Galois Representations Attached to Weight 1 Modular Forms

Sean Gonzales

December 4, 2024

1 Introduction

This paper largely serves as a translation of *Formes modulaires de poids 1* by Deligne and Serre [DS74], in which they prove the following result:

Theorem 1.1. *Let $N \geq 1$ be an integer, ε a Dirichlet character mod N such that $\varepsilon(-1) = -1$, and f a nonzero modular form of weight 1, level $\Gamma_0(N)$, and character ε. Suppose that f is an eigenform for T_p, $p \nmid N$, with eigenvalues a_p. Then there exists a representation*

$$\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{C})$$

that is unramified away from N and such that for all $p \nmid N$,

$$\mathrm{Tr}(\rho(\mathrm{Frob}_p)) = a_p \qquad \text{and} \qquad \det(\rho(\mathrm{Frob}_p)) = \varepsilon(p)$$

Furthermore, this representation is irreducible if f is a cusp form.

Note that, as compared to Theorem 3.1 below, the representation ρ attached to a weight 1 modular form f is *complex* rather than λ-adic. One way to explain this is via *L-functions*. Let f be a cusp form of weight k, level $\Gamma_0(N)$, and character ε, and let $\sum_{n\geq 1} a_n q^n$ be its q-expansion. Recall that the L-function of f is given by

$$L(f, s) = \sum_{n=1}^{\infty} a_n n^{-s}$$

Its completed L-function is given by

$$\Lambda(f, s) = \left(\frac{\sqrt{N}}{2\pi}\right)^s \Gamma(s) L(f, s)$$

Now, define the modular form g by $g(z) = (\sqrt{N}z)^{-k} f(-1/Nz)$; it is a cusp form of weight k, level $\Gamma_0(N)$, and character $\overline{\varepsilon}$. Writing $\sum_{n\geq 0} b_n q^n$ for the q-expansion of g, its L-function and completed L-function are defined as above. We have the following fundamental theorem due to Hecke (see, for example, Theorem 4.3.5 in [Miy06]):

Theorem 1.2. *With notation as above, we have that $\Lambda(f,s)$ is entire, bounded in vertical strips, and the following functional equation is satisfied:*

$$\Lambda(f,s) = i^k \Lambda(g, k-s)$$

It turns out that these conditions are (nearly) sufficient to give a sort of converse. The following theorem is due to Weil (see Theorem 4.3.15 in [Miy06]):

Theorem 1.3. *Let $f(z) = \sum_{n\geq 1} a_n q^n$ and $g(z) = \sum_{n\geq 1} b_n q^n$ be two series such that $a_n, b_n = O(n^\alpha)$ for some $\alpha > 0$. Fix integers N, k and a Dirichlet character $\varepsilon : (\mathbb{Z}/N\mathbb{Z})^* \to \mathbb{C}^*$ such that $\varepsilon(-1) = (-1)^k$. Then f is a cusp form of weight k, level $\Gamma_0(N)$, and character ε, and g is given by $g(z) = (\sqrt{N}z)^{-k} f(-1/Nz)$, as long as the following conditions are satisfied:*

(i) $\Lambda(f,s)$, $\Lambda(g,s)$ are entire, bounded in vertical strips, and satisfy the functional equation

$$\Lambda(f,s) = i^k \Lambda(g, k-s)$$

(ii) The L-functions of twists of f, g by Dirichlet characters are entire, bounded in vertical strips, and satisfy a certain functional equation.

In the case that f is a noramlized newform for the Hecke operators T_p, $p \nmid N$, the L-function of f splits into *Euler factors* (Theorem 4.5.16 in [Miy06]):

$$L(f,s) = \prod_p (1 - a_p p^{-s} + \varepsilon(p) p^{k-1} p^{-2s})^{-1}$$

Note that $\varepsilon(p) = 0$ if $p \mid N$.

The appearance of L-functions in other branches of math is a primary motivator in the association of modular (or, more generally, *automorphic*) forms to seemingly unrelated objects. For example, an *elliptic curve* $E/\mathbb{Q}$ has an associated L-function given by

$$L(E,s) = \prod_{p \nmid N_E} (1 - a_p p^{-s} + p \cdot p^{-2s})^{-1} \prod_{p \mid N_E, p^2 \nmid N_E} (1 \pm p^{-s})^{-1}$$

where N_E is the conductor of E and $a_p = p + 1 - |E(\mathbb{F}_p)|$. Thus, if $L(E,s)$ is given by the L-function of a modular form, it better be a weight 2 newform; this is precisely the Modularity Theorem.

In the case of weight 1 cusp forms, we find a connection to *Artin L-functions* (see section VII.10 of [Neu99] for more detail). Let $\rho : G_K \to \mathrm{GL}(V)$ be a complex representation of the absolute Galois group of a number field K. For a prime $\mathfrak{p}$ of K, we define the local L-factor of ρ as

$$L_{\mathfrak{p}}(\rho, s) = \det\left(1 - N(\mathfrak{p})^{-s} \rho|_{V^{I_{\mathfrak{p}}}}(\mathrm{Frob}_{\mathfrak{p}})\right)^{-1}$$

where $N(\mathfrak{p}) = |\mathcal{O}_K/\mathfrak{p}|$ is the absolute norm, $V^{I_{\mathfrak{p}}}$ is the subspace of V fixed by the inertia subgroup $I_{\mathfrak{p}}$ at $\mathfrak{p}$, and $\mathrm{Frob}_{\mathfrak{p}}$ is a choice of Frobenius element at $\mathfrak{p}$. The Artin L-function of ρ is

$$L(\rho, s) = \prod_{\mathfrak{p}} L_{\mathfrak{p}}(\rho, s)$$

We obtain a completed Artin L-function by multiplying by the "infinite local factors"

$$\Lambda(\rho, s) = A(\rho)^{s/2} L_\infty(\rho, s) L(\rho, s)$$

The completed L-function satisfies the following functional equation:

$$\Lambda(\rho, s) = W(\rho)\Lambda(\rho^*, 1 - s)$$

where ρ^* is the dual representation and $W(\rho)$ is a complex constant of modulus 1, called the *Artin root number*.

