GALOIS REPRESENTATIONS

ANIRUDDHA SUDARSHAN

ABSTRACT. These are the notes for an introductory talk on Galois representations in the Algebra Number Theory Seminar at IISER Bhopal.

CONTENTS

1. Introduction 1
1.1. Profinite groups 2
1.2. Ramification of a Galois representation 3
1.3. The Artin L-functions 5
2. The Chebotarev density theorem 7
3. Traces of Galois representations 8
3.1. Multiplicity one theorems 8
References 13

1. INTRODUCTION

Fermat's Last Theorem states that the equation $X^n + Y^n = Z^n$ has no non-trivial integral solutions in X, Y, Z for $n > 2$. Its proof, which took nearly about 350 years, is due to the settlement of the *Taniyama–Shimura–Weil conjecture* (the modularity conjecture) by many mathematicians starting from Wiles. There are certain (2-dimensional) *Galois representations* attached to elliptic curves and Hecke eigenforms. The Taniyama–Shimura–Weil conjecture states that the Galois representations attached to elliptic curves over $\mathbb{Q}$ must arise from a Galois representation attached to a Hecke eigenform.

Throughout the notes, F is a number field (a finite extension of $\mathbb{Q}$), $\overline{F}$ is a fixed algebraic closure of F, and we denote G_F for the absolute Galois group $\mathrm{Gal}(\overline{F}/F)$.

DEFINITION 1.1. For a topological ring R, a *Galois representation* of G_F into R is a continuous representation $G_F \to \mathrm{GL}_n(R)$.

Remarks. In the above definition, the Galois group G_F is endowed with the Krull topology. In this topology, the basic open sets are of the form

$$B(\sigma, L) := \{\tau \in G_F \mid \tau = \sigma \text{ on } L\} = \{\tau \in G_F \mid \tau\sigma^{-1} \in \mathrm{Gal}(\overline{F}/L)\}.$$

Moreover, we have a topological group isomorphism (cf. Section 1.1)

$$G_F \cong \varprojlim_{L/F \text{ finite}} \mathrm{Gal}(L/F).$$

This makes the absolute Galois group of F a compact topological group. For infinite Galois theory, a good reference is Neukirch [Neu99].

EXAMPLE 1.2 ($\bmod p^m$ CYCLOTOMIC CHARACTER). Let p be a prime, m be a positive integer, and let $\mu_{p,m} = \{z \in \mathbb{C} \mid z^{p^m} = 1\}$ be the set of p^m-th roots of unity. We have the representation

$$\varepsilon_{p,m} : G_{\mathbb{Q}} \xrightarrow{restriction} \mathrm{Gal}(\mathbb{Q}(\mu_{p,m})/\mathbb{Q}) \cong (\mathbb{Z}/p^m\mathbb{Z})^*.$$

EXAMPLE 1.3 (TORSION POINTS OF AN ELLIPTIC CURVE). An elliptic curve over $\mathbb{Q}$ is a projective curve given by the equation of type,

$$y^2 = x^3 + ax + b, \quad a, b \in \mathbb{Q},$$

with a point $[0,1,0]$ at infinity. Denote

$$E(\overline{\mathbb{Q}}) = \{[x,y,1] \in \overline{\mathbb{Q}} \mid y^2 = x^3 + ax + b\} \cup \{[0,1,0]\}.$$

The set $E(\overline{\mathbb{Q}})$ forms a group under a specific operation $+$. For a positive integer m, define the multiplication-by-m map by,

$$[m] : E(\overline{\mathbb{Q}}) \to E(\overline{\mathbb{Q}}), \quad [m](P) = \underbrace{P + \cdots + P}_{m\text{-times}}$$

Denote $E[m] = \ker[m]$. An isomorphism $E[m] \cong (\mathbb{Z}/m\mathbb{Z})^2$ and the action of $G_{\mathbb{Q}}$ on $E[m]$ induces the representation,

$$\rho_{E,m} : G_{\mathbb{Q}} \to \mathrm{Aut}_{\mathbb{Z}}((\mathbb{Z}/m\mathbb{Z})^2) \cong \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z}).$$

1.1. **Profinite groups.** A *directed set* is a poset $(I, \leq)$ such that, for any $a, b \in I$, there is a $c \in I$ such that $a \leq c$ and $b \leq c$.

Examples.

1. The usual partial order $\leq$ on $\mathbb{R}$ makes $(\mathbb{R}, \leq)$ a directed set.
2. Consider the set $(\mathbb{N}, \leq)$ where $a \leq b$ when $b|a$. This is a directed set as, for $a, b \in \mathbb{N}$, we have $c = \gcd(a,b)$ such that $a \leq c$ and $b \leq c$.

Let $(I, \leq)$ be a directed set. The set of groups $\{G_i \mid i \in I\}$ is called an *inverse system* with respect to (group) homomorphisms $\{\varphi_i^j : G_j \to G_i \mid i \leq j\}$ if:

1. $\varphi_i^i : G_i \to G_i$ is an isomorphism for all $i \in I$.
2. If $i \leq j \leq k$, then $\varphi_i^k = \varphi_i^j \circ \varphi_j^k$.

Given an inverse system $(\{G_i\}_{i \in I}, \{\varphi_i^j : i \leq j\})$, we define its *projective (or inverse) limit* as

$$\varprojlim_{i \in I} G_i := \{(g_i)_{i \in I} \mid \varphi_i^j(g_j) = g_i \text{ for all } i \leq j\} \subseteq \prod_{i \in I} G_i.$$

We have the natural projection maps $\pi_j : \varprojlim G_i \to G_j$ for all $j \in I$. The projective limit satisfies the following universal property: Given a group G with homomorphisms $\phi_i : G \to G_i$ such that $\phi_i = \varphi_i^j \circ \phi_j$, for all $i \in I$, then there is a unique homomorphism from $\phi : G \to \varprojlim G_i$ such that $\phi \circ \pi_i = \phi_i$.

DEFINITION 1.4. A *profinite group* is a projective limit of finite groups.

Examples.

1. Let $(\mathbb{N}, \leq)$ be a directed set with $\leq$ the partial order induced by the partial order on $\mathbb{R}$. Given a prime p, consider the set of groups $\{\mathbb{Z}/p^n\mathbb{Z}\}_{n \in \mathbb{N}}$. For $n \leq m$, define the map

$$\varphi_n^m : \mathbb{Z}/p^m\mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z}, \quad a \bmod p^m \mapsto a \bmod p^n.$$

We see that $(\mathbb{Z}/p^n\mathbb{Z}, \{\varphi_n^m \mid n \leq m\})_{n \in \mathbb{N}}$ form an inverse system, whose projective limit is isomorphic to $\mathbb{Z}_p$.

