$,
2) $\Gamma' \cap SS^{-1} = \Gamma$, and
3) $\Gamma' S = S'$.

Observe that this compatibility relation is not an equivalence relation, since it is not symetric (because of the inclusion in condition 1). Then we have:

Lemma 3.1. *a)* $(\Gamma(p), S_p(p))$ *and* (Γ_U, S_U) *are compatible Hecke pairs.*
b) (Γ_U, S_U) *and* $(\Gamma(1), S_p(1))$ *are compatible Hecke pairs.*

Proof. a) Clearly $\Gamma(p) \subset \Gamma_U$ and $S_p(p) \subset S_U$. Suppose now $\gamma \in \Gamma_U \cap S_p(p) S_p(p)^{-1}$. Then γ is congruent to $diag(1,1,...,1,*)$ mod p and has determinant 1. Thus γ is congruent to $diag(1,1,...,1,1)$ mod p, so $\gamma \in \Gamma(p)$. Since the other inclusion is trivial, we get that $\Gamma_U \cap S_p(p) S_p(p)^{-1} = \Gamma(p)$. Since any matrix from U^* can be written as a product of a matrix from U and a matrix from $diag(1,1,...,1,*)$ we get that $S_U \subset \Gamma_U S_p(p)$; hence $S_U = \Gamma_U S_p(p)$. Since the three conditions have been verified, we have that $(\Gamma(p), S_p(p))$ and (Γ_U, S_U) are compatible Hecke pairs.

b) Clearly $\Gamma_U \subset \Gamma(1)$ and $S_U \subset S_p(1)$. Suppose now that $\gamma \in \Gamma(1) \cap S_U S_U^{-1}$. Then $\gamma \in SL_n(\mathbb{Z})$ and $\overline{\gamma} \in U^*$. Thus $\overline{\gamma} \in U$ so $\gamma \in \Gamma_U$. So $\Gamma(1) \cap S_U S_U^{-1} = \Gamma_U$. The last thing that we have to prove is that $\Gamma(1) S_U = S_p(1)$. But from [Ash] p.238, Lemma 1.1 a), we have $\Gamma(1) S_p(p) = S_p(1)$ and since $S_p(p) \subset S_U$, we get that $\Gamma(1) S_U = S_p(1)$. So (Γ_U, S_U) and $(\Gamma(1), S_p(1))$ are compatible Hecke pairs. □

Also recall from [Ash] the following:

Definition 3.3. A Hecke pair (Γ, S) is called a congruence Hecke pair of level N if the following hold:
a) $(\Gamma(N), S_N(N))$ and (Γ, S) are compatible Hecke pairs,
b) (Γ, S) and $(GL_n(\mathbb{Z}), GS_N(1))$ are compatible Hecke pairs.

Corollary 3.2. *(Γ_U, S_U) is a congruence Hecke pair of level p.*

Proof. Point a) of the above definition holds because of point a) of the previous lemma.

Point b) holds because of point b) of the previous lemma, and the fact that $(\Gamma(1), S_p(1))$ and $(GL_n(\mathbb{Z}), GS_p(1))$ are compatible Hecke pairs and the relation of compatibility is transitive (see [Ash], p. 238). □

Recall that $H(S//\Gamma) = H(\Gamma\backslash S/\Gamma)$ is the Hecke algebra of double cosets $\Gamma s \Gamma$, $s \in S$. It is the free $\mathbb{Z}$-module on the double cosets $\Gamma s\Gamma$, $s \in S$ with the multiplication of

$$\Gamma s\Gamma = \coprod_{i\in I} \Gamma s_i, \text{ and } \Gamma t\Gamma = \coprod_{j\in J} \Gamma t_j, \text{ given by}$$

$$(\Gamma s\Gamma)\cdot(\Gamma t\Gamma) = \sum_{k\in K} m(\Gamma s\Gamma, \Gamma t\Gamma; \Gamma\epsilon_k\Gamma)\Gamma\epsilon_k\Gamma$$

where $\Gamma s\Gamma t\Gamma = \coprod_{k\in K}\Gamma\epsilon_k\Gamma$ and $m(\Gamma s\Gamma, \Gamma t\Gamma; \Gamma\epsilon_k\Gamma)$ is the number of elements in the set $\{(i,j), \Gamma s_i t_j = \Gamma\epsilon_k\}$. For more details, see [AS].