Since modular forms correspond to 2-dimensional Galois representations, we are particularly interested in 2-dimensional Artin representations $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{C})$, specifically in the case when ρ is *odd*, i.e. $\det(\rho(c)) = -1$ for any complex conjugation $c \in G_{\mathbb{Q}}$. If $L(\rho, s) = L(f, s)$ for some modular form f, the functional equation for ρ combined with Weil's converse theorem strongly suggests that f should be a weight 1 cusp form. This was the primary motivation for Deligne and Serre in proving Theorem 1.1. We will not focus too much on this point throughout the paper, but it should serve as an overarching motivator for the main result.

2 Classical Results on Galois Representations

Definition 2.1. Let L/K be a finite extension of number fields unramified at the prime $\mathfrak{p}$. The conjugacy class of the Frobenius element of $\mathrm{Gal}(L/K)$ is denoted by $\mathrm{Frob}_{\mathfrak{p}}$.

If L/K is an infinite extension unramified at $\mathfrak{p}$, we obtain a well-defined conjugacy class $\mathrm{Frob}_{\mathfrak{p}}$, essentially given by the limit of the conjugacy classes of each finite subextension.

Proposition 2.2. *(Chebotarev Density Theorem) Let L/K be a finite Galois extension with Galois group $G = \mathrm{Gal}(L/K)$, and let S be the set of unramified primes of K. Let C be a conjugacy class in G. Then the set of primes $\mathfrak{p} \in S$ such that $\mathrm{Frob}_{\mathfrak{p}} = C$ has density $\frac{|C|}{|G|}$.*

Among the important applications of Chebotarev density is the following proposition.

Proposition 2.3. *Let K be a number field, S a finite set of primes of K, and K^S the maximal extension of K unramified outside of S. The set $\{\mathrm{Frob}_{\mathfrak{p}}\}_{\mathfrak{p} \notin S}$ is dense in $G_{K,S} = \mathrm{Gal}(K^S/K)$ for the Krull topology.*

Proof. By definition of the Krull topology, it suffices to show that for every finite subextension $K \subset L \subset K^S$, every element of $G = \mathrm{Gal}(L/K)$ is a Frobenius element. In fact, we get an even stronger statement: every element of G is a Frobenius element for infinitely many primes $\mathfrak{p}$. To see why, let $\sigma \in G$ and denote by $C(\sigma)$ its conjugacy class. Chebotarev density says that the set of $\mathfrak{p} \notin S$ such that $C(\sigma) = \mathrm{Frob}_{\mathfrak{p}}$ has positive density; in particular, $C(\sigma) = \mathrm{Frob}_{\mathfrak{p}}$ for infinitely many primes $\mathfrak{p}$. □

Another useful result is the following, due to Brauer and Nesbitt. For an element $g \in \mathrm{GL}_n(F)$, write $P(g)$ for the characteristic polynomial of g, and $\mathrm{Tr}(g)$ for the trace of g.

Proposition 2.4. *(Brauer-Nesbitt Theorem) Let G be a group and F a field. If $\rho_i : G \to \mathrm{GL}_n(F)$, $i = 1, 2$ are two finite dimensional semisimple representations such that $P(\rho_1(g)) = P(\rho_2(g))$ (or simply $\mathrm{Tr}\rho_1(g) = \mathrm{Tr}\rho_2(g)$ if $\mathrm{char}F = 0$) for all $g \in G$, then ρ_1 and ρ_2 are isomorphic.*

The objects of importance in this survey paper are Galois representations, which are linear representations $\rho : G_K \to \mathrm{GL}_n(F)$ where K is a number field, $G_K = \mathrm{Gal}(\bar{K}/K)$ is the absolute Galois group of K, and F is a field. We are mainly interested in the case when ρ factors through $G_{K,S} = \mathrm{Gal}(K^S/K)$ for some finite set S of primes in K. Such a Galois representation is called *unramified almost everywhere.*

In more detail, a Galois representation ρ is unramified at a prime $\mathfrak{p}$ if the image of the inertia subgroup $I_\mathfrak{p} \subset G_K$ is trivial. If ρ is unramified at each prime $\mathfrak{p}$ outside of a finite set of primes S, then the image of the group $I^S = \langle I_\mathfrak{p} \rangle_{\mathfrak{p} \notin S}$ generated by inertia groups is trivial, and hence ρ factors through $G_K/I^S \cong G_{K,S}$.

Combining the Brauer-Nesbitt theorem with Chebotarev density yields the following fundamental result, which states that an ℓ-adic Galois representation is determined by its traces of Frobenius.

Proposition 2.5. *Let K be a number field and $\rho_i : G_K \to \mathrm{GL}_n(F)$, $i = 1, 2$ be two semisimple Galois representations which are unramified almost everywhere. Then $\rho_1 \cong \rho_2$ if and only if $P(\rho_1(\mathrm{Frob}_\mathfrak{p})) = P(\rho_2(\mathrm{Frob}_\mathfrak{p}))$ (or simply $\mathrm{Tr}\rho_1(\mathrm{Frob}_\mathfrak{p}) = \mathrm{Tr}\rho_2(\mathrm{Frob}_\mathfrak{p})$ if $\mathrm{char}F = 0$) for all primes $\mathfrak{p}$ at which ρ_1 and ρ_2 are both unramified.*

Note that, while $\mathrm{Frob}_\mathfrak{p}$ is not a specific element but a conjugacy class, the characteristic polynomial and trace are invariant under conjugation.