2. Let $(\mathbb{N}, \leq)$ be the directed set with $a \leq b$ if $b|a$. Then we have the inverse system $(\mathbb{Z}/n\mathbb{Z})_{n\in\mathbb{N}}$ where the morphisms $\varphi_n^m : \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ are defined by $a \mapsto a$. The projective limit of this system is denoted by $\widehat{\mathbb{Z}}$.
3. Given a Galois extension L/F, its Galois group $\mathrm{Gal}(L/F)$ is isomorphic to the projective limit of the inverse system
$$\{\mathrm{Gal}(E/F) \mid E/F \text{ is finite, } E \subset L\}$$
with the restriction morphisms
$$\varphi_E^{E'} : \mathrm{Gal}(E'/F) \to \mathrm{Gal}(E/F), \quad \sigma \mapsto \sigma|_E,$$
for $F \subset E \subset E'$. The isomorphism is given by
$$\mathrm{Gal}(L/F) \to \varprojlim_E \mathrm{Gal}(E/F), \quad \sigma \mapsto (\sigma|_E)_E.$$
If $\overline{\mathbb{F}}_p$ is an algebraic closure of $\mathbb{F}_p$, then $\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p) \cong \widehat{\mathbb{Z}}$.

Let $G = \varprojlim G_i$ be a profinite group. The topology on G is induced by the subspace topology in $\prod G_i$, where G_i's are finite groups with discrete topology. Hence, due to Tychonoff's theorem, G is *compact* topological group. Moreover, it is seen to be *Hausdorff* and *totally disconnected*.

1.2. **Ramification of a Galois representation.** This section deals with Decomposition groups, inertia groups, and Frobenius elements. A good reference is [Neu99]. Let K/F be an extension of number fields. Let $\mathcal{O}_K, \mathcal{O}_F$ be their respective ring of integers (the integral closure of $\mathbb{Z}$ in the extension). Since both are *Dedekind domains*, given a prime ideal $\mathfrak{p}$ of $\mathcal{O}_F$, we have the unique factorization of prime ideals
$$\mathfrak{p}\mathcal{O}_K = \prod_i \mathfrak{P}_i^{e_i},$$
where the product is finite, $\mathfrak{P}_i$ are prime (maximal) ideals in $\mathcal{O}_K$, and $e_i \geq 1$ are positive integers.

Definition 1.5. Let $\mathfrak{p}\mathcal{O}_K = \prod \mathfrak{P}_i^{e_i}$. Then,

(1) the primes $\mathfrak{P}_i$ are said to be the primes in K *lying above* $\mathfrak{p}$, (One also says $\mathfrak{P}_i|\mathfrak{p}$)
(2) a prime $\mathfrak{p}$ of F is said to be *ramified* in the extension K if some $e_i > 1$. Else, we say the prime $\mathfrak{p}$ is *unramified* in K.

Examples. Let $F = \mathbb{Q}$, and $K = \mathbb{Q}(i)$. Therefore, $\mathcal{O}_K = \mathbb{Z}[i]$. We have the following prime ideal factorization.
$$\begin{aligned}(2) &= (1+i)^2,\\ (5) &= (2+i)(2-i),\\ (3) &= (3).\end{aligned}$$
It is seen that only 2 is ramified in $\mathbb{Q}(i)$.

It is known that only *finitely* many primes ramify in a given finite extension of F.

1.2.1. *Frobenius elements.* Let K/F be a finite Galois extension of number fields. The Galois group $\mathrm{Gal}(K/F)$ acts transitively on the set of primes lying above $\mathfrak{p}$, i.e. if $\mathfrak{P}_1, \mathfrak{P}_2$ are primes lying above $\mathfrak{p}$, then there is $\sigma \in \mathrm{Gal}(K/F)$ such that $\sigma\mathfrak{P}_1 = \mathfrak{P}_2$.

Definition 1.6. Let $\mathfrak{P}$ be a prime in $\mathcal{O}_K$, the ring of integers in K, lying above the prime $\mathfrak{p}$ of F. The *decomposition group* of $\mathfrak{P}$ over K is the subgroup $G_{\mathfrak{P}}$ of the Galois group $\mathrm{Gal}(K/F)$ which fixes $\mathfrak{P}$, i.e.
$$G_{\mathfrak{P}} = \{\sigma \in \mathrm{Gal}(K/F) \mid \sigma\mathfrak{P} = \mathfrak{P}\}.$$

Let $\kappa = \mathcal{O}_K/\mathfrak{P}, \mathfrak{f} = \mathcal{O}_F/\mathfrak{p}$ denote the residue fields. Then we have the exact sequence

$$1 \to I_{\mathfrak{P}} \to G_{\mathfrak{P}} \xrightarrow{\tau} \mathrm{Gal}(\kappa/\mathfrak{f}) \to 1,$$

where $I_{\mathfrak{P}} = \ker \tau$ is defined to be the *inertia group* of $\mathfrak{P}$ over K. If $\mathfrak{p}$ is unramified, then we see that $I_{\mathfrak{P}} = 1$ for any prime $\mathfrak{P}$ lying above $\mathfrak{p}$. In this case, the *Frobenius element* $\sigma_{\mathfrak{P}}$ is the element in $G_{\mathfrak{P}}$ which maps to the Frobenius element of $\mathrm{Gal}(\kappa/\mathfrak{f})$ under τ. Given another prime $\mathfrak{P}'$ lying above $\mathfrak{p}$, the elements $\sigma_{\mathfrak{P}}$ and $\sigma_{\mathfrak{P}'}$ are conjugates in $\mathrm{Gal}(K/F)$. We denote this conjugacy class by $\sigma_{\mathfrak{p}}$.

1.2.2. *Ramified places of a Galois representation.* Let F be a number field. For a prime $\mathfrak{p}$ in F, let $\overline{\mathfrak{p}}$ be a prime in $\overline{F}$ lying above $\mathfrak{p}$, i.e. $\overline{\mathfrak{p}} \cap \mathcal{O}_F = \mathfrak{p}$. Define the *decomposition group* $D_{\overline{\mathfrak{p}}}$ of $\overline{\mathfrak{p}}$ over F as,

$$D_{\overline{\mathfrak{p}}} = \varprojlim_{\mathfrak{P}} D_{\mathfrak{P}},$$

where the projective limit is over primes $\mathfrak{P}$ in a finite Galois extension of F, lying above $\mathfrak{p}$. Similarly as before, we have the exact sequence

$$1 \to I_{\overline{\mathfrak{p}}} \to D_{\overline{\mathfrak{p}}} \to \mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q) \to 1,$$

where $q = |\mathfrak{f}|$. The normal subgroup $I_{\overline{\mathfrak{p}}}$ is called as the *inertia group* at a place $\overline{\mathfrak{p}}$ lying above $\mathfrak{p}$. Similarly as before, by changing the prime lying above $\mathfrak{p}$, we get a conjugate subgroup of $D_{\overline{\mathfrak{p}}}$. We denote this conjugacy class by $D_{\mathfrak{p}}$. Let $\sigma_{\mathfrak{p}}$ be the conjugacy class of Frobenius elements, as before, in $D_{\overline{\mathfrak{p}}}$ for a $\overline{\mathfrak{p}}|\mathfrak{p}$.

