Introduction to Galois Representations

Zachary Gardner

July 2, 2021

These notes are a shameless ripoff of some notes by Samuel Marks. Go read those notes if you want some actually good exposition. Any errors are my own.

1 Introduction

The aim of these notes is to introduce Galois representations. We let $G_{\mathbb{Q}}$ denote the absolute Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, for $\overline{\mathbb{Q}}$ a fixed algebraic closure. Our first and most important definition is the following.

Definition 1. *A **Galois representation** is a continuous group homomorphism $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_n(F)$ for F a topological vector space.*[1] *The representation is **ℓ-adic** if F is an extension of $\mathbb{Q}_\ell$ (typically a finite extension or $\overline{\mathbb{Q}_\ell}$).*

Remark 2. *There is a corresponding notion of Galois representation of $G_K := \mathrm{Gal}(K^{\mathrm{sep}}/K)$ for any field K. If no K is specified then we always take $K = \mathbb{Q}$.*

Before we say anything about Galois representations, we should first talk more about $G_{\mathbb{Q}}$ itself.

2 Galois Theory

Fittingly, one of the most fundamental results in Galois theory is the following.

Theorem 3 (Fundamental Theorem of Galois Theory)**.** *Let L/K be a finite Galois extension. Then, there is an inclusion-reversing bijection*

$$\{\textit{subgroups } H \leq \mathrm{Gal}(L/K)\} \longleftrightarrow \{\textit{subextensions } L/M/K\}$$

given by $H \mapsto L^H$ and $M \mapsto \mathrm{Aut}(L/M)$. This bijection preserves degree and restricts to a bijection between normal subgroups of $\mathrm{Gal}(L/K)$ and Galois subextensions of L/K (in the sense that M/K is Galois).

If L/K is an infinite Galois extension[2] then the above result no longer holds true. The fix comes from considering the topology on $\mathrm{Gal}(L/K)$. Working over $\mathbb{Q}$, consider the collection of finite

[1] We equip $\mathrm{GL}_n(F)$ with the subspace topology coming from the product topology on $M_n(F) \cong F^{n^2}$.

[2] In general, a Galois extension L/K is defined to be algebraic, separable, and normal. Equivalently, L/K is algebraic and $L^{\mathrm{Aut}(L/K)} = K$.

Galois extensions $K/\mathbb{Q}$ (contained inside $\overline{\mathbb{Q}}$), partially ordered with respect to inclusion. This gives rise to an inverse system of groups $\mathrm{Gal}(K/\mathbb{Q})$ with restriction maps

$$\mathrm{Gal}(L/\mathbb{Q}) \twoheadrightarrow \mathrm{Gal}(K/\mathbb{Q}), \qquad \sigma \mapsto \sigma|_K$$

for $K \subseteq L$.[3] We obtain an inverse limit

$$\varprojlim_K \mathrm{Gal}(K/\mathbb{Q}) = \left\{ (\sigma_K) \in \prod_K \mathrm{Gal}(K/\mathbb{Q}) : \sigma_L|_K = \sigma_K \text{ for every } L \supseteq K \right\}.$$

Theorem 4. *Let L/K be a Galois extension. Then, the natural map*

$$\mathrm{Gal}(L/K) \to \varprojlim_M \mathrm{Gal}(M/K), \qquad \sigma \mapsto \sigma|_M$$

with RHS ranging over finite Galois subextensions $L/M/K$ is a group isomorphism. In particular, taking $L = \overline{\mathbb{Q}}$ and $K = \mathbb{Q}$ gives a description of $G_{\mathbb{Q}}$ as an inverse limit of finite groups.

The group $\varprojlim_M \mathrm{Gal}(M/K)$ can be equipped with a topology by endowing each $\mathrm{Gal}(M/K)$ with the discrete topology (which is the only choice since this is a finite group) and endowing $\varprojlim_M \mathrm{Gal}(M/K)$ with the subspace topology coming from the induced product topology. Using the above isomorphism, this gives a topology on $\mathrm{Gal}(L/K)$ called the **Krull topology**.[4]

Proposition 5. *Let L/K be a Galois extension.*

(a) $\mathrm{Gal}(L/K)$ *is a topological group – i.e., the multiplication and inversion maps on* $\mathrm{Gal}(L/K)$ *are continuous.*

(b) *Let $L/M/K$ be a Galois subextension. Then, the restriction map* $\mathrm{Gal}(L/K) \twoheadrightarrow \mathrm{Gal}(M/K)$ *is continuous with kernel* $\mathrm{Gal}(L/M)$. *Hence, there is a short exact sequence of topological groups*

$$1 \longrightarrow \mathrm{Gal}(L/M) \longrightarrow \mathrm{Gal}(L/K) \longrightarrow \mathrm{Gal}(M/K) \longrightarrow 1$$

(c) *Let $L/M/K$ be a finite Galois subextension. Then,* $\mathrm{Gal}(L/M)$ *is a normal clopen subgroup of* $\mathrm{Gal}(L/K)$.