Proof. One direction of the proof is obvious, so we focus on the other direction. Let S be the finite set of primes at which either ρ_1 or ρ_2 ramify. Then ρ_1, ρ_2 factor through $G_{K,S}$. Assume that $P(\rho_1(\mathrm{Frob}_\mathfrak{p})) = P(\rho_2(\mathrm{Frob}_\mathfrak{p}))$ for all primes $\mathfrak{p} \notin S$ (similarly using Tr if $\mathrm{char}F = 0$). Consider the function $f : G_{K,S} \to F$ given by $f(g) = P(\rho_1(g)) - P(\rho_2(g))$ (again using Tr if $\mathrm{char}F = 0$). This is continuous since ρ_1, ρ_2, and P (or Tr) are continuous functions. Since $f(\mathrm{Frob}_\mathfrak{p}) = 0$ for all $\mathfrak{p} \notin S$, and $\{\mathrm{Frob}_\mathfrak{p}\}_{\mathfrak{p} \notin S}$ is dense in $G_{K,S}$ by Proposition 2.3, f is identically 0. Thus, by Proposition 2.4, $\rho_1 \cong \rho_2$. □

3 Galois Representations Attached to Modular Forms of Weight ≥ 2

We recall the case when f is a modular form of weight ≥ 2. The main result is the following.

Theorem 3.1. *Let f be a modular form of weight $k \geq 2$, level $\Gamma_0(N)$, and character ε. Suppose that f is an eigenfunction for the Hecke operators T_p, $p \nmid N$, with eigenvalues a_p. Let K be a finite extension of $\mathbb{Q}$ containing the a_p and $\varepsilon(p)$, let λ be a finite place of K of residue characteristic ℓ. Then there exists a semisimple representation*

$$\rho_\lambda : G_\mathbb{Q} \to \mathrm{GL}_2(K_\lambda)$$

that is unramified away from $N\ell$ and such that for all $p \nmid N\ell$, we have

$$\mathrm{Tr}(\rho_\lambda(\mathrm{Frob}_p)) = a_p \qquad \textit{and} \qquad \det(\rho_\lambda(\mathrm{Frob}_p)) = \varepsilon(p)p^{k-1}$$

We briefly summarize the cases:

1. f **is an Eisenstein series**: (due to Hecke; see [Hec83]). This is arguably the simplest case. If f is an Eisenstein series, it is associated to a unique pair of Dirichlet characters χ_1, χ_2 of $(\mathbb{Z}/N\mathbb{Z})^\times$ such that $\chi_1\chi_2 = \varepsilon$ and $\chi_1(p) + \chi_2(p) = a_p$ for all $p \nmid N$. Thus, the corresponding Galois representation is $\chi_1 \oplus \chi_2$.

2. f **is a weight 2 cusp form**: (due to Eichler and Shimura; see chapter 9 of [DS05] for a friendly overview). In this case, we can directly relate f to a geometric object in order to construct the Galois representation. First, let $J_1(N) = \Omega^\vee_{X_1(N)}/H_1(X_1(N), \mathbb{Z})$ be the Jacobian variety of the modular curve $X_1(N)$. Recall that $\Omega_{X_1(N)} \cong S_2(\Gamma_1(N))$, so in fact $J_1(N) = S_2(\Gamma_1(N))^\vee/H_1(X_1(N), \mathbb{Z})$. Let $V_\ell(X_1(N)) = T_\ell(J_1(N)) \otimes \mathbb{Q} \cong \mathbb{Q}_\ell^{2g}$ denote the rational ℓ-adic Tate module of $J_1(N)$, where g is the genus of $X_1(N)$. The Hecke algebra $\mathcal{H} = \mathbb{Z}[\{T_n, \langle n\rangle\}]$ and $G_\mathbb{Q}$ both act on $J_1(N)$ and these actions commute with each other, hence the same is true for $V_\ell(X_1(N))$. Thus, the representation $\rho_{X_1(N),\ell} : G_\mathbb{Q} \to \mathrm{GL}_{2g}(\mathbb{Q}_\ell)$ obtained from the Galois action is unramified away from $N\ell$ and by Eichler-Shimura it has the property that $\rho_{X_1(N),\ell}(\mathrm{Frob}_p)$ satisfies the polynomial $x^2 - T_p x + \langle p\rangle p$ for $p \nmid N\ell$.

   Next, we relate this representation to f. Let $I_f = \{T \in \mathcal{H} : Tf = 0\}$ be the kernel of the eigenvalue map, and define the d-dimensional abelian variety $A_f = J_1(N)/I_f J_1(N)$. The quotient of the Hecke algebra $\mathcal{H}/I_f$ is isomorphic to the ring of integers $\mathcal{O}_K$ of the field K (as defined in the theorem statement), and the actions of $T_p, \langle p\rangle$ on A_f under this isomorphism are given by $a_p, \varepsilon(p)$, respectively. Transfering the Galois action to A_f and taking the ℓ-adic Tate module $V_\ell(A_f) = T_\ell(A_f) \otimes \mathbb{Q} \cong \mathbb{Q}_\ell^{2d}$ gives a Galois representation $\rho_{A_f,\ell} : G_\mathbb{Q} \to \mathrm{GL}_{2d}(\mathbb{Q}_\ell)$ which is unramified away from $N\ell$ and has the property that $\rho_{A_f,\ell}(\mathrm{Frob}_p)$ satisfies the polynomial $x^2 - a_p x + \varepsilon(p)p$ for $p \nmid N\ell$.

