Student Learning Seminar on Galois Deformations.

Rafah Hajjar, September 17, 2023

These notes are based on Gouvea's book *Deformations of Galois Representations* and Mazur's paper *An Introduction to the Deformation Theory of Galois Representations.*

1 Introduction and review of Galois Representations

To understand the role of Galois deformations in Number Theory, we first need to become familiar with the basic objects in this theory: Galois representations. This is nothing more than the representation theory of Galois groups. Therefore, the first thing we should ask is what we already know about these groups. In the following section, we describe their structure as far as it is known and state some of their properties.

1.1 Structure of Galois groups

Let F/K be a normal and separable extension of fields (not necessarily finite). The Galois group $\mathrm{Gal}(F/K)$ has a natural topology given by

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

where the $K' \subset F$ run through the finite normal extensions of K, making it a profinite group.

Theorem 1.1. *There is a correspondence between subextensions of F/K and closed subgroups of $\mathrm{Gal}(F/K)$. It is given by*

$$K' \mapsto \mathrm{Gal}(F/K'), \quad H \mapsto F^H$$

In the special case in which $F = \overline{K}$ is an algebraic closure of K, we call $\mathrm{Gal}(\overline{K}/K)$ the absolute Galois group of K and denote it G_K. For this section let's also assume $K = \mathbb{Q}$

The group $G_{\mathbb{Q}}$ is not very well understood in general (let alone G_K). One of the most useful tools for its study is its "local structure". For each place p there is a canonical inclusion $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$. However, there are many different inclusions $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$ (equivalent to the different extensions of the p-adic valuation on $\mathbb{Q}$ to $\overline{\mathbb{Q}}$). Choosing one, we get an inclusion $G_{\mathbb{Q}_p} \hookrightarrow G_{\mathbb{Q}}$, and changing the choice of embedding changes this by conjugation. We call the image of $G_{\mathbb{Q}_p}$ inside $G_{\mathbb{Q}}$ the *decomposition group at* p (well-defined up to conjugation).

We understand the groups $G_{\mathbb{Q}_p}$ much better. There is a surjective map

$$\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p) \to \mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p) \cong \widehat{\mathbb{Z}}$$

given by restriction to $\mathbb{Q}_p^{\mathrm{ur}}$ and the fact $\mathrm{Gal}(\mathbb{Q}_p^{\mathrm{ur}}/\mathbb{Q}_p) \cong \mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$. The kernel of this map is called the *inertia group at* p and denoted I_p. In turn, the inertia group has a normal Sylow pro-p-subgroup W_p (*wild inertia*), and the quotient (*tame inertia*) satisfies

$$I_p/W_p \cong \prod_{\ell \neq p} \mathbb{Z}_\ell$$

Remark 1. A Galois extension $K/\mathbb{Q}$ is unramified iff the composite

$$I_p \hookrightarrow G_{\mathbb{Q}_p} \hookrightarrow G_{\mathbb{Q}} \to \mathrm{Gal}(K/\mathbb{Q})$$

is trivial. Same with tamely ramified and W_p.

This whole picture is determined only up to conjugation, hence the best way to study these groups is via their representations.

1.1.1 Restricting the ramification

Another way to simplify the study of the absolute Galois group is by restricting the ramifications. Fix S a finite set of primes including all the archimedean ones. Consider the maximal extension $\mathbb{Q}_S$ unramified outside S. We want to study the group

$$G_{\mathbb{Q},S} = \mathrm{Gal}(\mathbb{Q}_S/\mathbb{Q}),$$

which is a quotient of $G_{\mathbb{Q}}$, but much easier to understand. Still, there are many things we don't know about these groups, for example, whether they are topologically finitely generated (it is conjectured by Shafarevich that they are). However, we know they satisfy a weaker condition, that will turn out to be enough for our purposes.

Definition 1.1. We say that a profinite group G satisfy the *p-finiteness condition* if for any open subgroup $H \subset G$, there are finitely many continuous homomorphisms from H to $\mathbb{Z}/p\mathbb{Z}$

Proposition 1.1. The group $G_{K,S}$ satisfies the p-finiteness condition.

Since a nontrivial element of $\mathrm{Hom}_{\mathrm{cont}}(G_{K,S}, \mathbb{Z}/p\mathbb{Z})$ corresponds to an extension of degree d unramified outside S, this is a consequence of the following well-known result

Theorem 1.2 (Hermite-Minkowski)**.** Let K be a number field, S a finite set of primes, and d a positive integer. There are finitely many extensions F/K of degree d unramified outside S.

Regarding the local structure of $G_{K,S}$, we have the following stronger result

Theorem 1.3. If K is a finite extension of $\mathbb{Q}_p$, then G_K is topologically finitely generated.

Therefore we are interested in studying

- The group $G_{K,S}$
- The conjugacy classes of the homomorphisms $G_{K_v} \to G_{K,S}$

1.2 Galois representations

Why are we interested in Galois representations? There are two main reasons:

1. They arise naturally from very well-known objects such as elliptic curves and modular forms (to be discussed in more detail later)

2. The local picture described earlier is only defined up to conjugation. In this case, group representations come in particularly handy. As an example, even though the Frobenius elements φ_p are only defined up to conjugation, their image under a representation has some useful well-defined properties, such as the trace, the determinant, or in general its characteristic polynomial.