Lemma 3.3. *Let (Γ, S) and (Γ', S') be compatible Hecke pairs. Consider a morphism $(\Gamma', S') \xrightarrow{\phi} (\Gamma_1, S_1)$ of Hecke pairs (i.e $\phi : S' \to S_1$ is a morphism of semigroups and $\Gamma_1 = \phi(\Gamma)$). Define the Hecke pair $(\overline{\Gamma}, \overline{S}) = (\phi(\Gamma), \phi(S))$.*

If $(\overline{\Gamma}, \overline{S})$ and (Γ_1, S_1) are compatible Hecke pairs then we have the following commutative diagram of Hecke algebras:

$$\begin{array}{ccc} H(S'//\Gamma') & \hookrightarrow & H(S//\Gamma) \\ \downarrow & & \downarrow \\ H(S_1//\Gamma_1) & \hookrightarrow & H(\overline{S}//\overline{\Gamma}) \end{array}$$

Proof. We have such a diagram on the Hecke algebras, we only need to prove that it is commutative.

Since (Γ, S) and (Γ', S') are compatible Hecke pairs, by property 3) of the definition of compatible Hecke pairs we get that any simple coset $\Gamma' a$, $a \in S'$ is equal to $\Gamma' s$ for some $s \in S$. We thus have the following commutative diagram of single cosets:

$$\begin{array}{ccc} \Gamma' s & \to & \Gamma s \\ \downarrow & & \downarrow \\ \Gamma_1\phi(s) & \to & \overline{\Gamma}\phi(s) \end{array}$$

Since each of these maps on cosets gives rise to a map on double cosets by joining together the simple cosets that make up the double coset, we obtain a commutative diagram on the double cosets, and on the corresponding Hecke algebras. □

Corollary 3.4. *Let $H(p) = H(S_p(1)//\Gamma(1))$. We have the following commutative diagram of Hecke algebras:*

$$\begin{array}{ccc} H(p) & \hookrightarrow & H(S_U//\Gamma_U) \\ \downarrow & & \downarrow \\ H(GL_n(\mathbb{F}_p)//SL_n(\mathbb{F}_p)) & \hookrightarrow & H(U^*//U). \end{array}$$

Proof. We only need to prove that (U, U^*) and $(SL_n(\mathbb{F}_p), GL_n(\mathbb{F}_p))$ are compatible Hecke pairs. Then by applying the previous lemma, we get the result.

It is clear that $U^* \subset GL_n(\mathbb{F}_p)$ and $U \subset SL_n(\mathbb{F}_p)$. We also have $U^* SL_n(\mathbb{F}_p) = GL_n(\mathbb{F}_p)$, since by taking a matrix A of $GL_n(\mathbb{F}_p)$ and multiplying it with the inverse of $diag(1, 1, ..., 1, \det A)$ we obtain a matrix of $SL_n(\mathbb{F}_p)$.

We need now to check that $SL_n(\mathbb{F}_p) \cap U^* U^{*-1} = U$. Since U^* is a group it implies that $U^* U^{*-1} = U^*$ so we have to prove that $SL_n(\mathbb{F}_p) \cap U^* = U$ which is obvious. □

4. The Main Result

Definition 4.1. As in [Ash], given a Hecke pair (Γ, S) and a left S-module M, we define an action of the Hecke algebra $H(S//\Gamma)$ on $H^*(\Gamma, M)$. We first define the action of $\Gamma s \Gamma$ for $s \in S$ as the Hecke operator T_s defined below:

$$T_s(\beta) = tr_{\Gamma \cap s\Gamma s^{-1} \to \Gamma} res_{\Gamma \cap s\Gamma s^{-1}} s^*(\beta) \text{ for any } \beta \in H^*(\Gamma, M).$$

We extend this action to the entire Hecke algebra $H(S//\Gamma)$ by linearity.