   Lastly, one can show that $V_\ell(A_f)$ is a 2-dimensional $K \otimes \mathbb{Q}_\ell$-vector space, hence we obtained a representation $\rho_{f,\ell} : G_\mathbb{Q} \to \mathrm{GL}_2(K \otimes \mathbb{Q}_\ell)$. Decomposing $K \otimes \mathbb{Q}_\ell \cong \prod_{\lambda|\ell} K_\lambda$ produces a family of 2-dimensional irreducible Galois representations $\rho_\lambda : G_\mathbb{Q} \to \mathrm{GL}_2(K_\lambda)$ which satisfy the conditions of the theorem.

3. f **is a weight** ≥ 2 **cusp form**: (Due to Deligne; see [Del71]). This case generalizes the weight 2 case. Here, we cannot directly relate f to an abelian variety like we did in the weight 2 case. Instead, we resort to étale cohomology. We assume $k \geq 2$ and $N \geq 5$. Let $\pi : \mathcal{E}_{Y_1(N)} \to Y_1(N)$ be the universal elliptic curve and $\iota : Y_1(N) \hookrightarrow X_1(N)$ be the open immersion. Deligne produced a canonical isomorphism of $\mathcal{H}_{\mathbb{R}}$-modules

$$H^1(X_1(N)_{\mathbb{C}}, \iota_* \mathrm{Sym}^{k-2} R^1\pi_* \mathbb{Q}) \otimes \mathbb{R} \xrightarrow{\sim} S_k(\Gamma_1(N))_{\mathbb{C}}$$

Note that in the $k = 2$ case, this isomorphism is precisely the isomorphism $\Omega_{X_1(N)} \cong S_2(\Gamma_1(N))$. From this, we obtain that $H^1(X_1(N)_{\overline{\mathbb{Q}}}, \iota_* \mathrm{Sym}^{k-2} R^1\pi_* \mathbb{Q}_\ell)$ is a free $\mathcal{H}_{\mathbb{Q}_\ell}$-module of rank 2, and hence for any $\lambda | \ell$ in K, we obtain a 2-dimensional K_λ-vector space

$$V_{f,\lambda} = H^1(X_1(N)_{\overline{\mathbb{Q}}}, \iota_* \mathrm{Sym}^{k-2} R^1\pi_* \mathbb{Q}_\ell) \otimes_{\mathcal{H}_{\mathbb{Q}_\ell}} K_\lambda$$

which satisfies the conditions of the theorem.

By combining Theorem 3.1 with Proposition 2.5, we obtain the following corollary:

Corollary 3.2. *Let $(f, N, k, \varepsilon, (a_p))$ and $(f', N', k', \varepsilon', (a'_p))$ be as in Theorem 3.1. If the set of primes p such that $a_p = a'_p$ is density 1, then $k = k'$, $\varepsilon = \varepsilon'$, and $a_p = a'_p$ for all $p \nmid NN'$.*

In fact, for a choice of K and λ, the representations attached to f and f' are isomorphic.

4 Reduction mod ℓ

This section covers section 6 of [DS74]. Let K be a number field, λ a finite place of K, $\mathcal{O}_\lambda$ its ring of valuations, $\mathfrak{m}_\lambda$ its maximal ideal, $k_\lambda = \mathcal{O}_\lambda / \mathfrak{m}_\lambda$ the residue field, and ℓ the characteristic of k_λ.

Let f be a modular form of weight k, level $\Gamma_0(N)$, and character ε. We call f *λ-integral* if the coefficients of its q-expansion lie in $\mathcal{O}_\lambda$. If moreover the coefficients lie in $\mathfrak{m}_\lambda$, then we simply write $f \equiv 0 \pmod{\lambda}$. If f is λ-integral, we say that f is an *eigenform of* $T_p \pmod{\lambda}$ *with eigenvalue* $a_p \in k_\lambda$ if we have

$$T_p f - a_p f \equiv 0 \pmod{\lambda}$$

Proposition 4.1. *With the preceding notation, let f be a modular form of weight k, level $\Gamma_0(N)$, and character ε, with coefficients in K. Suppose that f is λ-integral, $f \not\equiv 0 \pmod{\lambda}$, and that f is an eigenform for $T_p \pmod{\lambda}$ with eigenvalue $a_p \in k_\lambda$ for $p \nmid N\ell$. Let k_f be the subfield of k_λ generated by the a_p and the reductions $\pmod{\lambda}$ of the $\varepsilon(p)$. Then there exists a semisimple representation*

$$\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(k_f)$$

that is unramified away from $N\ell$ and such that, for all $p \nmid N\ell$, we have

$$\mathrm{Tr}(\rho(\mathrm{Frob}_p)) = a_p \qquad \text{and} \qquad \det(\rho(\mathrm{Frob}_p)) \equiv \varepsilon(p) p^{k-1} \pmod{\lambda}$$

Remark 4.2. Let $(K', \lambda', f', k', \varepsilon', (a'_p))$ be as in the proposition statement, where $K \subset K'$ and $\lambda' \mid \lambda$. If $a_p \equiv a'_p \pmod{\lambda'}$ and $\varepsilon(p)p^{k-1} \equiv \varepsilon'(p)p^{k'-1} \pmod{\lambda'}$ for all $p \nmid N\ell$, the proposition is true for f if and only if it is true for f'. The determinant condition can be verified as soon as $\varepsilon = \varepsilon'$ and $k \equiv k' \pmod{(\ell-1)}$ and the trace condition follows from this provided that $f \equiv f' \pmod{\lambda'}$.