Definition 1.2. A *Galois representation* defined over A, unramified outside S, is a continuous homomorphism

$$\rho : G_{K,S} \to \mathrm{GL}_n(A),$$

where A is a topological ring and $n \in \mathbb{Z}^+$. We say two representations ρ_1, ρ_2 are *equivalent* if $P\rho_1 P^{-1} = \rho_2$ for some $P \in \mathrm{GL}_n(A)$.

An equivalent definition of a Galois representation is a free A-module of rank n with a continuous action of $G_{K,S}$ and a choice of basis (changing the basis gives an equivalent representation), with the obvious correspondence. We will use both notions interchangeably.

The standard choices for the ring A are the following

1. $A = \mathbb{C}$. These are known as *Artin representations* and are the most classical. In this case, the image of $G_{K,S}$ must be finite, so they factor through a finite quotient.

2. A is a finite field. These arise naturally from elliptic curves and modular forms. Serre's famous conjecture asserts that every Galois representation of this kind is modular.

3. $A = \mathbb{Z}_p$ or $\mathbb{Q}_p$ or a finite extension. They also arise from elliptic curves and modular forms. This case gives the best match in topologies since $\mathbb{Z}_p$ also carries a profinite topology.

We are mainly interested in the last two cases. We want to understand all the finitely ramified representations into $\mathrm{GL}_n(A)$. For $n = 1$ this is essentially done by Class Field Theory, in fact

Theorem 1.4 (Kronecker-Weber)**.** There are isomorphisms

$$G_{\mathbb{Q}}^{\mathrm{ab}} \cong \prod_p \mathbb{Z}_p^\times \cong \widehat{\mathbb{Z}}^\times, \quad G_{\mathbb{Q},S}^{\mathrm{ab}} \cong \prod_{p \in S} \mathbb{Z}_p^\times$$

Therefore we will care about the case $n > 1$, and mostly about the case $n = 2$, since the representations that arise from elliptic curves and modular forms are of this kind.

Our goal is to understand the whole "package" of $G_{K,S}$ together with its local structure $G_{K_v} \to G_{K,S}$ via these representations

$$\rho : G_{K,S} \to \mathrm{GL}_n(A).$$

Note that, since the groups G_{K_v} are topologically generated by a choice of Frobenius φ_v, the restriction of ρ to G_{K_v} is given by simply giving the conjugacy class of the image of the Frobenius under ρ. As we mentioned earlier, the trace $a_v := \mathrm{tr}_A(\rho(\varphi_v))$ is independent of the choice of Frobenius. Also, in many instances, the data

$$v \mapsto a_v \in A, \quad v \notin S$$

will be enough to reconstruct ρ up to equivalence (by Chebotarev, it suffices to have this data for a set of places of density 1).

1.3 Coefficient rings

In general, we will consider the ring A to be a coefficient ring

Definition 1.3. A *coefficient ring* is a complete noetherian local ring A with finite residue field k, of characteristic p.

Such a ring carries a profinite topology, a basis of opens being given by powers of the maximal ideal,

$$A = \varprojlim_{\nu \to \infty} A/\mathfrak{m}_A^\nu$$

Analogously, the group $\mathrm{GL}_n(A)$ carries the corresponding profinite topology

$$\mathrm{GL}_n(A) = \varprojlim_{\nu \to \infty} \mathrm{GL}_n(A/\mathfrak{m}_A^\nu)$$

Definition 1.4. A coefficient ring homomorphism is a map $f : A' \to A$ such that $f^{-1}(\mathfrak{m}_A) = \mathfrak{m}_{A'}$ and the induced homomorphism on residue fields is an isomorphism.

There is a natural ring homomorphism $\mathbb{Z}_p \to A$, but this is only a coefficient ring homomorphism if $k = \mathbb{F}_p$. Instead, one takes the ring of Witt vectors $W(k)$, which is the absolutely unramified extension of $\mathbb{Z}_p$ with residue field k. Now any coefficient ring A with residue field k is naturally endowed with a coefficient ring homomorphism $W(k) \to A$ that makes A into a topological $W(k)$-algebra

1.4 Sources of Galois representations

1.4.1 Elliptic curves

Given an elliptic curve E defined over a number field K, consider the group of n-torsion points $E[n]$, which is the group of rational points over $\overline{K}$ which lie in the kernel of the homomorphism $x \mapsto nx$.

The group G_K acts naturally as a group of automorphisms of $E(\overline{K})$, and hence induces an action of G_K on $E[n]$. Since $E[n]$ is abstractly the product of two cyclic groups of order n, this action gives a homomorphism

$$G_K \to \mathrm{Aut}(E[n]) \cong \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}).$$

Passing to the projective limit of these representations as n ranges over the natural numbers, or as n ranges over all powers of a fixed prime p, we get representations

$$\rho_E : G_K \to \mathrm{GL}_2(\widehat{Z})$$
$$\rho_{E,p^\infty} : G_K \to \mathrm{GL}_2(\mathbb{Z}_p)$$

A similar construction on a general abelian variety of dimension g gives a Galois representation of degree $2g$.