Galois representations

Samuel Marks

Let K be a number field with fixed algebraic closure $\overline{K}$. A Galois representation is nothing more than a continuous representation of $G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on a finite-dimensional vector space V. In most of the cases we consider, V will be a vector space over $\mathbb{Q}_\ell$ the field of ℓ-adic numbers for a prime number ℓ.

The Galois representations we see will be *unramified* at all but finitely many primes p; this means that we can make sense of the action of the *Frobenius endomorphism* $\sigma_p = (x \mapsto x^p) \in G_{\mathbb{F}_p} = \mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$ on V. For example, this is the case for the representation

$$G_{\mathbb{Q}} \twoheadrightarrow \mathrm{Gal}(K/\mathbb{Q}) \to \mathrm{GL}_n(\mathbb{Q})$$

where $K/\mathbb{Q}$ is a degree n extension unramified at p, and the first arrow is the natural restriction to K.

An important object associated to a Galois representation ρ is its L-function $L(s, \rho)$, which is a holomorphic function defined on some half-plane of $\mathbb{C}$ defined via an Euler product over the primes. An important example is the *Riemann zeta function*, which is associated to the trivial representation of $G_{\mathbb{Q}}$. In the best cases, these L-functions have good analytic properties, such as a meromorphic continuation to $\mathbb{C}$ and a functional equation.

1 The absolute Galois group of $\mathbb{Q}$

Recall that a *Galois extension* L/K of fields is an algebraic extension such that the subfield of L fixed by all automorphisms of

$$\mathrm{Aut}(L/K) = \{\text{field automorphisms } \sigma \text{ of } L : \sigma|_K = \mathrm{id}\}$$

is exactly K. In this case, we write $\mathrm{Gal}(L/K)$ for this automorphism group. If L/K is finite, then

$$\#\,\mathrm{Aut}(L/K) \leq [L : K]$$

with equality if and only if L/K is Galois. If $H \leq G$ is a subgroup of automorphisms, then we denote by L^H the subfield of L fixed by all $\sigma \in H$.

The algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$ is Galois over $\mathbb{Q}$. We define the *absolute Galois group* of $\mathbb{Q}$ to be $G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Similarly, $\overline{\mathbb{F}}_p$ is Galois over $\mathbb{F}_p$, and we write $G_{\mathbb{F}_p} = \mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$ to denote the absolute Galois group of $\mathbb{F}_p$.[1]

We recall here the fundamental theorem of Galois theory for finite extensions.

Theorem 1.1 (Fundamental theorem of Galois theory for finite extensions)**.** *Let L/K be a finite Galois extension with Galois group $G = \mathrm{Gal}(L/K)$. Then there is an inclusion-reversing, degree-preserving bijection*

[1] $\mathbb{Q}$ and $\mathbb{F}_p$ are both *perfect fields*, meaning that their algebraic closures are the same as their seperable closures. For an arbitrary field K, we have that the seperable closure K^{sep} is Galois over K and we write $G_K = \mathrm{Gal}(K^{sep}/K)$ for the absolute Galois group.

$$\{\textit{subgroups } H \leq G\} \longleftrightarrow \{\textit{subextensions } L/M/K\}$$

$$H \longmapsto L^H$$

$$\mathrm{Aut}(L/M) \longmapsfrom M$$

which furthermore restricts to a bijection

$$\{\textit{normal subgroups } H \leq G\} \longleftrightarrow \{\textit{Galois subextensions } L/M/K\}.$$

If L/K is not finite, then theorem 1.1 no longer holds. However, it can be easily repaired. It ends up that $\mathrm{Gal}(L/K)$ has a natural topology (which is discrete in the case $[L:K] < \infty$), and that theorem 1.1 holds if we replace "subgroup" with "closed subgroup" everywhere.

To discuss the topology on $\mathrm{Gal}(L/K)$ we will first need a digression on *inverse limits*.

1.1 Inverse limits

Given a suitable "compatible system" of objects, the inverse limit of this system is an object that packages together the data of the system. Inverse limits can be defined in great generality, though we'll try to stay down-to-Earth here.

Definition 1.2.