(d) *The collection* $\{\mathrm{Gal}(L/M) : M/K \textit{ finite Galois}\}$ *is a basis of open sets at* id_L *in* $\mathrm{Gal}(L/K)$.

The fact that $\mathrm{Gal}(L/K)$ is a topological group implies that multiplication by any fixed element is a homeomorphism of $\mathrm{Gal}(L/K)$ and that any open subgroup is automatically closed. The above result allows us to modify the statement of the Fundamental Theorem of Galois Theory so that it holds for infinite Galois extensions. The key is that closed normal subgroups correspond to Galois extensions and open subgroups correspond to finite extensions, so open normal subgroups correspond to finite Galois extensions.

[3] This is well-defined since $K/\mathbb{Q}$ is Galois and so $\sigma(K) \subseteq K$ for every $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$.

[4] In fact, $\mathrm{Gal}(L/K)$ is a typical example of a profinite group, which are topological groups that are always compact (by Tychonoff's theorem) and totally disconnected (in the sense that they have no nontrivial connected subsets).

3 Cyclotomic Characters

Given $n \geq 1$, let $\mu_n := \{\zeta \in \overline{\mathbb{Q}}^\times : \zeta^n = 1\}$ denote the set of nth roots of unity in $\overline{\mathbb{Q}}$. Then, the extension $\mathbb{Q}(\mu_n)/\mathbb{Q}$ is Galois with

$$(\mathbb{Z}/n\mathbb{Z})^\times \xrightarrow{\sim} \mathrm{Gal}(\mathbb{Q}(\mu_n)/\mathbb{Q}), \qquad a \mapsto (\zeta \mapsto \zeta^a)$$

where ζ is any element of μ_n (check that this is well-defined). Then, the union $\mu_{\ell^\infty} := \bigcup_{n\geq 1} \mu_{\ell^n}$ satisfies

$$\mathrm{Gal}(\mathbb{Q}(\mu_{\ell^\infty})/\mathbb{Q}) \cong \varprojlim_{n\geq 1} \mathrm{Gal}(\mathbb{Q}(\mu_{\ell^n})/\mathbb{Q}) \cong \varprojlim_{n\geq 1} (\mathbb{Z}/\ell^n\mathbb{Z})^\times \cong \mathbb{Z}_\ell^\times,$$

where you should think through carefully where each isomorphism comes from. We define the **ℓ-adic cyclotomic character** χ_ℓ to be the composition

$$G_\mathbb{Q} \twoheadrightarrow \mathrm{Gal}(\mathbb{Q}(\mu_{\ell^\infty})/\mathbb{Q}) \xrightarrow{\sim} \mathbb{Z}_\ell^\times \hookrightarrow \mathbb{Q}_\ell^\times = \mathrm{GL}_1(\mathbb{Q}_\ell).$$

Let's now cast this example in a slightly different light. We have an inverse system

$$\mu_\ell \xleftarrow{(\cdot)^\ell} \mu_{\ell^2} \xleftarrow{(\cdot)^\ell} \mu_{\ell^3} \xleftarrow{(\cdot)^\ell} \cdots$$

giving rise to $M := \varprojlim_{n\geq 1} \mu_{\ell^n}$. There is a natural action of $\mathbb{Z}_\ell$ on M given by

$$a \cdot \zeta = \zeta^a := (\zeta_n^{a_n})$$

for $a = (a_n) \in \mathbb{Z}_\ell$ and $\zeta = (\zeta_n) \in M$ (check that this is well-defined). This makes M into a free $\mathbb{Z}_\ell$-module of rank 1. There is a natural (continuous) action of $G_\mathbb{Q}$ on M, which one can check satisfies

$$\sigma \cdot \zeta = \zeta^\sigma = \zeta^{\chi_\ell(\sigma)}$$

for $\sigma \in G_\mathbb{Q}$ and $\zeta \in M$ thinking of χ_ℓ with values in $\mathbb{Z}_\ell$. This Galois action is also compatible with the $\mathbb{Z}_\ell$-module structure on M, which is equivalent to the identity $(\zeta^a)^\sigma = (\zeta^\sigma)^a$. Now tensor with $\mathbb{Q}_\ell$ to get a Galois representation of $G_\mathbb{Q}$. This is typically denoted $\mathbb{Q}_\ell(1)$ and called a **Tate twist**.