We will reduce the proof to a simpler situation in two steps:

1. **Reduction to the case** $k \geq 2$: For $n > 2$ even, let E_n denote the normalized (i.e. constant coefficient is 1) weight n Eisenstein series for $\mathrm{SL}_2(\mathbb{Z})$. If n is chosen so that $\ell - 1 \mid n$, then E_n is ℓ-integral and $E_n \equiv 1 \pmod{\ell}$. Then the product $fE_n \equiv f \pmod{\lambda}$, and the weight $k + n \equiv k \pmod{\ell-1}$. Thus, by Remark 4.2, we can reduce to the case where $k \geq 2$.

2. **Reduction to the case where** f **is an eigenform for** T_p: It suffices to prove the proposition for a modular form f', as in Remark 4.2, with $k = k'$, $\varepsilon = \varepsilon'$, and such that f' is an eigenform for T_p (not just an eigenform mod λ'). Such an f' exists by the following lemma, applied to T_p acting on the $\mathcal{O}_\lambda$-module M of modular forms of weight k, level $\Gamma_0(N)$, and character ε, with coefficients in $\mathcal{O}_\lambda$:

Lemma 4.3. *Let M be a free module of finite type over a discrete valuation ring $\mathcal{O}$. Let $\mathfrak{m}$ be the maximal ideal, k the residue field, and K the field of fractions. Let $\mathcal{T}$ be a set of endomorphisms of M that commute with each other. Let $f \in M/\mathfrak{m}M$ be a common eigenvector of the $T \in \mathcal{T}$, and let $a_T \in k$ be the corresponding eigenvalues. Then there exists a discrete valuation ring $\mathcal{O}'$ containing $\mathcal{O}$, with maximal ideal $\mathfrak{m}'$ such that $\mathfrak{m}' \cap \mathcal{O} = \mathfrak{m}$, and field of fractions K' finite over K, and a nonzero element $f' \in M' = M \otimes_{\mathcal{O}} \mathcal{O}'$ which is a common eigenvector for the $T \in \mathcal{T}$ with eigenvalues a'_T satisfying $a'_T \equiv a_T \pmod{\mathfrak{m}'}$.*

Note that the lemma does not provide a lift of the eigenvector: it only lifts the eigenvalues.

Proof. Let $\mathcal{H}$ be the subalgebra of $\mathrm{End}(M)$ generated by $\mathcal{T}$. By taking a finite extension of scalars, we may assume that $\mathcal{H} \otimes K$ is a product of Artinian rings with residue field K. Let $\chi : \mathcal{H} \to k$ be the homomorphism given by $hf = \chi(h)f$ for all $h \in \mathcal{H}$. Since $\mathcal{H}$ is free over $\mathcal{O}$, there exists a prime ideal $\mathfrak{p}$ of $\mathcal{H}$ contained in the maximal ideal $\ker(\chi)$ and such that $\mathfrak{p} \cap \mathcal{O} = 0$; it is the kernel of a homomorphism $\chi' : \mathcal{H} \to \mathcal{O}$ whose reduction mod $\mathfrak{m}$ is χ. The ideal of $\mathcal{H} \otimes K$ generated by $\mathfrak{p}$ belongs to the support of the module $M \otimes K$; we then conclude that there exists a nonzero element f'' of $M \otimes K$ that is annihilated by this ideal, i.e. such that $hf'' = \chi'(h)f''$ for all $h \in \mathcal{H}$. We then take for f' a nonzero multiple of f'' belonging to M. □

Proof of Proposition 4.1. By the above reductions, we may assume that $k \geq 2$ and that f is an eigenform for T_p, $p \nmid N\ell$. Since T_ℓ commutes with T_p, we may also assume that f is an eigenform for T_ℓ if $\ell \nmid N$. Let

$$\rho_\lambda : G_{\mathbb{Q}} \to \mathrm{GL}_2(K_\lambda)$$

be the representation associated to f given by Theorem 3.1. By replacing ρ_λ with an isomorphic representation, we may assume that $\rho_\lambda(G_\mathbb{Q})$ is contained in $\mathrm{GL}_2(\hat{\mathcal{O}}_\lambda)$, where $\hat{\mathcal{O}}_\lambda$ is the ring of integers of K_λ (i.e. the completion of $\mathcal{O}_\lambda$). By reducing the representation ρ_λ mod λ, we obtain a representation

$$\tilde{\rho}_\lambda : G_\mathbb{Q} \to \mathrm{GL}_2(k_\lambda)$$

Let $\tilde{\rho}_\lambda^{\mathrm{ss}}$ denote the semisimplification of $\tilde{\rho}_\lambda$. This is a semisimple representation, unramified away from $N\ell$, and which satisfies the trace and determinant conditions of the proposition statement. The group $\tilde{\rho}_\lambda^{\mathrm{ss}}(G_\mathbb{Q})$ is finite, hence by Proposition 2.3, every element of $\tilde{\rho}_\lambda^{\mathrm{ss}}(G_\mathbb{Q})$ is of the form $\tilde{\rho}_\lambda^{\mathrm{ss}}(\mathrm{Frob}_p)$ for some $p \nmid N\ell$. By definition of the field k_f, we thus see that for every $\alpha \in \tilde{\rho}_\lambda^{\mathrm{ss}}(G_\mathbb{Q})$, the characteristic polynomial of α has its coefficients in k_f. The existence of the representation ρ then follows from the following lemma. □

Lemma 4.4. *Let $\varphi : G \to \mathrm{GL}_n(k')$ be a semisimple representation of a group G over a finite field k'. Let k be a subfield of k' containing the coefficients of the characteristic polynomials of $\varphi(g)$ for all $g \in G$. Then φ is realizable over k, i.e. it is isomorphic to a representation $\rho : G \to \mathrm{GL}_n(k)$.*

Proof. In order for φ to be realizable over k, it suffices to show that φ is isomorphic to $\sigma(\varphi)$ for any k-automorphism σ of k'. This is because the Brauer group of a finite field is trivial, hence the Schur index must be 1. Since φ and $\sigma(\varphi)$ have the same characteristic polynomials, and are both semisimple, they must be isomorphic. □

5 Analytic Results on Mod ℓ Galois Representations

This section covers most of section 4, section 7, and the beginning of section 8 of [DS74]. We prove a few analytic properties of modular forms and Galois representations. The end product is that we establish an upper bound on the cardinality of the image of the mod ℓ Galois representations constructed in Section 4.