We also define $T_{l,k}$, $l \neq p$, to be the Hecke operator corresponding to the double coset $\Gamma diag(1, ..., 1, l, ..., l)\Gamma \in H(p)$, where l appears k times and $\Gamma = \Gamma(1)$, $S = S_p(1)$.

This action is compatible with the algebra structure because:

Proposition 4.1. *Let (Γ, S) be a Hecke pair and M be a left S-module. Then $H^*(\Gamma)$ has a structure of a right $H(S//\Gamma)$-module via the Hecke operator action described above. More precisely for any $a, b \in H(S//\Gamma)$ and any $\beta \in H^*(\Gamma, M)$:*

$$T_{ab}(\beta) = T_b(T_a(\beta)).$$

Proof. See [RW]. □

Corollary 4.2. *Under the commutative diagram from 3.4, the image of $T_{l,k} \in H(p)$ in $H(U^*//U)$ is*

$$d_{l,k} T_{U diag(1,1,...,1,l^k)U} \text{ where } d_{l,k} = \deg(T_{l,k}) = \frac{(l^n - 1)...(l^n - l^{k-1})}{(l^k - 1)...(l^k - l^{k-1})}.$$

Note 4.1. The last equality has been proved in [Shi], prop. 3.18, p. 58.

Proof. The image of $T_{l,k}$ in $H(GL_n(\mathbb{F}_p)//SL_n(\mathbb{F}_p))$ is of the form $d\overline{T_{l,k}}$ where d is such that the degree is preserved. In $H(GL_n(\mathbb{F}_p)//SL_n(\mathbb{F}_p))$, $\overline{T_{l,k}}$ is in the same double coset as $diag(1, 1, ..., 1, l^k) \in U^*$. Furthermore, this double coset splits as only one single coset since $diag(1, 1, ..., 1, l^k)$ normalizes U. So $\deg \overline{T_{l,k}} = 1$. Since all maps from the above commutative diagram maintain the degree, we get that $d = d_{l,k}$. The image of $\overline{T_{l,k}}$ in $H(U^*//U)$ is $diag(1, 1, ..., 1, l^k)$, since $\overline{T_{l,k}}$ can be represented by only one single coset. Therefore the image of $T_{l,k}$ in $H(U^*//U)$ is $d_{l,k} T_{U diag(1,1,...,1,l^k)U}$. □

Definition 4.2. Let $\beta \in H^*(U, \mathbb{F}_p)$ be an eigenclass for $T_{l,k}$ for all primes l, and all $1 \le k \le n$. Thus $T_{l,k}\beta = a(l,k)\beta$ for some $a(l,k) \in F_p$. Define

$$P(\beta, l) = \sum (-1)^k l^{k(k-1)/2} a(l,k) X^k.$$

Theorem 4.3. *Let $\beta \in H^*(U, \mathbb{F}_p)$ be an eigenclass for $T_{l,k}$ for all primes $l \neq p$, and all $1 \le k \le n$. Then there is an integer d such that the representation*

$$\rho = \omega^d \oplus \omega^{d+1} \oplus ... \oplus \omega^{d+n-1} : G_{\mathbb{Q}} \to GL_n(\mathbb{F}_p), \tag{2}$$

where $G_{\mathbb{Q}} = Gal(\overline{\mathbb{Q}}/\mathbb{Q})$, has the property that

$$P(\beta, l) = det(I - \rho(Frob_l)X) \text{ for all } l \neq p.$$

Proof. Let $T_m = T_{diag(1,1,...,1,m)}$ for any $m \in \mathbb{F}_p^*$. Then $T_{l,k} = d_{l,k} T_{l^k}$. There is a prime q that generates $\mathbb{F}_p^\times$. Since β is an eigenclass then $T_{q,1}\beta = a\beta$ for some $a \in \mathbb{F}_p^*$. The eigenvalue a is nonzero, since $a^{p-1}\beta = T_{q^{p-1}}\beta = T_1\beta = \beta$, so $a^{p-1} = 1$. But then $a \equiv q^d \pmod p$, for some $d \in \mathbb{Z}$. Then $T_{q,k}\beta = d_{l,k}(T_{q^k})\beta = d_{q,k}(T_q)^k\beta = d_{q,k} q^{dk}\beta$. For any prime l and any k we have $T_{l,k} = d_{l,k} T_{diag(1,1,...,1,l^k)} = d_{l,k} T_{q^m}$ for some m such that $l^k \equiv q^m \pmod p$. Then $T_{l,k}\beta = d_{l,k} q^{md}\beta = d_{l,k} l^{dk}\beta$. Therefore $a(l,k) = d_{l,k} l^{dk}$ for all primes l. Then