4 Complex Representations

So far we've been looking at ℓ-adic Galois representations, so what about complex Galois representations? Since the topologies on $\mathbb{Q}_\ell$ and $\mathbb{C}$ are quite different it is perhaps not surprising that both kinds of representations should have different flavors. A good illustration of this is the following result.

Proposition 6. *Let $\rho : G_\mathbb{Q} \to \mathrm{GL}_n(\mathbb{C})$ be a complex Galois representation. Then, there exists a finite Galois extension $K/\mathbb{Q}$ such that there is a factorization*

$$\begin{tikzcd}
G_\mathbb{Q} \arrow[r, "\rho"] \arrow[d, two heads] & \mathrm{GL}_n(\mathbb{C}) \\
\mathrm{Gal}(K/\mathbb{Q}) \arrow[ur, dotted, "\exists!"'] &
\end{tikzcd}$$

Hence, studying *individual* complex Galois representations boils down to the representation theory of finite groups. Note, however, that the K in the proposition depends on ρ and so it is natural to take our domain to be $G_{\mathbb{Q}}$ when considering *families* of complex Galois representations (as one wants to do when studying things like the Langlands program).

Proof. The key is that $G_{\mathbb{Q}}$ has arbitrarily small subgroups while $\mathrm{GL}_n(\mathbb{C})$ does not, in the sense that there is an open neighborhood $U \subseteq \mathrm{GL}_n(\mathbb{C})$ of the identity containing no nontrivial subgroups. The set $\rho^{-1}(U)$ is an open neighborhood of $\mathrm{id}_{\overline{\mathbb{Q}}}$ in $G_{\mathbb{Q}}$ and so contains an open normal subgroup of the form $\mathrm{Gal}(\overline{\mathbb{Q}}/K)$ for some finite Galois $K/\mathbb{Q}$. Then, $\rho(\mathrm{Gal}(\overline{\mathbb{Q}}/K))$ is a subgroup of $\mathrm{GL}_n(\mathbb{C})$ contained in U hence must be trivial. The result follows since $G_{\mathbb{Q}}/\mathrm{Gal}(\overline{\mathbb{Q}}/K) \cong \mathrm{Gal}(K/\mathbb{Q})$. □

5 Ramification

Given a Galois representation $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_n(F)$, when can we "lift" $\mathrm{Fr}_p \in G_{\mathbb{F}_p}$ and make sense of $\rho(\mathrm{Fr}_p)$?[5] Intuitively, we can do this when ρ has "good local behavior" at p, something which ultimately boils down to ramification. While we're at it, we may as well as examine Galois representations $\rho : G_K \to \mathrm{GL}_n(F)$ for K any number field.

Recall from last time the setup of decomposition and inertia groups. Given L/K a finite Galois extension of number fields, consider $\mathfrak{q}$ a prime of L lying above a prime $\mathfrak{p}$ of K. Then, there is a decomposition group

$$D_{\mathfrak{q}} := \mathrm{Stab}_{\mathrm{Gal}(L/K)}(\mathfrak{q}) = \{\sigma \in \mathrm{Gal}(L/K) : \sigma(\mathfrak{q}) = \mathfrak{q}\}$$

and inertia group

$$I_{\mathfrak{q}} := \ker(D_{\mathfrak{q}} \twoheadrightarrow \mathrm{Gal}(k_{\mathfrak{q}}/k_{\mathfrak{p}}))$$

for residue fields $k_{\mathfrak{q}} := \mathcal{O}_L/\mathfrak{q}$ and $k_{\mathfrak{p}} := \mathcal{O}_K/\mathfrak{p}$. The group $\mathrm{Gal}(k_{\mathfrak{q}}/k_{\mathfrak{p}})$ is finite cyclic generated by Frobenius $\mathrm{Fr}_{\mathfrak{p}}$, characterized by $\mathrm{Fr}_{\mathfrak{p}} = (\cdot)^{N\mathfrak{p}}$ for $N\mathfrak{p} := |k_{\mathfrak{p}}|$.[6] If $I_{\mathfrak{q}} = 0$ (i.e., if L/K is unramified at $\mathfrak{q}$) then $D_{\mathfrak{q}} \cong \mathrm{Gal}(k_{\mathfrak{q}}/k_{\mathfrak{p}})$ and so $\mathrm{Fr}_{\mathfrak{p}}$ certainly makes sense as an element of $D_{\mathfrak{q}} \subseteq \mathrm{Gal}(L/K)$. This is a bit overkill though, since if we have a representation $\rho : \mathrm{Gal}(L/K) \to \mathrm{GL}_n(F)$ then our argument shows that all we need to define $\rho(\mathrm{Fr}_{\mathfrak{p}})$ is that $I_{\mathfrak{q}} \subseteq \ker \rho$.

If $F = \mathbb{C}$ then the above is enough to make sense of $\rho(\mathrm{Fr}_{\mathfrak{p}})$ (thinking of $\mathrm{Fr}_{\mathfrak{p}}$ as an element of $G_{k_{\mathfrak{p}}}$) by the factorization result we proved earlier. The only caveat is that we have to choose a prime $\mathfrak{q}$ of L lying above $\mathfrak{p}$, which presents little difficulty since different choices of lift yield conjugate decomposition groups. However, we want our theory to work for more general F. In order to do this we need to make sense of an *absolute* inertia group $I_{\mathfrak{p}} \leq G_K$ that does not depend on choosing some finite extension of K. Assuming we have such a group, we can make the following definition.

Definition 7. *A Galois representation $\rho : G_K \to \mathrm{GL}_n(F)$ is **unramified** at a prime $\mathfrak{p}$ of K if $I_{\mathfrak{p}} \subseteq \ker \rho$. Equivalently, we can make sense of $\rho(\mathrm{Fr}_{\mathfrak{p}})$.*

The only caveat (which does not affect the above definition), as we will soon see, is that we will only be able to define $I_{\mathfrak{p}}$ up to conjugacy. One way to define the absolute inertia group is to port the above theory over to the setting of local fields. As discussed last time there is an isomorphism of short exact sequences

[5] Recall that the Frobenius Fr_p is defined by $\mathrm{Fr}_p(x) = x^p$ for every $x \in \overline{\mathbb{F}_p}$.

[6] This Frobenius evidently lifts to an element of $G_{k_{\mathfrak{p}}}$.

$$\begin{tikzcd}
1 \arrow[r] & I_{\mathfrak{q}} \arrow[r] \arrow[d, "\cong"] & D_{\mathfrak{q}} \arrow[r] \arrow[d, "\cong"] & \mathrm{Gal}(k_{\mathfrak{q}}/k_{\mathfrak{p}}) \arrow[r] \arrow[d, "\cong"] & 1 \\
1 \arrow[r] & I_{L_{\mathfrak{q}}/K_{\mathfrak{p}}} \arrow[r] & \mathrm{Gal}(L_{\mathfrak{q}}/K_{\mathfrak{p}}) \arrow[r] & \mathrm{Gal}(k_{L_{\mathfrak{q}}}/k_{K_{\mathfrak{p}}}) \arrow[r] & 1
\end{tikzcd}$$

Hence, lifting Frobenius can be interpreted in terms of local inertia groups. By passing to an inverse limit with respect to all finite Galois extensions of $K_{\mathfrak{p}}$, we obtain $I_{K_{\mathfrak{p}}}$ fitting into a short exact sequence

$$1 \longrightarrow I_{K_{\mathfrak{p}}} \longrightarrow G_{K_{\mathfrak{p}}} \longrightarrow G_{k_{K_{\mathfrak{p}}}} \longrightarrow 1$$

of *topological* groups (meaning that the maps in the above sequence are continuous). The key now is that the composite embedding $K \hookrightarrow K_{\mathfrak{p}} \hookrightarrow \overline{K_{\mathfrak{p}}}$ induces an embedding $\overline{K} \hookrightarrow \overline{K_{\mathfrak{p}}}$ unique up to conjugacy by G_K. Hence, we can define

$$I_{\mathfrak{p}} := \mathrm{im}(I_{K_{\mathfrak{p}}} \hookrightarrow G_{K_{\mathfrak{p}}} \hookrightarrow G_K),$$

once again unique up to conjugacy by G_K.

Example 8. *We claim that the ℓ-adic cyclotomic character $\chi_\ell : G_{\mathbb{Q}} \to \mathbb{Q}_\ell^\times$ is unramified at every prime $p \neq \ell$. Indeed, χ_ℓ factors through the map*

$$G_{\mathbb{Q}} \twoheadrightarrow \mathrm{Gal}(\mathbb{Q}(\mu_{\ell^\infty})/\mathbb{Q}) \cong \varprojlim_{n \geq 1} \mathrm{Gal}(\mathbb{Q}(\mu_{\ell^n})/\mathbb{Q})$$

and each extension $\mathbb{Q}(\mu_{\ell^n})/\mathbb{Q}$ is unramified at p (since its discriminant is, up to sign, a power of ℓ). In fact, one can check that $\chi_\ell(\mathrm{Fr}_p) = p$.