To begin, we have the following proposition, which we state without proof.

Proposition 5.1. *Let f be a nonzero cusp form of weight k, level $\Gamma_0(N)$, and character ε. We suppose that f is an eigenform for T_p, $p \nmid N$, with eigenvalues a_p. Then the series $\sum_{p \nmid N} |a_p|^2 p^{-s}$ converges for all real $s > k$, and we have*

$$\sum_{p \nmid N} |a_p|^2 p^{-s} \leq \log(1/(s-k)) + O(1) \qquad \text{for} \quad s \to k$$

Our primary interest in the preceding result is that it implies a rather strong finiteness result on the eigenvalues a_p which show up in weight 1 modular forms. Before proving this result, we need a definition.

Definition 5.2. Let P be the set of prime numbers and $X \subset P$ a subset. Define the *upper density* of X to be

$$\mathrm{dens.sup}X = \limsup_{s\to 1, s>1} \left(\sum_{p\in X} p^{-s} \right) / \log(1/(s-1))$$

This is a number between 0 and 1.

Proposition 5.3. *We assume the same hypotheses as in Proposition 5.1, and we further assume that the weight k of f is 1. Then, for all $\eta > 0$, there exists a set X_η of primes numbers and a finite subset $Y_\eta \subset \mathbb{C}$ of complex numbers such that*

$$\mathrm{dens.sup}X_\eta \leq \eta \qquad \textit{and} \qquad a_p \in Y_\eta \quad \textit{for all } p \notin X_\eta$$

Proof. It is known that the a_p are contained in the ring of integers of a finite extension K of $\mathbb{Q}$. If $c \geq 0$ is a constant, denote by $Y(c)$ the set of integral elements a of K such that $|\sigma(a)|^2 \leq c$ for all embeddings $\sigma : K \hookrightarrow \mathbb{C}$; this is a finite set. Denote by $X(c)$ the set of prime numbers p such that $a_p \notin Y(c)$. It is sufficient to prove that $\mathrm{dens.sup}X(c) \leq \eta$ for large enough c.

For any embedding σ of K into $\mathbb{C}$, $\sigma(f)$ is a modular form of weight 1, level $\Gamma_0(N)$, and character $\sigma(\varepsilon)$, and satisfies $T_p\sigma(f) = \sigma(a_p)\sigma(f)$. Thus, by Proposition 5.1, we have

$$\sum_\sigma \sum_p |\sigma(a_p)|^2 p^{-s} \leq r \log(1/(s-1)) + O(1) \qquad \text{for} \quad s \to 1$$

where $r = [K : \mathbb{Q}]$. Since $\sum_\sigma |\sigma(a_p)|^2 \geq c$ if $p \in X(c)$, we conclude that

$$c \sum_{p\in X(c)} p^{-s} \leq r \log(1/(s-1)) + O(1) \qquad \text{for} \quad s \to 1$$

hence

$$\mathrm{dens.sup}X(c) \leq r/c$$

and it is enough to take $c \geq r/n$. □

Next, we prove a result on upper bounds of the cardinality of linear groups over finite fields. Let ℓ be a prime number and let $\mathbb{F}_\ell$ be the finite field of ℓ elements. Let η, M be positive numbers, and let G be a subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell)$. We will make use of the following definition:

Definition 5.4. We say that G satisfies the condition $C(\eta, M)$ if there exists a subset $H \subset G$ with $|H| \geq (1-\eta)|G|$ such that the set of polynomials $\det(1-hT)$, $h \in H$, has at most M elements.

We say that G is semisimple if the identity representation $G \hookrightarrow \mathrm{GL}_2(\mathbb{F}_\ell)$ is semisimple.

Proposition 5.5. *Let $\eta < 1/2$ and $M \geq 0$. There exists a constant $A = A(\eta, M)$ such that, for all prime numbers ℓ and semisimple subgroups $G \subset \mathrm{GL}_2(\mathbb{F}_\ell)$ satisfying $C(\eta, M)$, we have $|G| \leq A$.*

Proof. Let G be a semisimple subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell)$. Recall that one of the following conditions is satisfied:

(a) G contains $\mathrm{SL}_2(\mathbb{F}_\ell)$

(b) G is contained in a Cartan subgroup T

(c) G is contained in the normalizer of a Cartan subgroup T, and is not contained in T

(d) The image of G in $\mathrm{PGL}_2(\mathbb{F}_\ell) = \mathrm{GL}_2(\mathbb{F}_\ell)/\mathbb{F}_\ell^*$ is isomorphic to the symmetric group $\mathfrak{S}_4$ or one of the alternating groups $\mathfrak{A}_4, \mathfrak{A}_5$

We provide an upper bound of $|G|$ in each case.

Case (a) – We set $r = [G : \mathrm{SL}_2(\mathbb{F}_\ell)]$. Then $|G| = r\ell(\ell^2 - 1)$. On the other hand, the number of elements of $\mathrm{GL}_2(\mathbb{F}_\ell)$ with a given characteristic polynomial is $\ell^2 + \ell$, ℓ^2, or $\ell^2 - \ell$, corresponding to when the polynomial in question has 2, 1, or 0 roots in $\mathbb{F}_\ell$, respectively. If G satisfies $C(\eta, M)$, we then have

$$(1 - \eta)r\ell(\ell^2 - 1) = (1 - \eta)|G| \leq |H| \leq M(\ell^2 + \ell)$$

hence

$$(1 - \eta)r(\ell - 1) \leq M$$

and thus

$$\ell \leq 1 + \frac{M}{(1 - \eta)r} \leq 1 + \frac{M}{1 - \eta}$$

which gives an upper bound on ℓ, and therefore an upper bound on $|G|$.

