ℓ-adic Galois Representations

Benjamin Church

August 1, 2018

Contents

1 Introduction

Considering the importance of Galois groups in number theory and geometry, it is natural to study their representation theory. However, Galois groups have additional structure which makes the theory of their representations remarkably rich. They are profinite topological groups and using topological arguments is extremely fruitful in studying their general representation theory. We will see that the topology is too restrictive to admit interesting Galois representations over $\mathbb{C}$. However, the profinite topology interacts much more favorably with ℓ-adic numbers due to their profinite-like topology. Therefore, we will seek out vector spaces over $\mathbb{Q}_\ell$ on which the Galois group naturally acts. Furthermore, Galois groups act on algebraic fields and preserve certain polynomial equations meaning that Galois groups act naturally on algebraic varieties built from fields and polynomials. This action allows many Galois representations to be viewed as automorphisms of certain geometric objects giving a powerful link between the number theory of field extensions and the geometry of algebraic objects.

Definition: Let G be a profinite group and F a topological field. An n-dimensional representation of G is a continuous homomorphism,

$$\rho : G \to \mathrm{GL}_n(F)$$

If $G = G_K = \mathrm{Gal}(\bar{K}/K)$, the absolute Galois group of K, then we call such a representation a Galois representation and if F is algebraic over $\mathbb{Q}_\ell$ then we call it an ℓ-adic Galois representation.

2 Machinery

2.1 Projective Limits

Definition: A projective system is a family of objects indexed by a poset $(I, \leq)$ with morphisms $f_{ij} : A_j \to A_i$ when $i \leq j$ such that,

1. $f_{ii} = \mathrm{id}_{A_i}$
2. $f_{ik} = f_{ij} \circ f_{jk}$ for all $i \leq j \leq k$
3. $(I, \leq)$ is directed meaning that for every $i, j \in I$ there exists $k \in I$ such that $i \leq k$ and $j \leq k$. This means that for all A_i and A_j there is an object A_k such that there are maps $f_{ik} : A_k \to A_i$ and $f_{jk} : A_k \to A_j$.

we define the projective limit $\varprojlim A_n$ to be the categorical limit of this system. Concretely, for groups or modules, we can give the explicit construction of such an object,

$$\varprojlim A_i = \left\{ (a_i)_I \in \prod_{i \in I} A_i \;\middle|\; \forall i \leq j : f_{ij}(a_j) = a_i \right\}$$

Therefore, the projective limit is the set of sequences which reduce compatibly under the maps f.

A very important special case is that of a leftward mapping sequence where $I = \mathbb{N}$ with the usual order.

Definition: Given a diagram,

$$A_0 \xleftarrow{f_0} A_1 \xleftarrow{f_1} A_2 \xleftarrow{f_2} A_3 \xleftarrow{f_3} \cdots$$

we define the projective limit $\varprojlim A_n$ to be the categorical limit of the diagram. Concretely, for groups or modules, we can give the explicit construction of such an object,

$$\varprojlim A_n = \left\{ (a_n) \in \prod_n A_n \;\middle|\; \forall n \in \mathbb{N} : f_n(a_n) = a_{n-1} \right\}$$

Therefore, the projective limit is the set of sequences which reduce compatibly under the maps f.

Remark. One should view the projective limit as the object which "naturally projects" compatibly with the maps onto each of the given objects. There are clear projection maps $\pi_i : \varprojlim A_n \to A_i$ given by $\pi_i((a_n)) = a_i$. Reversing all the maps, we can define the dual notion called the direct limit which is the objective into which each of the given objects include compatibly via maps $\iota_i : A_i \to \varinjlim A_n$. When the given morphisms are inclusions the direct limit is simply the union.

Example. Let R be a ring. The ring of formal power series on R is

$$R[[X]] \cong \varprojlim R[X]/X^n R[X]$$

with maps $R[X]/X^{n+1}R[X] \to R[X]/X^n R[X]$ given by reduction modulo X^n. The sequences making up the projective limit give the partial sums of a formal power series.

2.2 Infinite Galois Theory

Proposition 2.1. Let F/K be Galois. Then there exists an isomorphism,

$$\mathrm{Gal}(F/K) \cong \varprojlim_{L/K} \mathrm{Gal}(L/K)$$

where L runs over all finite Galois extensions $K \subset L \subset F$. The projective system is given by the restriction maps $\mathrm{Gal}(L/K) \to \mathrm{Gal}(L'/K)$ when $L' \subset L$.

Proof. Given $\sigma \in \mathrm{Gal}(F/K)$ we consider the restriction $\sigma|_L$ to each finite Galois extension L/K which are clearly compatible with restrictions between finite extensions. This gives a map to the projective limit. Since each $\alpha \in F$ is algebraic over K we know that α lies in a finite Galois extension of K so if σ is trivial on all finite Galois extensions then $\sigma(\alpha) = \alpha$ so $\sigma = \mathrm{id}_F$. Thus the map is injective. Furthermore, an element of the projective limit induces an automorphism of F/K by mapping each $\alpha \in F$ to its image under the automorphism acting on any finite Galois extension containing α. Thus the mapping is surjective. $\square$

Remark. The above identification gives a natural profinite topology on $\mathrm{Gal}(F/K)$ by making the projection maps $\mathrm{Gal}(F/K) \to \mathrm{Gal}(L/K)$ continuous for each finite Galois extension L/K. In particular, the kernels of these maps $\mathrm{Gal}(F/L)$ are open subgroups and form a neighborhood basis of id.