DEFINITION 1.7. A representation $\rho : G_F \to \mathrm{GL}_n(R)$ is said to be *unramified* at $\mathfrak{p}$ if $\rho(I_{\overline{\mathfrak{p}}}) = 1$, for a place $\overline{\mathfrak{p}}|\mathfrak{p}$. A prime at which ρ isn't unramified is called a *ramified prime*.

Remarks.

1. Note that the above definition doesn't depend on the place $\overline{\mathfrak{p}}$ above $\mathfrak{p}$ as any two inertia groups are conjugates.
2. If ρ is unramified at a place $\mathfrak{p}$, then $\rho(\sigma_{\mathfrak{p}})$ is a well-defined element of $\mathrm{GL}_n(R)$.

EXAMPLE 1.8 (p-ADIC CYCLOTOMIC CHARACTER). Earlier, we saw the $\bmod p^m$-cyclotomic character $\varepsilon_{p,m} : G_{\mathbb{Q}} \to (\mathbb{Z}/p^m\mathbb{Z})^*$. Similarly, we get the p-adic cyclotomic character

$$\varepsilon_p : G_{\mathbb{Q}} \xrightarrow{restriction} \mathrm{Gal}(\mathbb{Q}_{p,\infty}/\mathbb{Q}) \cong \mathbb{Z}_p^*,$$

where $\mathbb{Q}_{p,\infty} = \mathbb{Q}(\cup_m \mu_{p,m})$ is the minimal Galois extension $\mathbb{Q}$ containing all p-power roots of unity. One can prove the following properties of the cyclotomic character ε_p.

1. ε_p is surjective (hence has infinite image).
2. p is the only ramified prime of ε_p.
3. $\varepsilon_p(\sigma_q) = q$ for all $q \neq p$.

PROPOSITION 1.9. *A Galois representation $\rho : G_F \to \mathrm{GL}_n(R)$ with finite image ramifies at only finitely many primes (i.e. the set of ramified primes is finite). Moreover, it factors through $\mathrm{Gal}(K/F)$ for some finite Galois extension K/F.*

Proof. We know that $\ker \rho$ is a closed subgroup of G_F. Hence, by the fundamental theorem of infinite Galois theory, there is a Galois extension K/F such that $\mathrm{Gal}(\overline{F}/K) = \ker \rho$. Therefore, we get an injective map $\rho : \mathrm{Gal}(K/F) \to \mathrm{GL}_n(R)$. Hence, K/F is finite. Moreover, primes at which ρ ramifies are the primes in F which ramify in K, which are finite. □

1.3. **The Artin L-functions.** The study of L-functions is central to number theory. A famous example is the *Riemann zeta function* $\zeta(s)$ defined by

$$\zeta(s) = \sum_{n\geq 1} \frac{1}{n^s} = \prod_p (1-p^{-s})^{-1},$$

for $s \in \mathbb{C}$ with $\mathrm{Re}(s) > 1$. A generalisation of the Riemann zeta function is the *Dedekind zeta function* of a number field F, defined by

$$\zeta_F(s) = \sum_{\mathfrak{a}} \frac{1}{(\mathrm{N}\mathfrak{a})^s} = \prod_{\mathfrak{p}} (1-\mathrm{N}\mathfrak{p}^{-s})^{-1},$$

where $\mathrm{Re}(s) > 1$, and the sum is over all integral ideals $\mathfrak{a}$ of the ring of integers $\mathcal{O}_F$ of F. Here, $\mathrm{N}\mathfrak{a}$ denotes the norm of the ideal $\mathfrak{a}$ in $\mathcal{O}_F$. If $\mathfrak{a} = \prod_{i=1}^r \mathfrak{p}_i^{e_i}$, then

$$\mathrm{N}\mathfrak{a} := \prod_{i=1}^r (\mathrm{N}\mathfrak{p}_i)^{e_i},$$

where $\mathrm{N}\mathfrak{p}_i := [\mathcal{O}_F/\mathfrak{p}_i : \mathbb{F}_p]$.

Given a (mod m) Dirichlet character $\chi : \mathbb{Z} \to \mathbb{C}$, attached to a character $(\mathbb{Z}/n\mathbb{Z})^* \to \mathbb{C}^*$, we have the *Dirichlet L-function* defined by

$$L(s,\chi) := \sum_{n\geq 1} \frac{\chi(n)}{n^s},$$

where s lies in the half plane of convergence. Since χ is completely multiplicative, we have the *Euler product,*

$$L(s,\chi) = \sum_{n\geq 1} \frac{\chi(n)}{n^s} = \prod_{\text{prime } p} (1-\chi(p)/p^s)^{-1},$$

where s lies in the half plane of convergence.

If χ is a non-trivial character $(\mathrm{mod}\ m)$, i.e. its reduction to $(\mathbb{Z}/m\mathbb{Z})^*$ is not the trivial map, then $L(1,\chi)$ converges and is nonzero. This fact is used in proving Dirichlet's theorem for primes in arithmetic progression.

Can we extend the idea of the construction of a Dirichlet L-series to non-abelian representations? Given a representation $\Gamma \to \mathrm{GL}_n(\mathbb{C})$ of a certain group Γ, can we attach an L-series to it? The answer is yes, when Γ is a Galois group over a number field.

DEFINITION 1.10. A Galois representation $G_F \to \mathrm{GL}_n(\mathbb{C})$ is called as an *Artin representation*.

Due to the vast difference between $\mathbb{C}$ and a profinite group G, we have the following result.

PROPOSITION 1.11. *A continuous representation $G \to \mathrm{GL}_n(\mathbb{C})$ of a profinite group G has finite image.*

Proof. To be filled later. □

From Proposition 1.9, any Artin representation is ramified at only finitely many places. Hence, every Artin representation factors through a finite Galois extension.

1.3.1. *Local Euler factors of an Artin representation.* Let F be a number field, and let $\rho : G_F \to \mathrm{GL}_n(\mathbb{C})$ be a Galois representation. Define $V_{\mathfrak{p}}$ to be the subspace of $\mathbb{C}^n$ fixed by (an) inertia group at $\mathfrak{p}$. Note that $V_{\mathfrak{p}}$ doesn't depend on the inertia group chosen. It is easy to see that $V_{\mathfrak{p}} = \mathbb{C}^n$ if and only if ρ is unramified at $\mathfrak{p}$. The local Euler factor of ρ at $\mathfrak{p}$ is defined to be

$$L_{\mathfrak{p}}(s,\rho,F) = \det(I - \mathrm{N}(\mathfrak{p})^{-s}\rho(\sigma_{\mathfrak{q}})|_{V_{\mathfrak{p}}}),$$

where $\sigma_{\mathfrak{p}}$ is the Frobenius element at $\mathfrak{p}$

DEFINITION 1.12 (ARTIN). Let $\rho : G_F \to \mathrm{GL}_n(\mathbb{C})$ be a continuous representation. Define the *Artin L-function* as

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

for $s \in \mathbb{C}$ such that the Euler product converges.

Examples.

1. Let $F = \mathbb{Q}$, and let $\rho : G_F \to \mathrm{GL}_n(\mathbb{C})$ be the trivial homomorphism. Then we have

$$L(s,\rho,F) = \prod_p \det(I_n - p^{-s}I_n)^{-1} = \zeta(s)^n.$$

2. The Artin L-function attached to the $(\bmod\ m)$ cyclotomic character $\varepsilon_m : G_{\mathbb{Q}} \to \mathbb{C}^*$ is equal to the Dirichlet L-function attached to the character

$$(\mathbb{Z}/m\mathbb{Z})^* \xrightarrow{\cong} \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \xrightarrow{\rho} \mathbb{C}^*,$$

where ζ_m is a primitive m-th root of unity.

3. Let $F = \mathbb{Q}$, and let $K = \mathbb{Q}(i) \subset \mathbb{C}$. We have an isomorphism

$$\mathrm{Gal}(K/F) \to \left\{ I_2, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\},$$

which induces a representation $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{C})$. For $p \equiv 1 \bmod 4$, we have $\rho(\sigma_p) = I_2$, and for $p \equiv -1 \bmod 4$, we have $\rho(\sigma_p) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Also, $V_2 = (e_1 + e_2)\mathbb{C}$ implies that $L_2(s,\rho,\mathbb{Q}) = 1 - 2^{-s}$. Therefore, the Artin L-function attached to ρ is

$$L(s,\rho,\mathbb{Q}) = (1-2^{-s}) \prod_{p\equiv 1}(1-p^{-s})^{-2} \prod_{p\equiv -1}(1-p^{-2s})^{-1}.$$

Moreover, we see that $L(s,\rho,\mathbb{Q}) = L(s,\rho_1,\mathbb{Q})L(s,\rho_2,\mathbb{Q})$ where $\rho_1,\rho_2 : G_F \to \mathrm{Gal}(K/F) \to \mathbb{C}^*$ are the two irreducible representations of G_F, and $\rho = \rho_1 \oplus \rho_2$. It is also seen that $L(s,\rho,\mathbb{Q}) = \zeta_K(s)$ and, if ρ_1 is the trivial representation, $L(s,\rho_1,\mathbb{Q}) = \zeta_F(s)$. Hence,

$$\zeta_K(s) = \zeta_F(s)L(s,\rho_2,\mathbb{Q}).$$

Remarks (Properties of Artin L-functions, [Mur01], p. 15).

a) If $\rho_1,\rho_2 : G_F \to \mathrm{GL}_n(\mathbb{C})$ are two Galois representations, then

$$L(s,\rho_1 \oplus \rho_2,F) = L(s,\rho_1,F)L(s,\rho_2,F).$$

In particular, For a finite Galois extension K/F, the Artin L-function of the Galois representation r_K extending the left regular representation on $\mathrm{Gal}(K/F)$ is

$$L(s,r_K,F) = \prod_\rho L(s,\rho,F)^{\dim\rho},$$

where the product is taken over all irreducible representations $\rho : G_F \to \mathrm{GL}_n(\mathbb{C})$ factoring through $\mathrm{Gal}(K/F)$. It can be seen that $L(s,r_K,F) = \zeta_K(s)$ (cf. Remarks b), giving the equation,

$$\zeta_K(s) = \zeta_F(s)\prod_{\rho\neq 1} L(s,\rho,F)^{\dim\rho}.$$

b) Let K/F be a finite Galois extension, H be a subgroup of $G = \mathrm{Gal}(K/F)$. By Galois theory, $H = \mathrm{Gal}(K/K^H)$ where K^H is the fixed field of H. Let $\tau : G_{K^H} \to \mathrm{GL}_n(\mathbb{C})$ be a representation factoring through H. Then, we have

$$L(s,\tau,K^H) = L(s,\mathrm{ind}_H^G\tau,F).$$

CONJECTURE 1.1 (ARTIN). *The L-function attached to a non-trivial irreducible representation* $\mathrm{Gal}(K/F) \to \mathrm{GL}_n(\mathbb{C})$ *admits an analytic continuation to the whole complex plane.*

2. THE CHEBOTAREV DENSITY THEOREM

Using the analytical properties of the Artin L-function (cf. [Mur01, p. 20]) we get the *Chebotarev's density theorem*, a generalisation of the Dirichlet's theorem. Let F be a number field and let $\mathcal{O}_F$ be its ring of integers. By a prime in F, we mean a prime (or maximal) ideal in $\mathcal{O}_F$. For a prime ideal $\mathfrak{p}$, define its norm by

$$\mathrm{N}\mathfrak{p} := |\mathcal{O}_F/\mathfrak{p}|.$$

EXAMPLE 2.1. Let $F = \mathbb{Q}(i)$ be the field of Gaussian numbers. Its ring of integers is $\mathbb{Z}[i]$. For a prime $\mathfrak{p}$ in F, let $p \in \mathbb{Z}$ be the prime lying below it, i.e. $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$. We see that,

$$\mathrm{N}\mathfrak{p} = \begin{cases} p^2 & \text{if } p \equiv 3 \bmod 4, \\ p & \text{otherwise} \end{cases}$$

DEFINITION 2.2. Let A be a subset of primes in F. Let $P_A(x) = \{\mathfrak{p} \in A \mid \mathrm{N}\mathfrak{p} \le x\}$ and let $P_F(x) = \{\mathfrak{p} \mid \mathrm{N}\mathfrak{p} \le x\}$.
1. The *natural density* $d(A)$ of A is defined as

$$d(A) = \lim_{x\to\infty} \frac{|P_A(x)|}{|P_F(x)|} = \frac{|P_A(x)|}{x/\log x}.$$

2. The *Dirichlet density* $\delta(A)$ of A is defined as

$$\delta(A) = \lim_{s\to 1} \frac{\sum_{\mathfrak{p}\in A} 1/\mathrm{N}\mathfrak{p}^s}{\sum_{\mathfrak{p}} 1/\mathrm{N}\mathfrak{p}^s}.$$

By *density* of a set, we usually mean natural density.

Examples.
1. A finite set of primes has density zero.
2. By Dirichlet's theorem, the set of primes of the form $1 + 4k$ has density $1/2$.
3. The set of primes ending with 1 has no natural density.
4. Let $F = \mathbb{Q}(i)$ and $A = \{\mathfrak{p} \mid \mathfrak{p} = p\mathbb{Z}[i],\ p \equiv 3 \bmod 4\}$. For a prime $\mathfrak{p} \in P_A(x)$, we see that $p \le \sqrt{x}$. Hence, we have $|P_A(x)| \le \pi(\sqrt{x})$. Hence,

$$d(A) \le \lim_{x\to\infty} \frac{\pi(\sqrt{x})}{x/\log x} = 0.$$

Therefore, $d(A) = 0$. Moreover, since $\mathrm{N}\mathfrak{p} = p^2$, we see that $\sum_{\mathfrak{p}\in A} 1/\mathrm{N}\mathfrak{p}^s = \sum_{\mathfrak{p}\in A} 1/p^{2s} < \infty$ for $\mathrm{Re}(s) > 1/2$. Therefore, $\delta(A) = 0$.

THEOREM 2.3 (CHEBOTAREV). *Let K/F be a finite Galois extension of number fields, $G = \mathrm{Gal}(K/F)$ be its Galois group, and let C be a conjugacy class of G. Then the density of (unramified) primes $\mathfrak{p}$ of F such that $\sigma_{\mathfrak{p}} = C$ is $|C|/|G|$.*

EXAMPLE 2.4. Taking $K = \mathbb{Q}(\zeta_n)$, the n-th cyclotomic field, and $F = \mathbb{Q}$, we have Dirichlet's theorem for primes in arithmetic progression.

An important consequence of Theorem 2.3 is the following result regarding the Frobenius elements in a Galois extension.

COROLLARY 2.5. *Let K/F be a Galois extension of number field, unramified outside a finite set S of places of F. Then, the set $\{\sigma_{\mathfrak{p}} \mid \mathfrak{p} \notin S\}$ is dense in* $\mathrm{Gal}(K/F)$.

Proof. Let $\sigma \in \mathrm{Gal}(K/F)$, and let $X = \sigma\mathrm{Gal}(K/L)$ be a basic open set around σ. By the classical Chebotarev density theorem for the finite extension L/F, there is a place v, unramified in L, such that the Frobenius element at v in $\mathrm{Gal}(L/F)$ is equal to $\sigma|_L$. Since K/F is unramified outside a finite set S, one can choose $v \notin S$ such that $\sigma_v|_L = \sigma|_L$. □

There is a version of Chebotarev density theorem for infinite Galois extensions unramified outside a finite set of places. For the following, we refer to [Ser98, §I.8 Corollary 2].

PROPOSITION 2.6 (INFINITE CHEBOTAREV DENSITY THEOREM). *Let K/F be an infinite Galois extension unramified outside a finite set of places, $G = \mathrm{Gal}(K/F)$ be its Galois group with a Haar measure μ. Let X be a closed subset of G, stable under conjugation, with its boundary having zero measure. Then, the density of (unramified) primes $\mathfrak{p}$ of F such that $\sigma_\mathfrak{p} \subset C$ is $\mu(X)/\mu(G)$.*

Remarks.

1. For an *algebraic version of Chebotarev density theorem*, we refer to Rajan [Raj98, Theorem 3]. This will be stated later, and used, for getting certain multiplicity one theorems.
2. In the statement of Proposition 2.6, one can consider K/F to be unramfied outside a set of density zero. Hence, even Corollary 2.5 extends to Galois extensions unramified outside a set of density zero.

3. TRACES OF GALOIS REPRESENTATIONS

This section deals with the question: Can traces tell something about the representations? We know from the representation theory of finite groups, two complex representations (semisimple due to Maschke's theorem) of a finite group with equal traces are isomorphic to each other. The following theorem of Brauer–Nesbitt generalises this statement.

THEOREM 3.1 (BRAUER–NESBITT). *Let G be a group, E be a field of characteristic zero, and let ρ_1, ρ_2 be two semisimple representations of G into $\mathrm{GL}_n(E)$. If the traces of $\rho_1(g)$ and $\rho_2(g)$ are equal for all $g \in G$, then ρ_1 is isomorphic to ρ_2.*

By the fact that the Frobenius elements at unramified places are dense in G_F, we have the following corollary.

COROLLARY 3.2. *Let $\rho_1, \rho_2 : G_F \to \mathrm{GL}_n(E)$ be two semisimple Galois representations unramified outside a finite set S, T be a finite set of places of $\mathbb{Q}$, and let $\mathrm{Tr}(\rho_1(\sigma_\mathfrak{p})) = \mathrm{Tr}(\rho_2(\sigma_\mathfrak{p}))$ for all $\mathfrak{p} \notin S \cup T$. Then ρ_1 is isomorphic to ρ_2.*

Proof. Follows by the fact that ρ_1, ρ_2 are continuous, and the fact that $\{\sigma_\mathfrak{p} \mid \mathfrak{p} \notin S \cup T\}$ is dense in G_F. The latter fact follows by the Chebotarev density theorem. □

By Remark 2, one can assume S, T are of density zero in Corollary 3.2.

3.1. Multiplicity one theorems.

The name *multiplicity one theorems* has to do with multiplicity of certain representations appearing in the theory of automorphic forms and representations, but the naive philosophy is: two objects which satisfy a same local property at "many" places are "same" globally. Corollary 3.2 is one such multiplicity one property for Galois representations.

3.1.1. *Elliptic curves.* Let $(E, \mathcal{O})$ be an elliptic curve over $\mathbb{Q}$, i.e. a smooth projective curve of genus 1 defined over $\mathbb{Q}$ with the point $\mathcal{O}$ at infinity. It can be thought of, by the Riemann–Roch theorem, as a projective curve (over $\mathbb{Q}$) in $\mathbb{P}^2_{\mathbb{Q}}$ of the form,

$$y^2 = f(x) = x^3 + ax + b, \quad a, b \in \mathbb{Z},$$

where $f(x)$ has distinct roots and $[0,1,0]$ is the point at infinity. Again due to the Riemann–Roch Theorem (RRT), there is an addition law on E making it an abelian group with $\mathcal{O}$ as its identity.

DEFINITION 3.3 (CF. [Sil09]). An *isogeny* between two elliptic curves $(E, \mathcal{O})$ and $(E', \mathcal{O}')$ is a morphism $E \to E'$ sending $\mathcal{O} \mapsto \mathcal{O}'$. Two elliptic curves E, E' are said to be *isogenous* if there is a non-zero isogeny $E \to E'$. If the isogeny is given by a set of polynomials over an extension K of $\mathbb{Q}$, then it is said to be *defined over* K.

It is seen that an isogeny between two elliptic curves is a homomorphism of groups. Let $E : y^2 = x^3 + ax + b$ be an elliptic curve over $\mathbb{Q}$ with $a, b \in \mathbb{Z}$. For a prime q consider the *reduction mod* q of E, denoted by $\tilde{E}_q$, over the finite field $\mathbb{F}_q$ given by equation

$$y^2 = x^3 + \bar{a}x + \bar{b},$$

where $\overline{x}$ is the image of x under the reduction (mod q) map $\mathbb{Z} \to \mathbb{F}_q$.

DEFINITION 3.4. A prime $q \in \mathbb{Z}$ is said to be a prime of *good reduction* for E if $\tilde{E}_q$ is an elliptic curve over $\mathbb{F}_q$.

It is known that the primes of bad reduction are *finite*. Our main motivation is to answer, in some sense, the following question.

QUESTION 3.5. Given two elliptic curves E and E' over $\mathbb{Q}$, if $|\tilde{E}_q(\mathbb{F}_q)| = |\tilde{E'}_q(\mathbb{F}_q)|$ for almost all q, then what can you say about E and E'?