Case (b) – At most 2 elements of T have a given characteristic polynomial. The hypothesis $C(\eta, M)$ (with $\eta < 1$) therefore gives

$$(1 - \eta)|G| \leq 2M$$

which gives the upper bound

$$|G| \leq \frac{2M}{1 - \eta}$$

Case (c) – The group $G' = G \cap T$ is index 2 in G. If G satisfies $C(\eta, M)$, G' satisfies $C(2\eta, M)$. Applying case *(b)* to G', we obtain

$$|G| \leq \frac{4M}{1 - 2\eta}$$

Case (d) – The image of G in $\mathrm{PGL}_2(\mathbb{F}_\ell)$ has order at most 60. The group $G \cap \mathrm{SL}_2(\mathbb{F}_\ell)$ is then of order at most 120, and there are in G at most 120 elements of a given determinant, hence *a fortiori* of a given characteristic polynomial. If G satisfies $C(\eta, M)$, then we have

$$(1 - \eta)|G| \leq 120M$$

and thus

$$|G| \leq \frac{120M}{1 - \eta}$$

□

We can apply the above theory to the Galois representations constructed in Section 4. Specifically, let f be a cusp form satisfying the hypotheses of Theorem 1.1. The numbers a_p and $\varepsilon(p)$ belong to the ring of integers $\mathcal{O}_K$ of a number field K, which we assume to be Galois over $\mathbb{Q}$. Let L be the set of primes numbers ℓ which split completely in K. For all $\ell \in L$, we choose a place λ_ℓ of K above ℓ; the corresponding residue field is equal to $\mathbb{F}_\ell$. By Proposition 4.1, there exists a continuous semisimple representation

$$\rho_\ell : G_\mathbb{Q} \to \mathrm{GL}_2(\mathbb{F}_\ell)$$

which is unramified away from $N\ell$ and such that

$$\det(1 - \rho_\ell(\mathrm{Frob}_p)T) \equiv 1 - a_p T + \varepsilon(p)T^2 \pmod{\lambda_\ell} \qquad \text{if} \quad p \nmid N\ell$$

Let G_ℓ denote the subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell)$ given by the image of ρ_ℓ.

Lemma 5.6. *With notation as above, for all $\eta > 0$, there exists a constant M such that G_ℓ satisfies the condition $C(\eta, M)$ for all $\ell \in L$.*

Proof. By Proposition 5.3, there exists a subset X_η of the set P of prime numbers such that $\mathrm{dens.sup} X_\eta \leq \eta$ and that the a_p for $p \notin X_\eta$ form a finite set. Denote by $\mathcal{M}$ the finite set of polynomials $1 - a_p T + \varepsilon(p)T^2$ for $p \notin X_\eta$, and set $M = |\mathcal{M}|$. We claim that G_ℓ satisfies $C(\eta, M)$ for all $\ell \in L$. Indeed, let H_ℓ be the subset of G_ℓ of Frobenius elements $\rho_\ell(\mathrm{Frob}_p)$ for $p \notin X_\eta$ and their conjugates. By Chebotarev density (Proposition 2.2), we have that $|H_\ell| \geq (1-\eta)|G_\ell|$. On the other hand, if $h \in H_\ell$, the polynomial $\det(1 - hT)$ is the reduction mod λ_ℓ of an element of $\mathcal{M}$, so it belongs to a set of at most M elements. The condition $C(\eta, M)$ is therefore satisfied. □

Corollary 5.7. *There exists a constant A such that $|G_\ell| \leq A$ for all $\ell \in L$.*

Proof. This follows immediately by the preceding lemma combined with Proposition 5.5. □

6 Galois Representations Attached to Modular Forms of Weight 1

In this section, we prove Theorem 1.1, covering the rest of section 8 of [DS74].

Proof of Theorem 1.1. We can assume that f is either an Eisenstein series or a cusp form. If f is an Eisenstein series, the proof is identical to the weight ≥ 2 case: there exist characters χ_1, χ_2 of $(\mathbb{Z}/N\mathbb{Z})^*$ such that $\chi_1 \cdot \chi_2 = \varepsilon$ and $\chi_1(p) + \chi_2(p) = a_p$ for $p \nmid N$, and the reducible representation ρ is given by $\rho = \chi_1 \oplus \chi_2$.

Henceforth, we assume that f is a cusp form. We recall the notation of the end of section 5: let K be a finite Galois extension of $\mathbb{Q}$ such that its ring of integers $\mathcal{O}_K$ contains the numbers a_p and $\varepsilon(p)$, and let L be the set of prime

numbers which split completely in K. For each $\ell \in L$, choose a place λ_ℓ of K over ℓ; its residue field is $\mathbb{F}_\ell$. By Proposition 4.1, there exists a continuous semisimple representation

$$\rho_\ell : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_\ell)$$

which is unramified away from $N\ell$ and such that

$$\det(1 - \rho_\ell(\mathrm{Frob}_p)T) \equiv 1 - a_p T + \varepsilon(p)T^2 \pmod{\lambda_\ell} \qquad \text{if} \quad p \nmid N\ell$$

Let G_ℓ denote the subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell)$ given by the image of ρ_ℓ. By Corollary 5.7, we may choose a constant A such that $|G_\ell| \leq A$ for all $\ell \in L$. By enlarging K (which would reduce L), we may assume that K contains the nth roots of unity for all $n \leq A$. Let Y be the set of polynomials $(1 - \alpha T)(1 - \beta T)$, where α, β are roots of unity of order $\leq A$. If $p \nmid N$, for all $\ell \in L$ with $\ell \neq p$ there exists $R(T) \in Y$ such that

$$1 - a_p T + \varepsilon(p)T^2 \equiv R(T) \pmod{\lambda_\ell}$$

Since Y is finite, there exists an R such that the above congruence is satisfied for infinitely many ℓ, and thus we have an equality

$$1 - a_p T + \varepsilon(p)T^2 = R(T)$$

In other words, the polynomials $1 - a_p T + \varepsilon(p)T^2$ are contained in Y.