Example. The absolute Galois group of $\mathbb{F}_p$ is equal to the profinite completion of $\mathbb{Z}$,

$$\mathrm{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p) \cong \hat{\mathbb{Z}} = \varprojlim \mathbb{Z}/n\mathbb{Z}$$

Theorem 2.2 (Galois Correspondence)**.** Let F/K be a Galois extension with $G = \mathrm{Gal}(F/K)$. There is an inclusion reversing correspondence between *closed* subgroups $H \subset G$ and subfields $K \subset L \subset F$ given by $H \mapsto F^H$ and $L \mapsto \mathrm{Gal}(F/L)$. Furthermore, finite extensions $K \subset L \subset F$ correspond to open subgroups $\mathrm{Gal}(F/L) \subset G$ whose cosets correspond to embeddings of L into F fixing K. Galois extensions $K \subset L \subset F$ correspond to closed normal subgroups.

2.3 ℓ-adic Numbers

Definition: The ℓ-adic integers are the projective limit,

$$\mathbb{Z}_\ell = \varprojlim \mathbb{Z}/\ell^n\mathbb{Z}$$

under the maps $\mathbb{Z}/\ell^{n+1}\mathbb{Z} \to \mathbb{Z}/\ell^n\mathbb{Z}$ given by reduction mod ℓ.

Remark. There is an inclusion $\mathbb{Z} \hookrightarrow \mathbb{Z}_\ell$ given by reducing $a \in \mathbb{Z}$ modulo each ℓ^n. The sequences representing $\mathbb{Z} \subset \mathbb{Z}_\ell$ are exactly those which are eventually constant after the largest power dividing the integer in question. Using the intuition gained from the ring of formal power series, we can write any ℓ-adic integer as a formal "base-ℓ" power series,

$$z = a_0 + a_1\ell + a_2\ell^2 + a_3\ell^3 + \cdots$$

which is the natural extension of how integers may be represented in base ℓ. Although this expression is simply convenient and suggestive shorthand for the projective limit sequence of partial sums,

$$z = (a_0,\ a_0 + a_1\ell,\ a_0 + a_1\ell + a_2\ell^2,\ a_0 + a_1\ell + a_2\ell^2 + a_3\ell^3,\ \cdots)$$

we can actually give meaning to this infinite sum by changing the standard definition of convergence. Define the ℓ-adic valuation $v_\ell : \mathbb{Z}_\ell \to \mathbb{N} \cup \{\infty\}$ by $v_\ell((a_i))$ equals the index of the first nonzero term a_i and $v_\ell(0) = \infty$. All terms in the sequence past $v_\ell((a_i))$ are nonzero because if $a_i = 0$ then $a_{i-1} = f_i(a_i) = 0$. We can then define an absolute value, $|z|_\ell = \ell^{-v_\ell(z)}$ which gives a non-archimedean metric on Z_ℓ. Under this metric, the sequence of elements in $\mathbb{Z} \subset \mathbb{Z}_\ell$ given by these the partial sums actually does converge to the ℓ-adic number,

$$z = a_0 + a_1\ell + a_2\ell^2 + a_3\ell^3 + \cdots$$

because the element,

$$z - z_{N-1} = z - \sum_{i=0}^{N-1} a_i \ell^n = a_N \ell^N + a_{N+1}\ell^{N+1} + a_{N+2}\ell^{N+2} + \cdots$$

has valuation $v_\ell(z_n) \geq N$ because $z_N = (0, \cdots, a_N\ell^N, a_{N+1}\ell^{N+1}, \cdots)$ where the first $N-1$ terms are 0. Therefore,

$$|z - z_n|_\ell \leq \frac{1}{\ell^N} \to 0$$

so the sequence converges $z_n \to z$.

Definition: The ℓ-adic field is the field of fractions of $\mathbb{Z}_\ell$,

$$\mathbb{Q}_\ell = \text{Frac}(\mathbb{Z}_\ell)$$

on which we extend the ℓ-adic valuation to $v_\ell : \mathbb{Q}_\ell \to \mathbb{Z}$ by $v_\ell(a/b) = v_\ell(a) - v_\ell(b)$.

Proposition 2.3. $\mathbb{Z}_\ell^\times = \{z \in \mathbb{Z}_\ell \mid |z|_\ell = 1\}$

Proof. Let $z = (a_i) \in \mathbb{Z}_\ell$. If $v_\ell(z) > 0$ then $a_0 = 0$ so for any $(b_i) \in \mathbb{Z}_\ell$ we have $a_0 b_0 = 0$ so $z \notin \mathbb{Z}_\ell$. However, if $v_\ell(z) = 0$ then choose $b_n = a_n^{-1} \in \mathbb{Z}/\ell^n\mathbb{Z}$ which exists because a_n is coprime to ℓ since it projects down to $a_0 \neq 0$ in $\mathbb{Z}/\ell\mathbb{Z}$. Then we have,

$$(a_i) \cdot (b_i) = (a_i b_i) = (1)$$

so $z \in \mathbb{Z}_\ell^\times$. □

Proposition 2.4. Every element $z \in \mathbb{Q}_\ell$ can be written uniquely as $z = \ell^n u$ where $u \in \mathbb{Z}_\ell^\times$ and $n = v_\ell(z)$.