$$\begin{aligned} P(\beta, l) &= \sum (-1)^k l^{k(k-1)/2} a(l,k) X^k = \sum (-1)^k l^{k(k-1)/2} d_{l,k} l^{kd} X^k \\ &= \sum (-1)^k l^{k(k-1)/2} d_{l,k} (l^d X)^k = \text{ (see [Shi] p.64)} \\ &= (1 - l^d X)(1 - l^{d+1} X)...(1 - l^{d+n-1} X) = \det(I - \rho(Frob_l)X) \end{aligned}$$

for the ρ given in (2). □

Now we prove that the Conjecture of Ash holds in our particular context:

Corollary 4.4. *The conjecture of Ash (Conjecture 1.1) is true for $\Gamma = \Gamma_U, S = S_U$ and for eigenclasses $\beta \in H^*(\Gamma_U, \mathbb{F}_p)$, which come from $H^*(U, \mathbb{F}_p)$ via the reduction mod p map, $\pi^* : H^*(U, \mathbb{F}_p) \to H^*(\Gamma_U, \mathbb{F}_p)$.*

Proof. In our context, $(\Gamma, S) = (\Gamma_U, S_U)$, $\mathbb{F} = \mathbb{F}_p$, $V = \mathbb{F}_p$ with the trivial S-action, and $N = p$.

Since β comes from $H^*(U, \mathbb{F}_p)$, $\beta = \pi^*(\beta')$ with $\beta' \in H^*(U, \mathbb{F}_p)$. Because the map π^* is compatible with the Hecke action (see [KPS] thm. 1.3.7), β is a $T_{l,k}$-eigenclass for all primes $l \neq p$ and $k \le n$ if and only if β' is a $T_{l,k}$-eigenclass for all primes $l \neq p$ and $k \le n$ and the eigenvalues are the same. Thus $P(\beta, l) = P(\beta', l)$.

Now we apply the previous theorem for β' and we get the result. □

Remark 4.2. It would be interesting to know what classes of $H^*(\Gamma_U, \mathbb{F}_p)$ actually come from $H^*(U, \mathbb{F}_p)$.

References

[Ash] A. Ash. Galois representations attached to mod p cohomology of $GL(n, \mathbb{Z})$. *Duke Math. Journal* **65** (1992) pp. 235-255

[AM] A. Adem, J. Milgram. Cohomology of Finite Groups. Springer-Verlag, Berlin, 1994

[AS] A. Ash, G. Stevens. Cohomology of arithmetic groups and congruences between systems of Hecke eigenvalues. *J. Reine Angew. Math.* **365** (1986), pp. 192–220

[Brn] K. Brown. Cohomology of Groups. Springer-Verlag, New York, 1982

[Ev] L. Evens. The Cohomology of Groups. Oxford University Press, New York, 1991

[Ho] R. Howe. Harish-Chandra homomorphisms for p-adic groups. *Regional Conference Series in Mathematics* **59**, American Mathematical Society, Providence, 1985

[KPS] M. Kuga, W. Parry, C. H. Sah. Group cohomology and Hecke operators. Manifolds and Lie groups. *Progr. Math.* **14**, Birkhuser, Boston, Mass., 1981. pp. 223-266

[RW] Y.H. Rhie, G. Whaples. Hecke operators in cohomology of groups. *J. Math. Soc Japan.* **22** (1970) pp. 431-442

[Shi] G. Shimura, Introduction to the arithmetic theory of automorphic functions, Princeton University Press, Princeton, NJ, 1994