Let us answer the above question with the help of Galois representations and the Brauer–Nesbitt theorem.

PROPOSITION 3.6 (THEOREM 9.4.1, [DS05]). *Let $E/\mathbb{Q}$ be an elliptic curve. Let $\rho_{E,p} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{Q}_p)$ be the p-adic Galois representation attached to the elliptic curve E induced by the action of $G_{\mathbb{Q}}$ on the $\mathbb{Z}_p$-Tate module $T_p(E) = \varprojlim_m E[p^m]$ of E. Then,*

(a) $\rho_{E,p}$ is an irreducible representation.
(b) If σ_q is the Frobenius at a good (unramified) prime q, then

$$\mathrm{Tr}(\rho_{E,p}(\sigma_q)) = a_q(E) := 1 + q - |\tilde{E}_q(\mathbb{F}_q)| \tag{1}$$

$$\det \rho_{E,p}(\sigma_q) = q. \tag{2}$$

From now on, unless specified, by a p-adic Tate module, we mean the $\mathbb{Q}_p$-vector space $V_p(E) := T_p(E) \otimes \mathbb{Q}_p$ with the action of $G_{\mathbb{Q}}$ via $\rho_{E,p}$.

THEOREM 3.7. *Let E, E' be elliptic curves over $\mathbb{Q}$. The following statements are equivalent:*

(a) E and E' are isogenous.
(b) The p-adic Tate modules of E, E' are isomorphic as Galois representations for all primes p.
(c) $|\tilde{E}_q(\mathbb{F}_q)| = |\tilde{E'}_q(\mathbb{F}_q)|$ for all most all primes q.

Given an isogeny $\varphi : E \to E'$, we have the following restriction map $E[m] \to E'[m]$ for every $m \geq 1$. It is well-defined as φ is a homomorphism. This induces a map on the p-adic Tate modules

$$\varphi_p : T_p(E) \to T_p(E').$$

If φ is defined over $\mathbb{Q}$, then φ_p is an inter-twinning operator between the Tate modules. This gives an injective map $\mathrm{Hom}_{\mathbb{Q}}(E, E') \hookrightarrow \mathrm{Hom}_{G_{\mathbb{Q}}}(T_p(E), T_p(E'))$, where $\mathrm{Hom}_{\mathbb{Q}}(E, E')$ denotes the group of all isogenies defined over $\mathbb{Q}$ and $\mathrm{Hom}_{G_{\mathbb{Q}}}(T_p(E), T_p(E'))$ is the group of $G_{\mathbb{Q}}$ inter-twinning operators of the Tate modules. Moreover, we have the following isogeny theorem due to Faltings, which was conjectured by Tate.

PROPOSITION 3.8 ([Sil09], THEOREM III.7.7). *Let E, E' be elliptic curves over $\mathbb{Q}$, and let p be a prime. The map $\varphi \mapsto \varphi_p$ induces an isomorphism*

$$\mathrm{Hom}_{\mathbb{Q}}(E, E') \otimes \mathbb{Z}_p \cong \mathrm{Hom}_{G_{\mathbb{Q}}}(T_p(E), T_p(E')). \tag{3}$$

COROLLARY 3.9. *Two elliptic curves E, E' over $\mathbb{Q}$ are isogenous if and only if their Tate modules (or the p-adic Galois representations attached to them) are isomorphic.*

Proof. Since $\mathbb{Q}_p$ is a torsion free module over the DVR $\mathbb{Z}_p$, $\mathbb{Q}_p$ is flat over $\mathbb{Z}_p$. Hence,

$$\mathrm{Hom}_{\mathbb{Q}}(E, E') \otimes \mathbb{Q}_p \cong \mathrm{Hom}_{G_{\mathbb{Q}}}(V_p(E), V_p(E')).$$

This implies that, if the Tate modules of E, E' are isomorphic, then $\mathrm{Hom}_{\mathbb{Q}}(E, E') \neq 0$, i.e. E and E' are isogenous.

Let $\varphi : E \to E'$ be a non-zero isogeny. Then, there is the dual isogeny $\widehat{\varphi} : E' \to E$ such that $\varphi \circ \widehat{\varphi} = [\deg \varphi]$. This implies,

$$\det(\varphi_p) \det(\widehat{\varphi}_p) = \det([\deg \varphi]_p).$$

By [Sil09, Proposition III.8.6], φ_p is invertible in $\mathrm{GL}_2(\mathbb{Q}_p)$, and hence is an isomorphism between the Tate modules. □

Proof of Theorem 3.7. From Corollary 3.9, (a) and (b) are equivalent. Moreover, it is immediate that (b) implies (c). Assume (c) holds. Then, except for a finite set of primes of bad reduction of both E and E', we have $\mathrm{Tr}(\rho_E(\sigma_q)) = \mathrm{Tr}(\rho_{E'}(\sigma_q))$. Therefore, by Corollary 3.2, the representations ρ_E and $\rho_{E'}$ are isomorphic. This in turn means that $V_p(E)$ and $V_p(E')$ are isomorphic, and hence E/E' are isogenous. □

Remarks. One can replace $\mathbb{Q}$ by a number field in all the theorems of this subsection. Moreover, due to the strong multiplicity one theorem of Rajan stated below (cf. Theorem 3.10), conjectured by Ramakrishnan [Ram94], we know that, if $|\tilde{E}_q(\mathbb{F}_q)| = |\tilde{E'}_q(\mathbb{F}_q)|$ for a set of primes q with density $> 1 - 1/(2 \cdot 2^2) = 7/8$, then E and E' are isogenous.

THEOREM 3.10 (THEOREM 1, [Raj98]). *Let $\rho, \rho' : G_F \to \mathrm{GL}_n(K)$ be two semisimple p-adic Galois representations, unramified outside a finite set S. If the set*

$$SM(\rho, \rho') := \{\mathfrak{p} \notin S \mid \mathrm{Tr}(\rho(\sigma_{\mathfrak{p}})) = \mathrm{Tr}(\rho'(\sigma_{\mathfrak{p}}))\}$$

has density $> 1 - 1/2n^2$, then ρ and ρ' are isomorphic.

3.1.2. *Modular forms.* In this section, we state the theorem of Deligne regarding Galois representations attached to Hecke eigenforms of weight > 1. By the traces of the attached Galois representations, using Corollary 3.2, we get certain multiplicity one results for modular forms.

Let N and k be natural numbers, $\Gamma_0(N)$ be the set of matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ in $\Gamma = \mathrm{SL}_2(\mathbb{Z})$ such that $N|c$. Let $\mathbb{H} = \{x + iy \in \mathbb{C} \mid y > 0\}$ be the upper half plane and let $\chi : \mathbb{Z} \to \mathbb{C}^*$ be a $\bmod N$ Dirichlet character.

DEFINITION 3.11. A holomorphic function $f : \mathbb{H} \to \mathbb{C}$ is said to be a *modular form of weight k, level N, and of nebentypus χ* if,

(1) the following modularity condition holds

$$f\left(\frac{az+b}{cz+d}\right) = (cz+d)^k \chi(d) f(z), \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N),$$

(2) the function $f(\gamma z)$ is holomorphic (bounded) at $i\infty$ for all $\gamma \in \Gamma$. If $f(\gamma z)$ vanishes at $i\infty$ for every $\gamma \in \Gamma$, then we call f a *cusp form*.

A modular form f as defined above has a Fourier expansion $f(z) = \sum_{m\geq 0} a_f(m)q^m$, where $q = e^{2\pi i z}$ and $z \in \mathbb{H}$. Studying these Fourier coefficients is one of the main aims for number theorists. One usually attaches a Dirichlet series to a modular form and study its analytic properties (analytic continuation and functional equation). We see later that the Fourier coefficients of an eigenform has nice properties. Moreover, the Dirichlet series attached to such an eigenform has a Euler product.

Examples.

1. *Ramanujan Δ function* is the normalized cusp form of weight 12, and level 1. It's Fourier expansion at $i\infty$ is given by
$$\Delta(z) = q\prod(1-q^n)^{24} = \sum_{m\geq 1}\tau(m)q^m.$$
Lehmer's conjecture states that $\tau(m)$ is a non-zero integer for all m.
2. Let $\chi : \mathbb{Z} \to \mathbb{C}^*$ be a $\bmod N$ Dirichlet character, then the function
$$(\Delta \otimes \chi)(z) := \sum_{m\geq 1}\chi(m)\tau(m)q^m,$$
is a modular form of weight 12, level N^2, and with nebentypus χ^2.
3. ([Shi94, Proposition 3.64]) More generally, given a modular form f of weight k, level N, with nebentypus χ, then, for a $\bmod D$ Dirichlet character ε, the function $f \otimes \varepsilon$ is a modular form of weight k, level ND^2, with nebentypus $\chi\varepsilon^2$.

Denote $M(k, N, \chi)$ for the finite dimensional $\mathbb{C}$-space of modular forms of weight k, level N, and nebentypus χ. Let $S(k, N, \chi)$ be the subspace of cusp forms. Let us define the following *Hecke operators* (cf. [Ser81, §7, p. 373], [DS05, Proposition 5.2.2]) T_n's on $M(k, N, \chi)$ as follows: For $f(z) = \sum_{m\geq 0} a_f(m)q^m$,

$$T_n(f) := \sum_{m\geq 0}\left(\sum_{d|(m,n)}\chi(d)a_f\left(\frac{mn}{d^2}\right)\right)q^m.$$

DEFINITION 3.12. A non-zero modular form $f \in M(k, N, \chi)$ is called a (Hecke) eigenform if it is an eigen vector for all the Hecke operators T_n, for $n \geq 1$.

Note the above definition makes sense as the Hecke operators commute with each other. The Ramanujan Δ function is an eigenform, since $M(12, 1, 1)$ is a one-dimensional vector space.

PROPOSITION 3.13 (THE FOURIER COEFFICIENTS OF AN EIGENFORM). *Consider a non-zero Hecke eigenform $f(z) = \sum_{m\geq 0} a_f(m)q^m$ with $a_f(1) = 1$. Then,*

a) $T_n(f) = a_f(n)f$, for all $n \geq 1$.
b) $a_f(m)a_f(n) = \sum_{d|(m,n)}\chi(d)a_f(mn/d^2)$.
c) $a_f(n)$ is an algebraic integer for all $n \geq 1$. Moreover, they lie in a number field. (cf. [RS11, p. 6], [DS74, Proposition 2.7.3]*)*

Let $K_f := \mathbb{Q}(\{a_f(n), \chi(n)\}_{n\geq 1})$ be the number field *associated* to a normalised Hecke eigenform f. Let $\mathcal{O}_f$ be the ring of integers in K_f. For a rational prime p, let $\mathfrak{p}$ be a prime in $\mathcal{O}_f$ lying above it. Let $K_{\mathfrak{p}}$ denote the completion of K_f with respect to the $\mathfrak{p}$-adic topology.

PROPOSITION 3.14 (THÉORÈME 6.1, [DS74]). *Let $f \in M(k, N, \chi)$ be a Hecke eigenform of weight $k \geq 2$. Given a prime p, there is a unique semisimple p-adic Galois representation*

$$\rho_f : G_{\mathbb{Q}} \to \mathrm{GL}_2(K_{\mathfrak{p}}),$$

unramified at primes $q \not| Np$, such that

$$\mathrm{Tr}(\rho_f(\sigma_q)) = a_f(q); \tag{4}$$

$$\det(\rho_f(\sigma_q)) = \chi(q)q^{k-1}. \tag{5}$$

Remarks. The uniqueness is seen by Corollary 3.2: if any other representation has same trace as ρ_f at σ_q, for all most all q, then it is isomorphic to ρ_f. From [Rib77, §3, Corollary 3.1] we see that $K_f = \mathbb{Q}(\{a_f(p)\})$.

PROPOSITION 3.15 (CF. COROLLAIRE 6.3., [DS74]). *Let $f \in M(k, N, \chi)$ and $f' \in M(N', \chi', k')$ be two normalized eigenforms. If $a_f(q) = a_{f'}(q)$ for all primes q in a set of density 1, then $k = k', \chi = \chi'$, and $a_f(q) = a_{f'}(q)$ for all primes $q \not| NN'$.*

Proof. Let $\rho_f, \rho_{f'}$ be the corresponding p-adic Galois representation attached to f, f'. From Proposition 3.14, and Chebotarev density theorem, we have $\rho_f \sim \rho_{f'}$. This implies

$$\chi(q)q^{k-1} = \chi'(q)q^{k'-1},$$

for all prime $q \not| NN'$. As χ, χ' are finite ordered (of order $\phi(N), \phi(N')$ respectively), we have $k = k'$ and $\chi = \chi'$. □

Note that the levels may be different. For example, let $f \in M(k, N, \chi)$, 1_D be the trivial $\mathrm{mod}\ D$ Dirichlet character, and let $g = f \otimes 1_D$ be a modular form in $M(k, ND^2, \chi)$. We have

$$a_g(p) = a_f(p), \quad \text{for all } p \not| D.$$

Hence, the Galois representations ρ_f, ρ_g are isomorphic.

3.1.3. *CM forms.* In this section, we define the notion of a modular form with complex multiplication.

DEFINITION 3.16 (CF. [Rib77], P. 34). For a non-trivial $(\mathrm{mod}\ D)$ Dirichlet character ε, we say a Hecke eigenform $f \in M(k, N, \chi)$ has *complex multiplication by* ε if

$$a_f(p) = \varepsilon(p)a_f(p),$$

for p in a set of primes of density one.

Remarks. The above notion can be defined as follows. A Dirichlet character $\varepsilon : (\mathbb{Z}/D\mathbb{Z})^* \to \mathbb{C}^*$ induces a linear map $M(k, N, \chi) \to M(k, ND^2, \chi\varepsilon^2)$ sending $f \mapsto f \otimes \varepsilon$. If f is a Hecke eigenform with complex multiplication by ε, then $\mathrm{Tr}(\rho_f(\sigma_p)) = \mathrm{Tr}(\rho_{f\otimes\varepsilon}(\sigma_p))$ for primes in density one set. Hence, ρ_f and $\rho_{f\otimes\varepsilon}$ are isomorphic, $a_f(p) = \varepsilon(p)a_f(p)$ for $p \not| N$, and $\varepsilon(p)^2 = 1$ for $p \not| ND$. Let L be the imaginary quadratic field fixed by the kernel of the map

$$\tilde{\varepsilon} : \mathrm{Gal}(\mathbb{Q}(\zeta_{ND^2})/\mathbb{Q}) \to (\mathbb{Z}/ND^2\mathbb{Z})^* \xrightarrow{\varepsilon} \{\pm 1\},$$

where ζ_{ND^2} is a primitive ND^2 root of unity. For a prime p, co-prime to ND^2, we see that $\tilde{\varepsilon}(\sigma_{p,L}) = \varepsilon(p)$, where $\sigma_{p,L}$ is the Frobenius of L at p, as $\tilde{\varepsilon}$ is the composition of ε and the $\mathrm{mod}\ ND^2$ cyclotomic character. Moreover, we see that $\epsilon(p) = -1$ if and only if p is inert in L, i.e. when $\sigma_{p,L} \neq 1$. Hence, $a_f(p) = 0$ for inert primes p.

EXAMPLE 3.17 (A NON-CM EIGENFORM: RAMANUJAN Δ FUNCTION??). We prove that $\Delta(z) = \sum_{n\geq 1} \tau(n)q^n$ is non-CM. Assume it is CM, i.e. there is a non-zero $\mathrm{mod} D$ Dirichlet character ε such that $\tau(p) = \tau(p)\varepsilon(p)$ for all $p \not| D$. We have $\tau(p) = 0$ for all primes p inert in an imaginary quadratic extension L of $\mathbb{Q}$.

3.1.4. *Results of Rajan and Murty–Pujahari.* Rajan's theorem [Raj98, Corollary 1] can be stated as follows:

THEOREM 3.18. *For $i = 1, 2$, let $f_i \in M(k_i, N_i, \chi_i)$ be two eigenforms, at least one non-CM. If the set of all primes p at which $a_{f_1}(p) = a_{f_2}(p)$ has positive upper density, then there is a Dirichlet character ε such that $f_1 = f_2 \otimes \varepsilon$.*

The following is a multiplicity one theorem by Murty–Pujahari.

THEOREM 3.19 ([MP17], THEOREM 1.1). *For $i = 1, 2$, let $f_i \in M(k_i, N_i, \chi_i)$ be two eigenforms, at least one non-CM. if the set of all primes p at which $a_{f_1}(p)/p^{k_1-1} = a_{f_2}(p)/p^{k_2-1}$ has positive upper density, then there is a Dirichlet character ε such that $f_1 = f_2 \otimes \varepsilon$.*

Due to Proposition 3.15, Theorem 3.18 is implied by Theorem 3.19. Patankar and Rajan [PR17] proved Theorem 3.19 using representation theoretic methods via the attached Galois representations to a Hecke eigenform. Note that in the theorems of Rajan, Murty–Pujahari, if f_1, f_2 are of the same level, then they must be same. If $f_1 = f_2 \otimes \varepsilon$ for a $\bmod\ D$ Dirichlet character, then the level N_1 of f_1 is N_2D^2. If $D \neq 1$, there is a natural number d such that $d|D$ but $d \not| N$. We see that

$$\chi_1(d) f_1(z) = f_1|\langle d\rangle(z) = (f_2 \otimes \varepsilon)|\langle d\rangle(z) = 0.$$

This implies $f_1 = 0$. Hence, we have $D = 1$ and $f_1 = f_2$.

REFERENCES

[DS74] Pierre Deligne and Jean-Pierre Serre, *Formes modulaires de poids* 1, Ann. Sci. École Norm. Sup. (4) **7** (1974), 507–530 (1975). MR 379379

[DS05] Fred Diamond and Jerry Shurman, *A first course in modular forms*, Graduate Texts in Mathematics, vol. 228, Springer-Verlag, New York, 2005. MR 2112196

[MP17] M. Ram Murty and Sudhir Pujahari, *Distinguishing Hecke eigenforms*, Proc. Amer. Math. Soc. **145** (2017), no. 5, 1899–1904. MR 3611306

[Mur01] Maruti Ram Murty, *On Artin L-functions*, Class field theory—its centenary and prospect (Tokyo, 1998), Adv. Stud. Pure Math., vol. 30, Math. Soc. Japan, Tokyo, 2001, pp. 13–29. MR 1846449

[Neu99] Jürgen Neukirch, *Algebraic number theory*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 322, Springer-Verlag, Berlin, 1999, Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder. MR 1697859

[PR17] Vijay M. Patankar and C. S. Rajan, *Distinguishing Galois representations by their normalized traces*, J. Number Theory **178** (2017), 118–125. MR 3646830

[Raj98] C. S. Rajan, *On strong multiplicity one for l-adic representations*, Internat. Math. Res. Notices (1998), no. 3, 161–172. MR 1606395

[Ram94] Dinakar Ramakrishnan, *Pure motives and automorphic forms*, Motives (Seattle, WA, 1991), Proc. Sympos. Pure Math., vol. 55, Amer. Math. Soc., Providence, RI, 1994, pp. 411–446. MR 1265561

[Rib77] Kenneth A. Ribet, *Galois representations attached to eigenforms with Nebentypus*, Modular functions of one variable, V (Proc. Second Internat. Conf., Univ. Bonn, Bonn, 1976), 1977, pp. 17–51. Lecture Notes in Math., Vol. 601. MR 0453647

[RS11] Kenneth A. Ribet and William A. Stein, *Lectures on modular forms and hecke operators*, 2011.

[Ser81] Jean-Pierre Serre, *Quelques applications du théorème de densité de Chebotarev*, Inst. Hautes Études Sci. Publ. Math. (1981), no. 54, 323–401. MR 644559

[Ser98] ______, *Abelian ℓ-adic representations and elliptic curves*, Research Notes in Mathematics (A K Peters), Vol 7, Peters, 1998.

[Shi94] Goro Shimura, *Introduction to the arithmetic theory of automorphic functions*, Publications of the Mathematical Society of Japan, vol. 11, Princeton University Press, Princeton, NJ, 1994, Reprint of the 1971 original, Kanô Memorial Lectures, 1. MR 1291394

[Sil09] Joseph H. Silverman, *The arithmetic of elliptic curves*, second ed., Graduate Texts in Mathematics, vol. 106, Springer, Dordrecht, 2009. MR 2514094