Proof. First we will prove this for $z = (a_i) \in \mathbb{Z}_\ell$. Take $n = v_\ell(z)$ so we know that $f_{n-1,k}(a_k) = 0$ so $\ell^n \mid a_k$ but ℓ^{n+1} does not. Thus we can write $a_k = \ell^n u_k$ with $u_k \in (\mathbb{Z}/\ell^k\mathbb{Z})^\times$. Take $u = (u_k)$ with $u_k = f_{kn}(u_n) \neq 0$ since $\ell \nmid u_n$ for $k < n$ so clearly $z = \ell^n u$ and $v_\ell(u) = 0$. Furthermore, if $z \in \mathbb{Q}_\ell$ then $z = \frac{a}{b}$ for $a, b \in \mathbb{Z}_\ell$ so we can write $a = \ell^n u$ and $b = \ell^m v$ with $u, v \in \mathbb{Z}^\times$. Thus,

$$z = \frac{\ell^n u}{\ell^m v} = \ell^{n-m} u v^{-1}$$

with $v_\ell(z) = v_\ell(a) - v_\ell(b) = n - m$ an $uv^{-1} \in \mathbb{Z}_\ell^\times$. □

Proposition 2.5.

$$\mathbb{Q}_\ell = \mathbb{Z}_\ell\left[\frac{1}{\ell}\right] = \bigcup_n \frac{1}{\ell^n}\mathbb{Z}_\ell$$

Therefore we may represent an element of $\mathbb{Q}_\ell$ as a power series,

$$a_{-N}\ell^{-N} + a_{-N+1}\ell^{-N+1} + \cdots + a_0 + a_1\ell + a_2\ell^2 + \cdots$$

with only finitely many negative exponent terms.

Proof. By the previous proposition we can write any element $z \in \mathbb{Q}_\ell$ as $\ell^n u$ for $u \in \mathbb{Z}_\ell^\times$ and $n \in \mathbb{Z}$. Therefore, we simply need to invert ℓ to get negative powers of ℓ to represent all of $\mathbb{Q}_\ell$ from $\mathbb{Z}_\ell$. □

Proposition 2.6. $\mathbb{Z}_\ell$ is a local PID (and thus a discrete valuation ring) with unique maximal ideal $\ell\mathbb{Z}_\ell$ and residue field $\mathbb{F}_\ell$.

Proof. Let $I \subset \mathbb{Z}_\ell$ be an ideal. Consider $n = v_\ell(I) = \min\{v_\ell(z) \in \mathbb{N} \mid z \in I\}$ where the minimum value exists by well ordering. Thus, there exists $z_0 \in I$ with $v_\ell(z) = n$. I claim that $I = (\ell)^n$. We can write $z_0 = \ell^n u$ for some $u \in \mathbb{Z}_\ell^\times$. Therefore, $I \subset (z) = (\ell^n u) = (\ell)^n$. Furthermore for any $z \in I$ we have $v_\ell(z) = m \geq n$ so $\ell^n \mid z$ since $z = \ell^m v$ for $v \in \mathbb{Z}_\ell^\times$ so $z = \ell^{m-n} v \ell^n$ with $\ell^{m-n} v \in \mathbb{Z}_\ell$ and thus $z \in (\ell)^n$. Therefore, $I = (\ell)^n$.

Thus, all proper ideals are contained in (ℓ) so $\mathfrak{m} = (\ell)$ is the unique maximal ideal. Consider the map,

$$\phi : \mathbb{Z} \to \mathbb{Z}_\ell/\ell\mathbb{Z}$$

given by inclusion and then projection. Given $z = (a_i) \in \mathbb{Z}_\ell$ take $a \in \mathbb{Z}$ such that $a \equiv a_i \bmod \ell$. Then $v_\ell(z - a) \geq 1$ so $\ell \mid z - a$. Therefore, $[a] = [z]$ in $\mathbb{Z}_\ell/\ell\mathbb{Z}_\ell$ so ϕ is surjective. Furthermore, $\ker\phi = \ell\mathbb{Z}$ since $[a] = 0$ exactly when $a = (0, a, \cdots)$ i.e. $a \equiv 0 \bmod \ell$. Therefore,

$$\mathbb{Z}/\ell\mathbb{Z} \cong \mathbb{Z}_\ell/\ell\mathbb{Z}$$

so the residue field is given by $\mathbb{Z}_\ell/\mathfrak{m} \cong \mathbb{F}_\ell$. □

Proposition 2.7. $\mathbb{Q}_\ell/\mathbb{Z}_\ell \cong \mathbb{Q}/\mathbb{Z}$ and $\mathbb{Z}_\ell/\ell^n\mathbb{Z}_\ell \cong \mathbb{Z}/\ell^n\mathbb{Z}$

Proof. Quotienting by $\ell^n\mathbb{Z}_\ell$ is equivalent to ignoring all elements of the sequence with index greater than or equal to n. Therefore, we can choose a rational number (or integer) which reduces modulo $\ell^n\mathbb{Z}$ to the required value which is consistently reduced my the reduction maps. □

Definition: A complete non-archimedean field K is a topological field which is complete with respect to an absolute value satisfying the non-archimedean property or ultrametric inequality,

$$|\alpha + \beta| \leq \max\{|\alpha|, |\beta|\}$$

For example $\mathbb{Q}_\ell$ with the ℓ-adic absolute value $|\cdot| : \mathbb{Q}_\ell \to \mathbb{Z}$.

Proposition 2.8. Let K be a complete non-archimedean field and L/K a separable extension. The absolute value on K extends uniquely to a non-archimedean absolute value on L. Furthermore, if L/K is finite then L is complete with respect to the extended absolute value.

Lemma 2.9 (Krasner)**.** Let K be a complete non-archimedean field and $\alpha, \beta \in \bar{K}$. If α is strictly closer to β than to any conjugate of α then $K(\alpha) \subset K(\beta)$.

Proof. Consider an automorphism $\sigma \in \mathrm{Gal}(\bar{K}/K)$. By assumption, $|\alpha - \beta| < |\alpha - \sigma(\alpha)|$ whenever $\sigma(\alpha) \neq \alpha$. Suppose that $\sigma(\beta) = \beta$ and consider the value,

$$|\alpha - \sigma(\alpha)| = |\alpha - \beta + \beta - \sigma(\alpha)| \leq \max\{|\alpha - \beta|, |\beta - \sigma(\alpha)|\}$$

We know that $|\beta - \sigma(\alpha)| = |\sigma(\beta - \alpha)| = |\alpha - \beta|$ by uniqueness of the absolute value. Therefore, unless $\sigma(\alpha) = \alpha$,

$$|\alpha - \sigma(\alpha)| \leq |\alpha - \beta| < |\alpha - \sigma(\alpha)|$$

which is a contradiction so $\sigma(\alpha) = \alpha$. Therefore, $\mathrm{Gal}(\bar{K}/K(\beta)) \subset \mathrm{Gal}(\bar{K}/K(\alpha))$ and thus $K(\alpha) \subset K(\beta)$. □

Theorem 2.10. Let $K/\mathbb{Q}_\ell$ be finite. There exists $\alpha \in \overline{\mathbb{Q}}$ such that $K = \mathbb{Q}_\ell(\alpha)$.

Proof. By the primitive element theorem, $K = \mathbb{Q}_\ell(\alpha')$ for some α' algebraic over $\mathbb{Q}_\ell$ with minimal polynomial $f \in \mathbb{Q}_\ell[X]$. Take $g \in \mathbb{Q}[X]$ which is monic of the same degree. Write,

$$g(X) = \prod_{i=0}^{n}(X - \alpha_i)$$

for roots $\alpha_i \in \overline{\mathbb{Q}}$. Consider,

$$|(f - g)(\alpha')|_\ell = |g(\alpha')|_\ell = \prod_{i=0}^{n} |\alpha' - \alpha_i|_\ell$$

by choosing g such that $f - g$ is sufficiently small we can ensure that for any $\epsilon > 0$ there is some root α of g such that $|\alpha' - \alpha| < \epsilon$. In particular, for sufficiently small ϵ the root α will be strictly closer to α' than any conjugate of α'. Therefore, by Krasner's Lemma,

$$\mathbb{Q}_\ell(\alpha') \subset \mathbb{Q}_\ell(\alpha)$$

However because f is irreducible,

$$[\mathbb{Q}_\ell(\alpha) : \mathbb{Q}_\ell] \leq \deg g = \deg f = [\mathbb{Q}_\ell(\alpha') : \mathbb{Q}_\ell] \leq [\mathbb{Q}_\ell(\alpha) : \mathbb{Q}_\ell]$$

forcing an equality. Therefore $\mathbb{Q}_\ell(\alpha) = \mathbb{Q}_\ell(\alpha') = K$ and furthermore g is irreducible in $\mathbb{Q}_\ell[X]$ thus in $\mathbb{Q}[X]$ so,

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg g = [\mathbb{Q}_\ell(\alpha) : \mathbb{Q}_\ell]$$

□

3 Galois Representations over $\mathbb{C}$

Lemma 3.1. There exists a neighborhood V of I in $\mathrm{GL}_n(\mathbb{C})$ 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 3.2. 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 3.1, 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 $\mathrm{Gal}(\bar{K}/F)$ for some galois extension F/K. Since ρ is a homomorphism, the image of $\mathrm{Gal}(\bar{K}/F)$ is subgroup contained in V. But V does not have any nontrivial subgroup so $\mathrm{Gal}(\bar{K}/F) \subset \ker \rho$ is actually in the kernel of ρ. Thus, ρ factors through the quotient,

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

which is finite. Hence ρ has finite image. □

Corollary 3.3. Every 1-dimensional Galois representation of $G_{\mathbb{Q}}$ over $\mathbb{C}$ is a Dirichlet character.

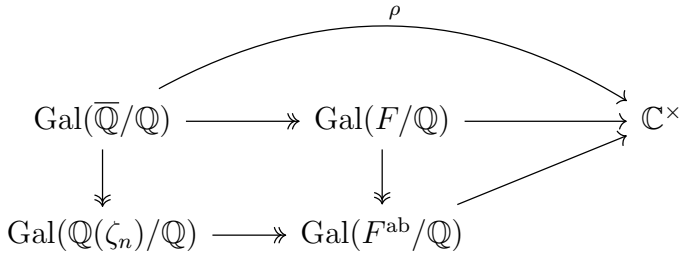
Proof. Any Galois representation $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_1(\mathbb{C}) \cong \mathbb{C}^\times$ factors through the quotient,

$$\rho : \mathrm{Gal}(F/\mathbb{Q}) \to \mathbb{C}^\times$$

where F is a Galois number field. However, $\mathbb{C}^\times$ is abelian so ρ descends to the abelianization. Let $C \triangleleft \mathrm{Gal}(F/\mathbb{Q})$ be the commutator subgroup. By the Galois correspondence, $F^{\mathrm{ab}} = F^C$ is a Galois extension of $\mathbb{Q}$ with Galois group,

$$\mathrm{Gal}(F^{\mathrm{ab}}/\mathbb{Q}) \cong \mathrm{Gal}(F/\mathbb{Q})/C = \mathrm{Gal}(F/\mathbb{Q})^{\mathrm{ab}}$$

By the Kronecker-Weber theorem, every abelian extension of $\mathbb{Q}$ lies inside some cyclotomic field. So $F^{\mathrm{ab}} \subset \mathbb{Q}(\zeta_N)$ giving a restriction map on the Galois groups. This gives a commutative diagram,



Thus ρ factors through a Dirichlet character,

$$\chi : \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$$

□

4 ℓ-adic Galois Representations

The archimedean nature of $\mathbb{C}$ leading to Lemma 3.1 made the theory of complex Galois representations fairly uninteresting. However, if we consider a non-archimedean field like $\mathbb{Q}_\ell$ this restriction is lifted. In fact,

Proposition 4.1. Every neighborhood of 1 in $\mathbb{Q}_\ell^\times$ contains a nontrivial subgroup.

Proof. Let U be an open neighborhood of 1 in $\mathbb{Q}_l^\times$, 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 $1 + \ell^n z \in \mathbb{Z}_\ell^\times$. □

4.1 One-Dimensional Galois Representations

Definition: Let $F/\mathbb{Q}$ be Galois, $p \in \mathbb{Z}$ be a prime, and $\mathfrak{p}$ is a prime in $\mathcal{O}_F$ lying above p. Then $\mathrm{Frob}_\mathfrak{p} \in \mathrm{Gal}(F/\mathbb{Q})$ is defined by

$$\mathrm{Frob}_\mathfrak{p}(x) \equiv x^p \equiv p \bmod$$

for $x \in \mathcal{O}_F$.

Lemma 4.2. Let $F = \mathbb{Q}(\zeta_N)$. Let p be a prime in $\mathbb{Z}$ such that $p \nmid N$. Let $\mathfrak{p}$ be a prime in F lying above p. Then $\mathfrak{f}_\mathfrak{p} = \mathcal{O}_F/\mathfrak{p} = \mathbb{F}_p[\zeta_N]$. Let $x \in \mathcal{O}_F$, then we can describe the action of $\mathrm{Frob}_\mathfrak{p}$ by

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

That is to say, the action of $\mathrm{Frob}_\mathfrak{p}$ takes ζ_N to ζ_N^p.

Definition: 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,

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

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

4.2 Higher-Dimensional Galois Representations

Theorem 4.3. Let G be profinite. Any continuous homomorphism $\rho : G \to \mathrm{GL}_n(\overline{\mathbb{Q}_\ell})$ has image $\rho(G) \subset \mathrm{GL}_n(K)$ where K is a finite extension of $\mathbb{Q}_\ell$.

Proof. By Theorem 2.10, the finite extensions of $\mathbb{Q}_\ell$ are indexed by elements $\alpha \in \overline{\mathbb{Q}}$ and are thus countable. Write,

$$\overline{\mathbb{Q}_\ell} = \bigcup_{i \in I} E_i$$

where E_i are finite extensions of $\mathbb{Q}_\ell$ and I is countable. A topological space X is a *Baire space* if and only if given any countable collection of closed sets F_i in X, each with empty interior in X, their union also empty interior. The image $\rho(G)$ is compact because G is compact and ρ is continuous. Therefore $\rho(G)$ is a complete metric space and thus Baire space by the Baire category theorem.

Let F_i be the closure of $\mathrm{GL}_n(E_i) \cap \rho(G)$ in $\rho(G)$. Then

$$\rho(G) = \bigcup_{i \in I} F_i$$

has nonempty interior in $\rho(G)$. Therefore, there exists $i \in I$ such that F_i contains a non-empty open subset $U \subset \rho(G)$. After translating and shrinking U, we may assume it is an open subgroup of $\rho(G)$. The quotient $\rho(G)/U$ is covered by the sets $\mathrm{GL}_n(E_j) \cap \rho(G)$ for each $E_j \supset E_i$. Since $\rho(G)$ is compact, the cover by open cosets must be finite because there do not exist any proper subcovers. Thus the quotient $\rho(G)/U$ is finite so we need only a finite number of such j. The compositum K of the fields E_j is then a finite extension of $\mathbb{Q}_\ell$. Furthermore, $\rho(G) \subset \mathrm{GL}_n(K)$ because it covers $\rho(G)/U$ and $U \subset \mathrm{GL}_n(K)$ so each coset $gU \subset \mathrm{GL}_n(K)$. □

Corollary 4.4. All ℓ-adic Galois representations $\rho : \mathrm{Gal}(F/K) \to \mathrm{GL}_n(\mathbb{Q}_\ell)$ are of the form,

$$\rho : \mathrm{Gal}(F/K) \to \mathrm{GL}_n(\mathbb{Q}_\ell(\alpha))$$

where $\alpha \in \overline{\mathbb{Q}}$.

5 Galois Representations Attached to Elliptic Curves

Definition: An elliptic curve is a smooth, projective curve of genus one with a distinguished point O. More concretely, an elliptic curve E defined over a field K is a planar algebraic curve given by,

$$\left\{(x, y) \in \bar{K}^2 \mid y^2 = x^3 + ax^2 + bx + c\right\} \cup \{O\} \subset \bar{K}^2$$

for constants $a, b, c \in K$ such that the equation is non-singular. The distinguished point O is viewed as the "point at infinity." For any L/K, the set of L-rational points of E is,

$$E(L) = \left\{(x, y) \in L^2 \mid y^2 = x^3 + ax^2 + bx + c\right\} \cup \{O\} \subset L^2$$

When L/K is algebraic, that is, $K \subset L \subset \bar{K}$, then $E(L) = E \cap L$ which is exactly the set of fixed points of E under the action of $\mathrm{Gal}(\bar{K}/L)$.

Remark. Elliptic curves are, remarkably, abelian varieties meaning there exists a map $+ : E \times E \to E$ expressed by rational functions which gives E the structure of an abelian group with identity O.

Definition: Let E be an elliptic curve defined over K. For $n \in \mathbb{Z}$, define the n-torsion of E, denoted by $E[n]$, to be the kernel of the map $x \mapsto nx$.

Proposition 5.1. Let E be an elliptic curve defined over a number field K (in particular $\mathbb{Q}$) then $E[n] \cong (\mathbb{Z}/n\mathbb{Z}) \oplus (\mathbb{Z}/n\mathbb{Z})$

Proof. I will give a sketch of the proof assuming some knowledge of Weierstrass elliptic functions. Associated to any elliptic curve E over $\mathbb{C}$ is a complex lattice $\Lambda \subset \mathbb{C}$ and a doubly periodic meromorphic function $\wp(z;\Lambda)$ defined on $\mathbb{C}$ which is constant on translates by Λ. Therefore $\wp$ descends to a function of quotient $\mathbb{C}/\Lambda \to \mathbb{C}$. It turns out that, magically, $\wp : \mathbb{C}/\Lambda \to E$ given by $z \mapsto (\wp(z), \wp'(z))$ is an isomorphism of groups. In particular, E is topologically a torus. Let Λ be generated by two complex numbers ω_1, ω_2 called the fundamental periods of the lattice. Then the n-torsion points in $\mathbb{C}/\Lambda$ are exactly the points,

$$z = \frac{a}{n}\omega_1 + \frac{b}{n}\omega_2 \text{ for } a, b \in \mathbb{Z}/n\mathbb{Z}$$

such that $nz = a\omega_1 + b\omega_2 \in \Lambda$ is trivial in $\mathbb{C}/\Lambda$. Therefore, $E[n] \cong (\mathbb{Z}/n\mathbb{Z}) \oplus (\mathbb{Z}/n\mathbb{Z})$ as abstract groups. □

5.1 The Tate Module

Proposition 5.2. Let E be an elliptic curve defined over K then there is a natural action of the absolute Galois group,

$$\mathrm{Gal}(\bar{K}/K) \to \mathrm{Aut}(E)$$

which, because automorphism preserve n-torsion, reduces to an action,

$$\mathrm{Gal}(\bar{K}/K) \to \mathrm{Aut}(E[n]) \cong \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$$

Proof. Let $\sigma \in \mathrm{Gal}(\bar{K}/K)$ act component-wise on E (and fix O). Because σ is a field automorphism fixing K, the action of σ preserves the defining equations of E so it gives a map $E \to E$. Furthermore, since addition in E is given by rational functions with coefficients in K, the action of σ also preserves addition, that is,

$$\sigma(P + Q) = \sigma(P) + \sigma(Q)$$

and thus σ, being inevitable point-wise, is an automorphism of E. Finally, let P_1, P_2 be a $\mathbb{Z}/n\mathbb{Z}$-basis of $E[n]$ as a free $\mathbb{Z}/n\mathbb{Z}$-module. Then there exist unique elements $a, b, c, d \in \mathbb{Z}/n\mathbb{Z}$ such that,

$$\sigma(P_1) = aP_1 + cP_2 \text{ and } \sigma(P_2) = bP_1 + dP_2$$

Then the action of σ on any element $n_1P_1 + n_2P_2$ is given by,

$$\sigma(n_1P_1 + n_2P_2) = n_1\sigma(P_1) + n_2\sigma(P_2) = (an_1 + bn_2)P_1 + (cn_1 + dn_2)P_2 = n_1'P_1 + n_2'P_2$$

Which we may write suggestively as,

$$\begin{pmatrix} n_1' \\ n_2' \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} n_1 \\ n_2 \end{pmatrix}$$

explicitly showing the representation of $\mathrm{Gal}(\bar{K}/K)$ as matrices in $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$. □

Definition: The Tate module of an elliptic curve E is the group,

$$T_\ell(E) = \varprojlim E[\ell^n]$$

under the multiplication by ℓ maps,

$$E[\ell] \longleftarrow E[\ell^2] \longleftarrow E[\ell^3] \longleftarrow \cdots$$

The Tate module $T_\ell(E)$ can be given the structure of a $\mathbb{Z}_\ell$ module via the action, $(a_n) \in \mathbb{Z}_\ell$ acts on $(P_n) \in T_\ell(E)$ via $(a_n) \cdot (P_n) = (a_n \cdot P_n)$. This action is well defined because P_n has ℓ^n torsion so a_n need only be defined up to multiples of ℓ^n.

Theorem 5.3. Let E be an elliptic curve over $K/\mathbb{Q}$. There exists an ℓ-adic Galois representation $V_\ell E = T_\ell(E) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$ with action,

$$\rho_{E,\ell} : \mathrm{Gal}(\bar{K}/K) \to \mathrm{Aut}(V_\ell E) \cong \mathrm{GL}_2(\mathbb{Q}_\ell)$$

called the Galois representation attached to E at ℓ.

Proof. For each $n \in \mathbb{Z}^+$ we have an action of $\sigma \in \mathrm{Gal}(\bar{K}/K)$ on $P \in E[\ell^n]$ componentwise. However, $\ell \cdot \sigma(P) = \sigma(\ell \cdot P)$ because σ is a group homomorphism of E so σ is compatible with the restriction maps. Therefore, σ lifts to $\tilde{\sigma}$ a unique automorphism of the Tate module $T_\ell(E)$. By choosing bases compatible with the multiplication by ℓ maps gives an isomorphism,

$$T_\ell(E) \cong \varprojlim (\mathbb{Z}/\ell^n\mathbb{Z}) \oplus (\mathbb{Z}/\ell^n\mathbb{Z}) \cong \mathbb{Z}_\ell \oplus \mathbb{Z}_\ell$$

The action on the Tate module induces a map,

$$\rho_T : \mathrm{Gal}(\bar{K}/K) \to \mathrm{Aut}(T_\ell(E)) \cong \mathrm{Aut}(\mathbb{Z}_\ell \oplus \mathbb{Z}_\ell) = \mathrm{GL}_2(\mathbb{Z}_\ell) \subset \mathrm{GL}_2(\mathbb{Q}_\ell)$$

The desired map is given by taking the tensor product with the trivial ℓ-adic representation $(\mathbb{Q}_\ell, \rho_0)$,

$$\rho_{E,\ell} = \rho_T \otimes \rho_0 : \mathrm{Gal}(\bar{K}/K) \to \mathrm{Aut}(T_\ell \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell) \cong \mathrm{Aut}(\mathbb{Q}_\ell \otimes \mathbb{Q}_\ell) = \mathrm{GL}_2(\mathbb{Q}_\ell)$$

and we take the $\mathbb{Q}_\ell$ vector space,

$$V_\ell E = T_\ell \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell \cong (\mathbb{Z}_\ell \oplus \mathbb{Z}_\ell) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell = \mathbb{Q}_\ell \oplus \mathbb{Q}_\ell$$

□

Remark. We have seen here an interesting ℓ-adic representation arising naturally from algebraic geometry. It is a truly remarkable fact that a very large class of all ℓ-adic Galois representations arise from geometric objects.

5.2 Complex Multiplication

We have discussed how ℓ-adic representations can give information about the underlying geometry. Galois representations can also be used to determine algebraic properties of Galois groups from geometric structures.

Definition: An elliptic curve E has complex multiplication, is CM for short, if there exists an endomorphism of E which is not a multiplication by n map.

Remark. From the complex analytic viewpoint, such a map is multiplication by $c \in \mathbb{C}$ hence the name. Note, an endomorphism of an elliptic curve is required to be an isogeny i.e. given by rational functions over $\bar{K}$.

Lemma 5.4. Let E be an elliptic defined over K with complex multiplication and denote the exceptional endomorphism by $\phi : E \to E$. There exists a finite extension K^{CM}/K such that $\forall \sigma \in \mathrm{Gal}(\bar{K}/K^{\mathrm{CM}}) : \phi \circ \sigma = \sigma \circ \phi$

Proof. Because ϕ is an isogeny, it is given by rational functions with coefficients in $\bar{K}$. Let $K^{\mathrm{CM}} = K(S)$ where S is the set of coefficients of ϕ. Then for any automorphism $\sigma \in \mathrm{Gal}(\bar{K}/K^{\mathrm{CM}})$ we know that σ preserves the coefficients of ϕ and thus, because σ is a field homomorphism and ϕ is a rational function, $\sigma \circ \phi(P) = \phi \circ \sigma(P)$ for any point $P \in E$. □

Definition: The field $K^{\mathrm{CM}}(E[n])$ is the field extension of K^{CM} generated by the coordinates of all points in $E[n]$. Furthermore define the ℓ^∞-torsion,

$$E[\ell^\infty] = \bigcup_n E[\ell^n]$$

and the field,

$$K^{\mathrm{CM}}(E[\ell^\infty]) = \bigcup_n K^{\mathrm{CM}}(E[\ell^n]) = \varinjlim K^{\mathrm{CM}}(E[\ell^n])$$

Lemma 5.5. For each $n \in \mathbb{Z}^+$ the extension $K^{\mathrm{CM}}(E[\ell^n])/K^{\mathrm{CM}}$ is finite Galois and therefore $K^{\mathrm{CM}}(E[\ell^\infty])/K^{\mathrm{CM}}$ is Galois.

Proof. Take $\sigma \in \mathrm{Gal}(\bar{K}/K^{\mathrm{CM}})$ and consider $\sigma(K^{\mathrm{CM}}(E[\ell^n]))$. Since σ fixes K^{CM} the image of $K^{\mathrm{CM}}(E[\ell^n])$ is entirely determined by where σ maps the generators which are coordinates of $E[\ell^n]$. However, we have shown that σ is an automorphism of E and thus must take ℓ^n-torsion to ℓ^n-torsion. Therefore, for each $P \in E[\ell^n]$ we have $\sigma(P) \in E[\ell^n]$ so σ must map coordinates of $E[\ell^n]$ to coordinates of $E[\ell^n]$. Therefore, $\sigma(K^{\mathrm{CM}}(E[\ell^n])) = K^{\mathrm{CM}}(E[\ell^n])$ proving that $K^{\mathrm{CM}}(E[\ell^n])$ is Galois over K^{CM}. Furthermore, since $E[\ell^n]$ is finite, there are only finitely many possible permutations and thus finitely map automorphisms of $K^{\mathrm{CM}}(E[\ell^n])$ proving the extension is finite. □

Theorem 5.6. Let E be an elliptic curve defined over K with complex multiplication $\phi : E \to E$ such that ϕ restricted to $E[\ell]$ is not the multiplication by n map for any $n \in \mathbb{Z}$. Then the extension $K^{\mathrm{CM}}(E[\ell^\infty])/K^{\mathrm{CM}}$ is abelian.

Proof. Restricting the map given in Theorem 5.3 gives a representation,

$$\rho_{E,\ell}^{\mathrm{CM}} : \mathrm{Gal}(\bar{K}/K^{\mathrm{CM}}) \to \mathrm{Aut}(V_\ell E) \cong \mathrm{GL}_2(\mathbb{Q}_\ell)$$

We have that $\rho_{E,\ell}^{\mathrm{CM}}(\sigma) = I \iff \sigma \cdot (P_n) = (\sigma(P_n)) = (P_n)$ for every $(P_n) \in T_\ell(E)$. Therefore, $\sigma \in \ker \rho_{E,\ell}^{\mathrm{CM}}$ if and only if σ acts trivially on $E[\ell^n]$ for each $n \in \mathbb{Z}^+$ or equivalently, since σ acts coordinate-wise on $E[\ell^n]$, acting trivially on the coordinates of $E[\ell^n]$. However, acting trivially on the generators is equivalent to fixing the field $K^{\mathrm{CM}}(E[\ell^n])$ for all n or, equivalently, fixing the compositum $K^{\mathrm{CM}}(E[\ell^\infty])$. Therefore,

$$\ker \rho_{E,\ell}^{\mathrm{CM}} = \mathrm{Gal}(\bar{K}/K^{\mathrm{CM}}(E[\ell^\infty]))$$

Furthermore, the kernel is closed (because the action is continuous) and normal so the quotient,

$$\mathrm{Gal}(\bar{K}/K^{\mathrm{CM}})/\mathrm{Gal}(\bar{K}/K^{\mathrm{CM}}(E[\ell^\infty])) \cong \mathrm{Gal}(K^{\mathrm{CM}}(E[\ell^\infty])/K^{\mathrm{CM}})$$

corresponds to the Galois extension $K^{\mathrm{CM}}(E[\ell^\infty])/K^{\mathrm{CM}}$. The action then injectivly factors through the quotient as,

$$\begin{array}{ccc} \mathrm{Gal}(\bar{K}/K^{\mathrm{CM}}) & \xrightarrow{\quad\rho_{E,\ell}^{\mathrm{CM}}\quad} & \mathrm{GL}_2(\mathbb{Q}_\ell) \\ & \searrow \quad \nearrow & \\ & \mathrm{Gal}(K^{\mathrm{CM}}(E[\ell^\infty])/K^{\mathrm{CM}}) & \end{array}$$

so the group $\mathrm{Gal}(K^{\mathrm{CM}}(E[\ell^\infty])/K^{\mathrm{CM}})$ is embedded in $\mathrm{GL}_2(\mathbb{Q}_\ell)$. However, $\sigma \circ \phi = \phi \circ \sigma$ for all $\sigma \in \mathrm{Gal}(\bar{K}/K)$ and ϕ is not multiplication by n on $E[\ell]$ so $\phi \in \mathrm{Aut}(V_\ell E) \cong \mathrm{GL}_2(\mathbb{Q}_\ell)$ corresponds to a non-scalar matrix. However, all matrices in $\mathrm{GL}_2(\mathbb{Q}_\ell)$ which commute with a fixed non-scalar matrix (which remains non-scalar in the reduction modulo ℓ) commute with each other (technical exercise). Therefore, the image of $\mathrm{Gal}(K^{\mathrm{CM}}(E[\ell^\infty])/K^{\mathrm{CM}})$ in $\mathrm{GL}_2(\mathbb{Q}_\ell)$ is abelian so by the embedding $\mathrm{Gal}(K^{\mathrm{CM}}(E[\ell^\infty])/K^{\mathrm{CM}})$ is abelian itself. □

Example. Consider the elliptic curve over $\mathbb{Q}$ defined by,

$$E : y^2 = x^3 + x$$

which has an exceptional automorphism $\phi : E \to E$ given by,

$$\phi(x, y) = (-x, iy)$$

which preserves the defining equation and the group law. Clearly, $K^{\mathrm{CM}} = \mathbb{Q}(i)$ since i is the only non-rational coefficient defining ϕ. One can easily check that ϕ is not multiplication by n on any torsion subgroup. Therefore, the extensions

$$\mathbb{Q}(i)(E[\ell^\infty])/\mathbb{Q}(i)$$

given by adjoining ℓ^n-torsion points of E are abelian for each ℓ.

Remark. This is an example of Kronecker's Jugendtraum or "Dream of Youth" which was to generate all abelian extensions of a number field K by adjoining special values of certain interesting functions. For example, the Kronecker-Weber theorem does this for $K = \mathbb{Q}$ saying that the abelian extensions of $\mathbb{Q}$ are exactly the subfields of $\mathbb{Q}(f(\frac{1}{n}))$ where $f(x) = e^{2\pi ix}$ is a very special analytic function. It turns out that, astonishingly, our above construction generated *all* the abelian extensions of $\mathbb{Q}(i)$. That is the compositum over all primes ℓ of $\mathbb{Q}(i)(E[\ell^\infty])$ gives the maximal abelian extension of $\mathbb{Q}(i)$. Equivalently, every finite abelian extension of $\mathbb{Q}(i)$ is contained in $\mathbb{Q}(i)$ adjoined some finite set of torsion points on the curve E. The theory of elliptic curves using Galois representations has now realized Kronecker's dream for all imaginary quadratic fields. However, the general case remains a mystery.