1 Introduction to the Langlands Program

1.1 Introduction

1.2 Galois Representations

Definition 1.2.1. For a field K we define the absolute Galois group $G_K = \mathrm{Gal}\left(\overline{K}/K\right)$. Let E be a topological field and $n \in \mathbb{Z}^+$ a positive integer. Then an E-valued n-dimensional Galois representation is a continuous homomorphism,

$$\rho : G_K \to \mathrm{GL}_n(E)$$

1.2.1 Complex Representations

Lemma 1.2.2. There exists a neighborhood V of I in $\mathrm{GL}_n(\mathbb{C})$ that contains no nontrivial subgroup.

Proof. Recall that $M_n(\mathbb{C})$ is a metric space under the absolute value $|A| = \max |A_{ij}|$.
Let $U_r = \{A \in M_n(\mathbb{C}) : |A - I| < r \text{ and } \mathrm{tr}\,(A) = 0\}$ and take $V_r = \exp(U_r)$ an open neighborhood of $I \in \mathrm{GL}_n(\mathbb{C})$ since $\det \exp A = \exp \mathrm{tr}\,(A) = 1$. Suppose that $H \subset V_r$ is a subgroup. For $B \in H$ we have $B = \exp A$ and thus $B^k = (\exp A)^k = \exp(kA)$ so $kA \in U_r$. However, $|kA| = |k| \cdot |A|$ which, by the archimedean property, can be taken arbitrarily large if $|A| > 0$. Since all $A \in U_r$ have $|A| < r$ this contradicts the fact that $kA \in U_r$ unless $|A| = 0 \implies A = 0 \implies B = I$. Thus, $H = \{I\}$. □

Remark. The above proof depends crucially on the archimedean property.

Proposition 1.2.3. Any continuous homomorphism $\rho : G_K \to \mathrm{GL}_n(\mathbb{C})$ factors through $\mathrm{Gal}\,(F/K)$ for some finite Galois extension F/K. Hence its image is finite.

Proof. By Lemma 1.2.2, let V be an neighborhood of I in $\mathrm{GL}_n(\mathbb{C})$ which contains no non-trivial subgroups. Then $U = \rho^{-1}(V)$ is an open neighborhood of $\mathrm{id} \in G_K$ and thus contains a normal subgroup of the form $\mathrm{Gal}\left(\bar{K}/F\right)$ for some galois extension F/K. Since ρ is a homomorphism, the image of $\mathrm{Gal}\left(\bar{K}/F\right)$ is subgroup contained in V. But V does not have any nontrivial subgroup so $\mathrm{Gal}\left(\bar{K}/F\right) \subset \ker \rho$ is actually in the kernel of ρ. Thus, ρ factors through the quotient,

$$\mathrm{Gal}\left(\bar{K}/K\right)/\mathrm{Gal}\left(\bar{K}/F\right) \cong \mathrm{Gal}\,(F/K)$$

which is finite. Hence ρ has finite image. □

1.2.2 ℓ-adic Galois Representations

Remark. The archimedean nature of $\mathbb{C}$ leading to Lemma 1.2.2 made the theory of complex Galois representations fairly uninteresting. However, if we consider a non-archimedean field such as $\mathbb{Q}_\ell$, this restriction is lifted.

Proposition 1.2.4. Every neighborhood of $1 \in \mathbb{Q}_\ell^\times$ contains a nontrivial subgroup.

Proof. Let U be an open neighborhood of $1 \in \mathbb{Q}_\ell^\times$, then there exists $n \in \mathbb{Z}^+$ such that

$$V(n) = 1 + \ell^n \mathbb{Z}_\ell \subset U$$

However, $V(n)$ is a nontrivial subgroup of $\mathbb{Q}_\ell^\times$ because

$$(1+\ell^n z)^{-1} - 1 = \frac{\ell^n z}{1+\ell^n z} = \ell^n \frac{z}{1+\ell^n z} \in \ell^n \mathbb{Z}_\ell$$

since $1+\ell^n z \in \mathbb{Z}_\ell^\times$. □

Definition 1.2.5. Let L/K be finite Galois extension of number fields, $\mathfrak{p} \in \mathcal{O}_K$ be an unramified prime, and $\mathfrak{P}$ a prime of $\mathcal{O}_L$ lying above $\mathfrak{p}$. Then, there is an isomorphism $D(\mathfrak{P}) \xrightarrow{\sim} \mathrm{Gal}\,(\kappa(\mathfrak{P})/\kappa(\mathfrak{p}))$. Let $\mathrm{Frob}_\mathfrak{p} \in D(\mathfrak{P}) \subset \mathrm{Gal}\,(L/K)$ denote the preimage of $\mathrm{Frob} \in \mathrm{Gal}\,(\kappa(\mathfrak{P})/\kappa(\mathfrak{p}))$. In particular,

$$\mathrm{Frob}_\mathfrak{P}(x) \equiv x^{\#\kappa(\mathfrak{p})} \mod \mathfrak{P}$$

for $x \in \mathcal{O}_L$. Since for any two $\mathfrak{P}, \mathfrak{P}'$ over $\mathfrak{p}$ there is $\sigma \in \mathrm{Gal}\,(L/K)$ such that $\sigma(\mathfrak{P}) = \mathfrak{P}'$ then $D(\mathfrak{P}') = \sigma D(\mathfrak{P})\sigma^{-1}$ so $\mathrm{Frob}_{\mathfrak{P}'} = \sigma \mathrm{Frob}_\mathfrak{P} \sigma^{-1}$ giving a well-defined conjugacy class $\mathrm{Frob}_\mathfrak{p}$.

Lemma 1.2.6. Let $F = \mathbb{Q}(\zeta_N)$. Let p be a prime in $\mathbb{Z}$ such that $p \not| N$. Let $\mathfrak{p}$ be a prime in F lying above p. Then $\kappa(\mathfrak{p}) = \mathcal{O}_F/\mathfrak{p} = \mathbb{F}_p[\zeta_N]$. Let $x \in \mathcal{O}_F$, then we can describe the action of Frob_p by

$$\mathrm{Frob}_p\left(\sum_{i=0}^{N-1} a_i \zeta_N^i\right) \equiv \left(\sum_{i=0}^{N-1} a_i \zeta_N^i\right)^p \equiv \sum_{i=0}^{N-1} a_i \zeta_N^{ip} \mod \mathfrak{p}$$

That is to say, the action of Frob_p takes ζ_N to ζ_N^p.

Definition 1.2.7. The ℓ-adic cyclotomic character $\chi_\ell : G_\mathbb{Q} \to \mathbb{Q}_\ell^\times$ of $G_\mathbb{Q}$ is defined by,

$$\sigma \mapsto (m_1, m_2, m_3, \dots) \text{ where } \sigma(\zeta_{\ell^n}) = \zeta_{\ell^n}^{m_n}$$

is a 1-dimensional Galois representation since m_n is defined up to multiples of ℓ^n.

Remark. Notice that when $p \neq \ell$ we have,

$$\chi_\ell(\mathrm{Frob}_p) = p$$

In particular, the image of χ_ℓ is infinite. Therefore, ℓ-adic Galois representations allow for richer structure than those over $\mathbb{C}$.

1.2.3 Uniqueness of Galois Representations

Theorem 1.2.8 (Chebotarev)**.** Let L/K be a finite Galois extension of number fields and $X \subset G = \mathrm{Gal}\,(L/K)$ is a conjugation-stable subset. Then,

$$\delta(\{\mathfrak{p} \subset \mathcal{O}_K \mid \mathfrak{p} \text{ unramified and } \mathrm{Frob}_\mathfrak{p} \subset X\} = \frac{\#X}{\#G}$$

where $\delta(S)$ is the natural density. In particular, $\mathfrak{p} \mapsto \mathrm{Frob}_\mathfrak{p}$ is surjective onto $\mathrm{Gal}\,(L/K)$.

Remark. This of course gives us more. It says that any cofinite set of primes $\mathfrak{p} \subset \mathcal{O}_K$ produce enough $\mathrm{Frob}_\mathfrak{p}$ to cover the Galois group.

Remark. Given a tower $E/L/K$ of finite Galois extensions we see that under $\mathrm{Gal}\,(E/K) \twoheadrightarrow \mathrm{Gal}\,(L/K)$ that $\mathrm{Frob}_{\mathfrak{p},E/K} \mapsto \mathrm{Frob}_{\mathfrak{p},L/K}$ for any unramified prime $\mathfrak{p} \subset \mathcal{O}_K$. Choosing primes $\mathfrak{p}_E$ over $\mathfrak{p}_L$ over $\mathfrak{p}$ this follows from the commutative diagram,

$$\begin{array}{ccc} D(\mathfrak{p}_E) & \xrightarrow{\sim} & \mathrm{Gal}\left(\kappa(\mathfrak{p}_E)/\kappa(\mathfrak{p})\right) \\ \downarrow & & \downarrow \\ D(\mathfrak{p}_L) & \xrightarrow{\sim} & \mathrm{Gal}\left(\kappa(\mathfrak{p}_L)/\kappa(\mathfrak{p})\right) \end{array}$$

Thus, for an infinite Galois extension E/K with $\mathfrak{p}$ unramified there is a well-defined conjugacy class,

$$\mathrm{Frob}_{\mathfrak{p}} \subset \mathrm{Gal}\left(E/K\right) = \varprojlim_{E/L/K} \mathrm{Gal}\left(L/K\right)$$

defined by $\varprojlim_{E/L/K} \mathrm{Frob}_{\mathfrak{p},L/K}$ where L runs over finite Galois intermediate extensions.

Proposition 1.2.9. Let E/K be any Galois extension unramified outside of a finite set S. The map $\mathfrak{p} \mapsto \mathrm{Frob}_{\mathfrak{p}}$ from unramified primes $\mathfrak{p} \subset \mathcal{O}_K$ to conjugacy classes in $\mathrm{Gal}\left(E/K\right)$ has dense (union of its) image.

Proof. By the universal property, a set $S \subset \mathrm{Gal}\left(E/K\right)$ is dense if and only if its image under each $\mathrm{Gal}\left(E/K\right) \to \mathrm{Gal}\left(L/K\right)$ is dense (i.e. equals all of $\mathrm{Gal}\left(L/K\right)$) where L/K is finite Galois and $E \supset L$. Since the set of primes $\mathfrak{p} \subset \mathcal{O}_K$ unramified in E is cofinite, the conjugacy classes $\mathrm{Frob}_{\mathfrak{p}} \mapsto \mathrm{Frob}_{\mathfrak{p},L/K}$ cover $\mathrm{Gal}\left(L/K\right)$ proving that the union of $\mathrm{Frob}_{\mathfrak{p}}$ is dense in $\mathrm{Gal}\left(E/K\right)$. ☐

Theorem 1.2.10 (Brauer-Nesbitt)**.** Let G be a group and E a field. Given a pair of semi-simple representations $\rho_1, \rho_2 : G \to \mathrm{GL}_n(E)$ such that $\forall g \in G$ the characteristic polynomials of $\rho_1(g)$ and $\rho_2(g)$ are equal then $\rho_1 \cong \rho_2$.

Remark. In characteristic zero, it suffices that $\chi_{\rho_1} = \chi_{\rho_2}$ meaning that $\mathrm{tr}\left(\rho_1(g)\right) = \mathrm{tr}\left(\rho_2(g)\right)$ for all $g \in G$ thus we only need to look at the leading (not the monic term) coefficient of the characteristic polynomial. To see this, notice that if λ_i are the (counted with algebraic multiplicity) eigenvalues of $\rho(g)$ then λ_i^n are the eigenvalues of $\rho(g^n) = \rho(g)^n$ so

$$\mathrm{tr}\left(\rho(g^n)\right) = \lambda_1^n + \cdots + \lambda_1^n$$

which (as long as $n!$ is invertible) determine the elementry symmetric polynomials in $\lambda_1, \ldots, \lambda_n$ (i.e. the coefficients of the minimal polynomial) via Newton sums.

Theorem 1.2.11. Let E/K is a (possibly infinite) Galois extension unramified outside of a finite set S. Then a (continuous) semi-simple Galois representation $\rho : \mathrm{Gal}\left(E/K\right) \to \mathrm{GL}_n(F)$ is determined uniquely by the characteristic polynomials,

$$\mathrm{char}(\rho(\mathrm{Frob}_{\mathfrak{p}}))(t) = \det\left[tI - \rho(\mathrm{Frob}_{\mathfrak{p}})\right]$$

for each $\mathfrak{p} \notin S$.

Proof. The map $\mathrm{char}(\rho) : \mathrm{Gal}\left(E/K\right) \to F[x]$ taking $g \mapsto \mathrm{char}(\rho(g))$ is continuous and therefore determined by its values on $\mathrm{Frob}_{\mathfrak{p}}$ (notice that $\mathrm{char}(\rho(\mathrm{Frob}_{\mathfrak{p}}))$ is well-defined because char is invariant under conjugation) since these are mutually dense. Therefore, by Brauer-Nesbitt, there is at most one semi-simple representation up to isomorphism with the proscribed characteristic polynomials. ☐

Remark. The situation for local fields K is even simpler. Any unramified Galois representation

$$\rho : \mathrm{Gal}\left(E/K\right) \to \mathrm{GL}_n(F)$$

(meaning equivalently $\rho(I_{E/K}) = \{I\}$ or ρ factors through some unramified L/K) is determined by $\mathrm{char}(\rho(\mathrm{Frob}_{\mathfrak{p}}))$ because $\mathrm{Gal}\left(K^{\mathrm{ur}}/K\right) = \hat{\mathbb{Z}} \cdot \mathrm{Frob}_{\mathfrak{p}}$ and thus the image of $\mathrm{Frob}_{\mathfrak{p}}$ determines any continuous map $\mathrm{Gal}\left(E/K\right) \to \mathrm{Gal}\left(L/K\right) \to \mathrm{GL}_n(F)$

1.3 The Dimension One Case

Definition 1.3.1. Given a Dirichlet character $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$ there is an associated complex 1-dimensional Galois representation,

$$\rho_\chi : \mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right) \twoheadrightarrow \mathrm{Gal}\left(\mathbb{Q}(\zeta_N)/\mathbb{Q}\right) = (\mathbb{Z}/N\mathbb{Z})^\times \xrightarrow{\chi} \mathrm{GL}_1(\mathbb{C})$$

Proposition 1.3.2. For any complex 1-dimensional Galois representation $\rho : \mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right) \to \mathrm{GL}_1(\mathbb{C})$ there is a Dirichlet character $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$ such that $\rho \cong \rho_\chi$.

Proof. By Proposition 1.2.3 ρ has finite image and thus $\ker \rho$ is an open subgroup which corresponds to some finite extension $K/\mathbb{Q}$ such that passing to the quotient, $\bar{\rho} : \mathrm{Gal}\left(K/\mathbb{Q}\right) \hookrightarrow \mathbb{C}^\times$. Since $\mathbb{C}^\times$ is abelian, $K/\mathbb{Q}$ is abelian and thus by the Kronecker-Weber theorem there is some N such that $K \subset \mathbb{Q}(\zeta_N)$. Since $\mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}(\zeta_N)\right) \subset \ker \rho$ we see that ρ defines a character,

$$\chi : (\mathbb{Z}/N\mathbb{Z})^\times = \mathrm{Gal}\left(\mathbb{Q}(\zeta_N)/\mathbb{Q}\right) \to \mathbb{C}^\times$$

such that the diagram

$$\begin{tikzcd}
\mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right) \arrow[r, two heads] \arrow[rr, bend left, "\rho"] \arrow[dr, two heads] & \mathrm{Gal}\left(K/\mathbb{Q}\right) \arrow[r, hook] & \mathrm{GL}_1(\mathbb{C}) \\
& \mathrm{Gal}\left(\mathbb{Q}(\zeta_N)/\mathbb{Q}\right) \arrow[u, two heads] \arrow[ur, "\chi"] &
\end{tikzcd}$$

commutes proving that $\rho = \rho_\chi$. $\square$

1.3.1 The Artin L-Function

Definition 1.3.3. Let $\rho : \mathrm{Gal}\left(L/K\right) \to \mathrm{Aut}\left(V\right)$ be a representation on a finite dimension F-vectorspace V with L/K finite Galois. Then define,

$$L(\rho, s) = \prod_{\mathfrak{p} \subset \mathcal{O}_K} \frac{1}{\det\left[I - N(\mathfrak{p})^{-s}\rho(\mathrm{Frob}_\mathfrak{p}) | V_{\mathfrak{p},\rho}\right]}$$

where $V_{\mathfrak{p},\rho} = V_{\rho(I_\mathfrak{p})}$ such that $\rho : \mathrm{Gal}\left(L/K\right) \to \mathrm{Aut}\left(V_{\mathfrak{p},\rho}\right)$ factors through an extension unramified at $\mathfrak{p}$ so that $\mathrm{Frob}_\mathfrak{p}$ is well-defined.

Remark. Notice that the local factors,

$$\det\left[I - N(\mathfrak{p})^{-s}\rho(\mathrm{Frob}_\mathfrak{p}) | V_{\mathfrak{p},\rho}\right]^{-1}$$

are a slight modification of the characteristic polynomial evaluated at $t = N(\mathfrak{p})^{-1}$ and thus determine the representation ρ.

Theorem 1.3.4. Let L/K be a Galois extension of degree n. Then,

$$\zeta_L(s) = \prod_{\rho \text{ irrep } \mathrm{Gal}(L/K)} L(\rho, s)^{\deg \rho}$$

Proof. Let e be the ramification index of $\mathfrak{p}$. Then notice that $G_{\mathfrak{p}} = G/I_{\mathfrak{p}}$ acts on $V_{\mathfrak{p},\rho}$ and has order n/e. For the local factor at $\mathfrak{p}$, notice that,

$$-\log\det\left[I - N(\mathfrak{p})^{-s}\rho(\mathrm{Frob}_{\mathfrak{p}})\right] = \sum_{m=1}^{\infty} \frac{\mathrm{tr}\left(\rho(\mathrm{Frob}_{\mathfrak{p}})^m\right)}{m} N(\mathfrak{p})^{-sm}$$

Furthermore, by the character orthogonality relations,

$$\sum_{\rho \text{ irrep}} \deg(\rho)\,\mathrm{tr}\left(\rho(\sigma)\right) = \sum_{\rho \text{ irrep}} \overline{\mathrm{tr}\left(\rho(\mathrm{id})\right)}\,\mathrm{tr}\left(\rho(\sigma)\right) = \begin{cases} n/e & \sigma = \mathrm{id} \\ 0 & \sigma \neq \mathrm{id} \end{cases}$$

Therefore,

$$-\sum_{\rho \text{ irrep}} \deg(\rho)\, \log\det\left[I - N(\mathfrak{p})^{-s}\rho(\mathrm{Frob}_{\mathfrak{p}})\right] = \frac{n}{e}\sum_{m=1}^{\infty} \frac{N(\mathfrak{p})^{-sfm}}{fm} = -g\log\left(1 - N(\mathfrak{p})^{-sf}\right)$$

where f is the order of $\mathrm{Frob}_{\mathfrak{p}}$ and $n = efg$. However, there is an Euler product,

$$\zeta_L(s) = \sum_{I \subset \mathcal{O}_L} \frac{1}{N(I)^{-s}} = \prod_{\mathfrak{P} \subset \mathcal{O}_L} \frac{1}{1 - N(\mathfrak{P})^{-s}} = \prod_{\mathfrak{p} \subset \mathcal{O}_K} \frac{1}{(1 - N(\mathfrak{p})^{-sf})^g}$$

because there are g primes above $\mathfrak{p}$ and each has $N(\mathbb{P}) = N(\mathfrak{p})^f$. Therefore, we see that,

$$\log\zeta_L(s) = -\sum_{\mathfrak{p} \subset \mathcal{O}_K} \log\left(1 - N(\mathfrak{p})^{-sf}\right)^g = -\sum_{\rho \text{ irrep}} \deg\rho\, \log\det\left[I - N(\mathfrak{p})^{-s}\rho(\mathrm{Frob}_{\mathfrak{p}})\right]$$

and thus,

$$\zeta_L(s) = \prod_{\rho \text{ irrep}} L(\rho, s)^{\deg\rho}$$

□

1.4 The Abelian Case

Hello

2 Introduction to Automorphic Forms