Let L' be the set of $\ell \in L$ such that $\ell > A$ and that $R, S \in Y, R \neq S$ implies $R \not\equiv S \pmod{\lambda_\ell}$; the set of $L \setminus L'$ is finite, so L' is infinite. Let $\ell \in L'$. The order of the group G_ℓ is prime to ℓ. It then follows, by a standard argument, that the identity representation $G_\ell \to \mathrm{GL}_2(\mathbb{F}_\ell)$ is the reduction mod λ_ℓ of a representation $G_\ell \to \mathrm{GL}_2(\mathcal{O}_{\lambda_\ell})$, where $\mathcal{O}_{\lambda_\ell}$ is the valuation ring for λ_ℓ. By combining this representation with the canonical map $G_{\mathbb{Q}} \to G_\ell$, we obtain the representation

$$\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathcal{O}_{\lambda_\ell})$$

By construction, ρ is unramified away from $N\ell$. If $p \nmid N\ell$, the eigenvalues of the Frobenius element $\rho(\mathrm{Frob}_p)$ are roots of unity of order $\leq A$ (because the image of ρ is isomorphic to G_ℓ, so has order $\leq A$); thus, $\det(1 - \rho(\mathrm{Frob}_p)T) \in Y$. On the other hand, because the reduction of ρ mod λ_ℓ is ρ_ℓ, we have

$$\det(1 - \rho(\mathrm{Frob}_p)T) \equiv 1 - a_p T + \varepsilon(p)T^2 \pmod{\lambda_\ell}$$

But the two polynomials $\det(1 - \rho(\mathrm{Frob}_p)T)$ and $1 - a_p T + \varepsilon(p)T^2$ are contained in Y. Since they are congruence mod λ_ℓ, they are equal, hence we have

$$\det(1 - \rho(\mathrm{Frob}_p)T) = 1 - a_p T + \varepsilon(p)T^2 \quad \text{for all } p \nmid N\ell$$

Let's now consider another prime number $\ell' \in L'$. We obtain a representation $\rho' : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathcal{O}_{\lambda_{\ell'}})$ in the same way as above, but for $p \nmid N\ell'$. In particular, we have

$$\det(1 - \rho(\mathrm{Frob}_p)T) = \det(1 - \rho'(\mathrm{Frob}_p)T) \quad \text{for all } p \nmid N\ell\ell'$$

By Proposition 2.5, this implies that ρ and ρ' are isomorphic as representations of K, and *a fortiori* as complex representations. It follows that ρ is unramified away from N, and that

$$\det(1 - \rho(\mathrm{Frob}_p)T) = 1 - a_p T + \varepsilon(p)T^2 \quad \text{for all } p \nmid N$$

It remains to show that ρ is irreducible. Suppose ρ is reducible, so it is the sum of two 1-dimensional representations. That is, there exist characters χ_1, χ_2 unramified away from N and such that

$$a_p = \chi_1(p) + \chi_2(p) \quad \text{for all } p \nmid N$$

Then we have

$$\sum |a_p|^2 p^{-s} = 2\sum \chi_1(p)\overline{\chi}_2(p)p^{-s} + \sum \chi_2(p)\overline{\chi}_1(p)p^{-s}$$

As s approaches 1, we have $\sum p^{-s} = \log(1/(s-1)) + O(1)$. On the other hand, the character $\chi_1\overline{\chi_2} \neq 1$ (otherwise $\varepsilon = \chi_1^2$ and $\varepsilon(-1) = 1$). It then follows that

$$\sum \chi_1(p)\overline{\chi}_2(p)p^{-s} = O(1) \qquad \text{and} \qquad \sum \chi_2(p)\overline{\chi}_1(p)p^{-s} = O(1)$$

From this, we obtain that

$$\sum |a_p|^2 p^{-s} = 2\log(1/(s-1)) + O(1) \qquad \text{for} \quad s \to 1$$

which contradicts Proposition 5.1. □

References

[Del71] Pierre Deligne. Formes modulaires et représentations l-adiques. In *Séminaire Bourbaki. Vol. 1968/69: Exposés 347–363*, volume 175 of *Lecture Notes in Math.*, pages Exp. No. 355, 139–172. Springer, Berlin, 1971.

[DS74] Pierre Deligne and Jean-Pierre Serre. Formes modulaires de poids 1. *Ann. Sci. École Norm. Sup. (4)*, 7:507–530, 1974.

[DS05] Fred Diamond and Jerry Shurman. *A first course in modular forms*, volume 228 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2005.

[Hec83] Erich Hecke. *Mathematische Werke*. Vandenhoeck & Ruprecht, Göttingen, third edition, 1983. With introductory material by B. Schoeneberg, C. L. Siegel and J. Nielsen.

[Miy06] Toshitsune Miyake. *Modular forms*. Springer Monographs in Mathematics. Springer-Verlag, Berlin, english edition, 2006. Translated from the 1976 Japanese original by Yoshitaka Maeda.

[Neu99] Jürgen Neukirch. *Algebraic number theory*, volume 322 of *Grundlehren der mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1999. Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder.