GALOIS REPRESENTATIONS ATTACHED TO MODULAR FORMS OF WEIGHT 1

AYAN NATH

Abstract. We provide an account of Deligne and Serre's result on attaching a two-dimensional Artin representation to a modular form of weight 1.

1 The main result

1.1. Theorem (Deligne-Serre). — *Let f be a normalized cuspidal newform of weight 1 and level N with Fourier coefficients a_n and Nebentypus χ satisfying $\chi(-1) = -1$. Then there exists an irreducible semisimple Galois representation $\rho_f \colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{C})$ which is unramified at all primes p not dividing N and Frob_p, any arithmetic Frobenius over p, has characteristic polynomial $X^2 - a_pX + \chi(p)$.*

Brauer-Nesbitt theorem from representation theory tells us that semisimple representations are uniquely determined upto isomorphism by their characteristic polynomials. Together with this and Chebotarev density theorem and some continuity arguments, it can be shown that the equality

$$\det(XI_2 - \rho_f(\mathrm{Frob}_p)) = X^2 - a_pX + \chi(p), \quad \text{for all } p \nmid N,$$

determines ρ_f, if exists, upto isomorphism.

2 Overview of the proof

Let $K_f = \mathbb{Q}(a_1, a_2, \ldots)$ be the number field associated to f. Define $\mathscr{L}$ to be the set of primes $p \in \mathbb{Z}$ which split completely in K_f, that is, $\mathscr{L}$ is the complement of the branch divisor of $\mathrm{Spec}\,\mathscr{O}_{K_f} \to \mathrm{Spec}\,\mathbb{Z}$. This is a cofinite set.

2.1. Definition. If λ is a prime of K_f above a rational prime $\ell \in \mathbb{Z}$, we say $f \in M_k(N,\chi)$ is **λ-integral** if its Fourier coefficients are in $\mathscr{O}_\lambda$, the local number ring at λ. Modular arithmetic for λ-integral modular forms is defined in the expected way.

2.2. Theorem (attaching mod ℓ Galois representations). — *Let f be a cusp form with K_f the field of definition of its Fourier series and Nebentypus χ. Let K be a number field containing K_f. Let λ be a prime of K above a rational prime $\ell \in \mathbb{Z}$. Suppose f is λ-integral and not all Fourier coefficients of f lie in the maximal ideal of $\mathscr{O}_\lambda$. Also let f be an eigenform away from $N\ell$ modulo λ with eigenvalues a_p in the sense that f is an eigenvector of T_p modulo λ with eigenvalue $a_p \in k_\lambda$ for all primes $p \nmid N\ell$. Further, let k be the subfield of k_λ generated by the eigenvalues a_p and the images of $\chi(p)$ for each $p \nmid N\ell$. Then there exists a semisimple representation $\rho \colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(k)$ which is unramified away from $N\ell$ such that for each prime $p \nmid N\ell$, the characteristic polynomial of $\rho(\mathrm{Frob}_p)$ is congruent to $X^2 - a_pX + \chi(p)p^{k-1}$ modulo λ.*

Proof. See Section 3. □

Date: 27th August, 2023.
Affiliation: BSc 3rd year, Chennai Mathematical Institute.

For each $\ell \in \mathscr{L}$, choose a prime $\lambda_\ell \in \operatorname{Spec}\mathscr{O}_{K_f}$ above ℓ. Apply Theorem 2.2 to get a mod ℓ Galois representation $\overline{\rho}_\ell \colon \operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F}_\ell)$ for each $\ell \in \mathscr{L}$.

2.3. Lemma. — *There exists a constant A such that $\#\operatorname{Im}\overline{\rho}_\ell \leqslant A$ for all $\ell \in \mathscr{L}$.*

Proof. See Section 4. □

We fix such a constant A. Adjoining algebraic numbers to K_f can only take away finitely many elements from $\mathscr{L}$. So we assume K_f has all nth roots of unity for each $n \leqslant A$. Denote by Y the (finite) set of polynomials of the form $(1-\alpha T)(1-\beta T)$ where α and β are roots of unity of order at most A. Let p be a fixed prime not dividing N. For each $\ell \in \mathscr{L}, \ell \neq p$, $1 - a_p T + \chi(p)T^2$ is congruent modulo λ_ℓ to an element of Y. This means that there is a fixed element of Y which is congruent to $1 - a_p T + \chi(p)T^2$ modulo infinitely many places λ_ℓ. This means that $1 - a_p T + \chi(p)T^2 \in Y$. Set $\mathscr{L}' = \{\ell \in \mathscr{L} : \ell > A \text{ and } R \equiv S \pmod{\lambda_\ell} \implies R = S \text{ for } R, S \in Y\}$. We may go ahead and replace $\mathscr{L}$ by $\mathscr{L}'$ since $\mathscr{L} \setminus \mathscr{L}'$ is finite.

2.4. Definition. Let G be a finite group. A number field is called a **splitting field** for G if any representation $G \to \mathrm{GL}_d(K)$ is irreducible over K if and only if it is irreducible over $\overline{K}$.

By [Fei, §1.11], we may replace K_f with a finite extension so that K_f becomes a splitting field for all groups of order at most A.

2.5. Theorem. — *Let G be a finite group whose order is not divisible by a prime p, K be a splitting number field for G, $\mathfrak{p}$ be a prime lying above the rational prime p. Also let $(\mathscr{O}_\mathfrak{p}, k_\mathfrak{p})$ be the local number ring at $\mathfrak{p}$. Then there is a bijective correspondence between isomorphism classes of representations $\rho \colon G \to \mathrm{GL}_n(\mathscr{O}_\mathfrak{p})$ and that of representations $\overline{\rho} \colon G \to \mathrm{GL}_n(k_\mathfrak{p})$ given by composing with the natural projection $\mathrm{GL}_n(\mathscr{O}_\mathfrak{p}) \to \mathrm{GL}_n(k_\mathfrak{p})$. Further, ρ is absolutely irreducible if and only if $\overline{\rho}$ is.*

Proof. See [Fei, §4.3]. □

Thus, for each $\ell \in \mathscr{L}$, we may lift $\overline{\rho}_\ell$ to a representation $\rho_\ell \colon \operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathscr{O}_{\lambda_\ell}) \hookrightarrow \mathrm{GL}_2(\mathbb{C})$ which is unramified away from $N\ell$. Here, we are implicitly using that $\operatorname{Im}\overline{\rho}_\ell$ is finite since $\operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ is profinite. By definition of $\mathscr{L}'$ we deduce $\det(1-\rho_\ell(\mathrm{Frob}_p)T) = 1 - a_p T + \chi(p)T^2$ for each prime $p \nmid N\ell$. By Brauer-Nesbitt and Chebotarev density theorem, all the ρ_ℓ are isomorphic for different primes ℓ. Therefore, we get a single Artin representation $\rho \colon \operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{C})$ which is unramified away from N and satisfies $\det(1-\rho(\mathrm{Frob}_p)T) = 1 - a_p T + \chi(p)T^2$ for each prime $p \nmid N$. Now we have to show that ρ is irreducible. Suppose not, and ρ be equal to $\chi_1 \oplus \chi_2$ for two Galois characters χ_1 and χ_2. Then

$$\sum_{p\nmid N} \frac{|a_p|^2}{p^s} = 2\sum_{p\nmid N}\frac{1}{p^s} + \sum_{p\nmid N}\frac{\chi_1(p)\overline{\chi_2(p)}}{p^s} + \sum_{p\nmid N}\frac{\overline{\chi_1(p)}\chi_2(p)}{p^s}.$$

Note that $\chi_1 \neq \chi_2$ as $\chi = \chi_1\chi_2$ satisfies $\chi(-1) = -1$. By routine estimation,

$$\sum_{p\nmid N}\frac{1}{p^s} = \log\left(\frac{1}{s-1}\right) + O(1), \qquad \sum_{p\nmid N}\frac{\chi_1(p)\overline{\chi_2(p)}}{p^s} = O(1)$$

as $s \to 1^+$. But this contradicts the following, which we treat as a blackbox–

2.6. Lemma (Rankin). — *Let $f = \sum_{n=1}^\infty a_n q^n$ be a weight k Hecke eigenform for T_p away from the level N. Then*

$$\sum_{p\nmid N}\frac{|a_p|^2}{p^s} \leqslant \log\left(\frac{1}{s-k}\right) + O(1)$$

as $s \to k^+$.

3 Proof of Theorem 2.2: reducing Galois representations mod ℓ

We would like to use the following result of Deligne–

3.1. Theorem (Deligne). — *Let ℓ be a prime and f be a normalized cuspidal newform of weight $k \geqslant 2$ and level N with Fourier coefficients a_n and Nebentypus χ. Let λ be a prime in K_f above ℓ and $K_{f,\lambda}$ be the completion of K_f at λ. Then there exists a semisimple Galois representation $\rho_{f,\ell}\colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(K_{f,\lambda})$ which is unramified at all primes p not dividing ℓN and Frob_p, any arithmetic Frobenius over p, has characteristic polynomial $X^2 - a_p X + p^{k-1}\chi(p)$.*

Without any loss in generality, we may change the data $(K, \lambda, f, k, \chi, (a_p))$ to $(K', \lambda', f', k', \chi', (a'_p))$ as long as $K \subset K'$, λ' lies above λ, λ' divides both $a_p - a'_p$ and $p^{k-1}\chi(p) - p^{k'-1}\chi'(p)$ for each prime p away from $N\ell$. Suppose $k = 1$ and E_n be the normalized Eisenstein series of level 1 and weight n defined by

$$E_n(z) = 1 - \frac{2n}{B_n}\sum_{m=1}^{\infty} \sigma_{n-1}(m) q^m.$$

It is a theorem of Von Staudt-Clausen that the denominator of B_n is the product of all primes p such that $p - 1 \mid n$. Therefore, setting $n = \ell - 1$, it follows that fE_n, which is of weight ℓ, is congruent to f modulo λ.

3.2. Lemma (Deligne-Serre lifting lemma). — *Let M be a free module of finite rank over a DVR $(\mathscr{O}, \mathfrak{m}, k)$ with fraction field K. Let S be a set of commuting $\mathscr{O}$-linear endomorphisms of M. Let $f \in M$ be a nonzero eigenvector modulo $\mathfrak{m}M$ for all operators in S, i.e., $Tf = a_T f \pmod{\mathfrak{m}M}$ for each $T \in S$. Then there exists a DVR $(\mathscr{O}', \mathfrak{m}', k')$, containing $\mathscr{O}$, with $\mathfrak{m} \subseteq \mathfrak{m}'$, whose field of fractions K' is a finite extension of K and a nonzero $f' \in \mathscr{O}' \otimes_{\mathscr{O}} M$ such that $Tf' = a'_T f'$, $a'_T \in \mathscr{O}'$ for each $T \in S$ satisfying $a'_T \equiv a_T \pmod{\mathfrak{m}'}$.*

Proof. See, for e.g., [Sai09, §4.1]. □

Using the above lemma we can find an honest cusp form f' of weight ℓ which is an eigenform for T_p, $p \nmid N\ell$, with eigenvalues a'_p so that $a'_p \equiv a_p \pmod{\lambda'}$ where λ' is some prime lying over λ. Note that f' must also be an eigenvector for T_ℓ since $\ell \nmid N$. Applying Theorem 3.1, we get a semisimple Galois representation $\rho_\lambda\colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(K_\lambda)$.

3.3. Lemma. — *Let F be a nonarchimedian local field. Let G be a profinite group and $\rho\colon G \to \mathrm{GL}_d(F)$ a continuous representation. Then ρ can be conjugated to a representation with values in $\mathrm{GL}_d(\mathscr{O}_F)$.*

Proof. Choose a basis and consider the standard lattice $L = \mathscr{O}_F^{\oplus d}$. The stabilizer of L is precisely $\mathrm{GL}_d(\mathscr{O}_F)$, which is open in $\mathrm{GL}_d(F)$. Set $H = \rho^{-1}(\mathrm{GL}_d(\mathscr{O}_F))$, an open subgroup. Then G/H is finite and G stabilizes $\sum_{g \in G/H} gL$. □

Using the above lemma, we may assume that the codomain of ρ_λ is $\mathrm{GL}_2(\widehat{\mathscr{O}}_\lambda)$ and subsequently compose with $\mathrm{GL}_2(\widehat{\mathscr{O}}_\lambda) \to \mathrm{GL}_2(k_\lambda)$ to get a mod ℓ representation $\overline{\rho}_\lambda\colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(k_\lambda)$. We then take the "semisimplification" of this to get a semisimple representation $\overline{\rho}_\lambda^{\mathrm{ss}}$. This is also unramified away from $N\ell$. What remains is to show that $\overline{\rho}_\lambda^{\mathrm{ss}}$ is realizable over k, the subfield of k_λ generated by the eigenvalues a_p and the images of $\chi(p)$ for each $p \nmid N\ell$. Due to Brauer-Nesbitt and Chebotarev density theorem, $\overline{\rho}_\lambda^{\mathrm{ss}}$ is conjugated under $\mathrm{Gal}(k_\lambda/k)$-action. It thus follows from Hilbert 90 that $\overline{\rho}_\lambda^{\mathrm{ss}}$ can be defined over k.

4 Proof of Lemma 2.3: images of mod ℓ representations

4.1. Definition. Let $\eta, M > 0$. A subgroup $G \subseteq \mathrm{GL}_2(\mathbb{F}_\ell)$ is said to satisfy $C(\eta, M)$ if there exists $H \subset G$ such that $|H| \geqslant (1-\eta)|G|$ and the set the characteristic polynomials $\{\det(1-hT) : h \in H\}$ has at most M elements.

4.2. Lemma. — *For each prime ℓ, let $G_\ell \subset \mathrm{GL}_2(\mathbb{F}_\ell)$ be a semisimple subgroup. Assume there exists $\eta < 1/2$ and $M \geqslant 0$ such that for all primes ℓ, G_ℓ satisfies $C(\eta, M)$. Then there exists $A = A(\eta, M) > 0$ such that for each ℓ, $|G_\ell| \geqslant A$.*

Proof. The proof uses classification of semisimple subgroups of $\mathrm{GL}_2(\mathbb{F}_\ell)$. See [DeSe]. □

To apply the above result, we need to show that $\mathrm{Im}\,\overline{\rho}_\ell$ satisfies a $C(\eta, M)$ property–

4.3. Lemma. — *For each $\eta < 1/2$ there exists $M > 0$, depending on η, such that for each prime $\ell \in \mathscr{L}$, $\mathrm{Im}\,\overline{\rho}_\ell$ satisfies $C(\eta, M)$.*

4.4. Definition. — Let X be a set of (rational) primes. Define the **upper density** of X as

$$\overline{\delta}(X) = \limsup_{s \to 1^+} \frac{\sum_{p \in X} \frac{1}{p^s}}{\log\left(\frac{1}{s-1}\right)}.$$

4.5. *Proof of Lemma 4.3.* For any positive real number c, define

$$Y(c) := \{a \in K_f : |\sigma(a)| \leqslant c \text{ for all complex embeddings } \sigma \text{ of } K_f\}$$
$$X(c) := \{p \text{ prime number} : a_p \notin Y(c)\}.$$

It's clear that $Y(c)$ are finite sets. Applying Lemma 2.6 to f^σ for each embedding $\sigma : K_f \hookrightarrow \mathbb{C}$ and summing, we get

$$\sum_{\substack{\sigma : K_f \hookrightarrow \mathbb{C}, \\ p \nmid N}} \frac{|\sigma(a_p)|^2}{p^s} \leqslant [K_f : \mathbb{Q}] \log\left(\frac{1}{s-1}\right) + O(1)$$

as $s \to 1^+$. From where we get

$$c \sum_{p \in X(c)} \frac{1}{p^s} \leqslant [K_f : \mathbb{Q}] \log\left(\frac{1}{s-1}\right) + O(1)$$

as $s \to 1^+$. In particular, $\overline{\delta}(X(c)) \leqslant \frac{1}{c}[K_f : \mathbb{Q}]$. Choose $c > [K_f : \mathbb{Q}]/\eta$. Note that $\{a_p : p \notin X(c)\} \subseteq Y(c)$ is a finite set. The set $\{X^2 - a_p T + \chi(p) : p \notin X(c)\}$ is also therefore finite, say of cardinality $M-1$. Then $\mathrm{Im}\,\overline{\rho}_\ell$ satisfies property $C(\eta, M)$. Indeed, consider the subgroup H_ℓ of G_ℓ generated by $\{\overline{\rho}_\ell(\mathrm{Frob}_p) : p \notin X(c)\}$ and conjugates thereof. An application of Chebotarev density theorem shows that H_ℓ satisfies the desired properties. □

References

[DeSe] P. Deligne and J-P. Serre, *Formes modulaires de poids 1*, Ann. Sci. École Norm. Sup (4), 7:507–530, 1974.
[Fei] W. Feit, *Characters of finite groups*, Mathematics lecture notes, W. A. Benjamin, New York, 1967
[Sai09] A. Saikia. *Ribet's construction of a suitable cusp eigenform*, arXiv:0910.1408v2, 2009
[Lag] J. Laga, *Modular forms of weight one*, https://www.dpmms.cam.ac.uk/~jcsl5/partIIIessay.pdf