(1) Let I be a set with a partial order $\leq$. An *inverse system* (also called a projective system) indexed by I is a collection of sets (or groups or rings or topological spaces) $\{A_i\}_{i\in I}$ together with maps (of sets, groups, rings, or topological spaces)

$$\varphi_{ij} : A_i \to A_j \qquad \text{for all } j \leq i$$

such that $\varphi_{ii} = \mathrm{id}_{A_i}$ for all $i \in I$ and $\varphi_{jk} \circ \varphi_{ij} = \varphi_{ik}$ for all $k \leq j \leq i$. The φ_{ij} are called *transition maps*.

(2) The *inverse limit* of the system $(\{A_i\}, \{\varphi_{ij}\})$ is the set/group/ring/topological space

$$\varprojlim_i A_i = \left\{ (a_i)_{i\in I} \in \prod_{i\in I} A_i : \varphi_{ij}(a_i) = a_j \text{ for all } j \leq i \right\}$$

of compatible systems of elements of the inverse system. In the case of topological spaces, we put the subspace topology on $\varprojlim A_i$.

Exercise 1.3.

(1) If $(\{A_i\}, \{\varphi_{ij}\})$ is an inverse system of groups, check that $\varprojlim_i A_i$ is a group. Do the same for an inverse system of rings.

(2) If $(\{A_i\}, \{\varphi_{ij}\})$ is an inverse system of Hausdorff topological spaces, check that the conditions $\varphi_{ij}(a_i) = a_j$ all define closed subsets of $\prod A_i$. Conclude that $\varprojlim A_i$ is a closed subset of $\prod A_i$.

Exercise 1.4. Let I be a partially ordered set. We call a subset $I' \subseteq I$ *cofinal* if any $i \in I$ is bounded by some $i' \in I'$, i.e. for some $i' \in I'$ we have $i \leq i'$. Show that if $I' \subseteq I$ is cofinal then the inverse systems $(\{A_i\}_{i\in I}, \{\varphi_{ij}\}_{j\leq i\in I})$ and $(\{A_i\}_{i\in I'}, \{\varphi_{ij}\}_{j\leq i\in I'})$ have isomorphic inverse limits.

If the above definition seems scary, then try reading the following key examples and then rereading the definition.

Example 1.5.

(1) Let p be prime and consider the inverse system of rings

$$A_i = \mathbb{Z}/p^i\mathbb{Z} \qquad \text{for } i \in \mathbb{N} = \{1, 2, 3, \dots\}$$

with transition maps

$$\mathbb{Z}/p^i\mathbb{Z} \overset{\bmod p^j}{\twoheadrightarrow} \mathbb{Z}/p^j\mathbb{Z}$$

for all $j \leq i$. Then $\varprojlim \mathbb{Z}/p^i\mathbb{Z}$ consists of systems $a = (a_i \mod p^i)$ such that $a_i \mod p^j = a_j$ whenever $j \leq i$. Intuitively, an element $a \in \varprojlim \mathbb{Z}/p^i\mathbb{Z}$ is a "number" which can be taken mod p^i for any $i \geq 1$, subject to the obvious compatibilities. But this is the same intuition one has for the p-adic integers $\mathbb{Z}_p$! Indeed, we have the following.

Exercise 1.6. The map

$$\begin{aligned} \mathbb{Z}_p &\longrightarrow \varprojlim_i \mathbb{Z}/p^i\mathbb{Z} \\ a &\mapsto (a \mod p^i)_{i\in\mathbb{N}} \end{aligned}$$

is an isomorphism of rings *and* a homeomorphism of topological spaces.

(2) Similarly, we can consider the inverse system $R[x]/(x^i)$ for a ring R and $i \in \mathbb{N}$, with the natural transition maps $R[x]/(x^i) \twoheadrightarrow R[x]/(x^j)$ for $j \leq i$. Then again, $\varprojlim R[x]/(x^i)$ consists of "polynomials" which can be taken mod x^i for any i; formally this is a sequence $(f_i \mod (x^i))$ such that $f_i \mod (x^j) = f_j$ whenever $j \leq i$. In this case we have and isomorphism

$$\begin{aligned} R[\![x]\!] &\xrightarrow{\sim} \varprojlim R[x]/(x^i) \\ f(x) &\mapsto (f(x) \mod x^i)_{i\in\mathbb{N}}. \end{aligned}$$

Do you see why it is said that "p-adic numbers are like power series in p"?

(3) This example defines the topology of $G_{\mathbb{Q}}$. Consider the inverse system of $\mathrm{Gal}(K/\mathbb{Q})$ of finite Galois extensions $K/\mathbb{Q}$ (that is, the index set is $I = \{\text{finite Galois extensions } K/\mathbb{Q}\}$ ordered by $K \leq L \iff K \subseteq L$). The transition maps are given by restriction:

$$\begin{aligned} \mathrm{Gal}(L/\mathbb{Q}) &\twoheadrightarrow \mathrm{Gal}(K/\mathbb{Q}) \\ \sigma &\mapsto \sigma|_K \end{aligned}$$

for $K \subseteq L$ (these restriction maps are well defined because $K/\mathbb{Q}$ is Galois; this guarantees that $\sigma(K) \subset K$ for any $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$). Then

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

consists of "automorphisms" which compatibly restrict to any finite Galois $K/\mathbb{Q}$. This should give an intuition for the following theorem.

Theorem 1.7. *Let L/K be a Galois extension with Galois group $\mathrm{Gal}(L/K)$. Then there is a group isomorphism*

$$\begin{aligned} \mathrm{Gal}(L/K) &\xrightarrow{\sim} \varprojlim_M \mathrm{Gal}(M/K) \\ \sigma &\mapsto \sigma|_M \end{aligned}$$

for the inverse system $\{\mathrm{Gal}(M/K)\}$ over finite Galois subextensions M/K, with transition maps given by restriction. In particular, we have

$$G_{\mathbb{Q}} \cong \varprojlim_{\substack{M/\mathbb{Q} \\ \textit{finite Galois}}} \mathrm{Gal}(M/\mathbb{Q}).$$

Proof. Let θ denote the map of the theorem. It is clear that θ is well-defined and has image in $\varprojlim_M \mathrm{Gal}(M/K) \subset \prod_M \mathrm{Gal}(M/K)$. It suffices to show that θ is a bijection.

Injectivity is easy: if $1 \neq \sigma \in \mathrm{Gal}(L/K)$ then $\sigma(x) \neq x$ for some $x \in L$. But x must lie in some finite subextension M/K, and thus $\sigma|_M \neq 1$, giving $\theta(\sigma) \neq 1$.

For surjectivity, let $(\sigma_M)_M \in \varprojlim \mathrm{Gal}(M/K)$. We define $\sigma \in \mathrm{Gal}(L/K)$ via

$$\sigma(x) = \sigma_M(x) \quad \text{for some finite Galois } M \text{ containing } x.$$

Some such M always exists because

$$L = \bigcup_{\substack{L/M/K \\ M/K \text{finite Galois}}} M.$$

To see σ is well-defined, note that if M and M' are both finite Galois extensions containing x then $x \in M \cap M'$ and

$$\sigma_M(x) = \sigma_{M\cap M'}(x) = \sigma_{M'}(x)$$

because $\sigma_M|_{M\cap M'} = \sigma_{M\cap M'} = \sigma_{M'}|_{M\cap M'}$. By a similar argument, σ is an automorphism of L fixing K because it is so when restricted to any finite Galois subfield. But clearly $\theta(\sigma) = (\sigma_M)_M$, so that θ is surjective. □

Exercise 1.8. Show that $\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p) \cong \hat{\mathbb{Z}}$ where

$$\hat{\mathbb{Z}} = \prod_p \mathbb{Z}_p$$

and the product is taken over the prime numbers p.

1.2 The topology of infinite Galois groups

Keeping with the notation of theorem 1.7, each of the finite Galois groups $\mathrm{Gal}(M/K)$ can be viewed as topological spaces with the discrete topology. This defines a topology on $\varprojlim_M \mathrm{Gal}(M/K) \cong \mathrm{Gal}(L/K)$, but it is *not* the discrete topology! It is called the *profinite topology* (since it arises from a limit of finite groups) or the *Krull topology*. The following proposition collects some basic facts about this topology.

Proposition 1.9. *Let L/K be a Galois extension.*

(1) $\mathrm{Gal}(L/K)$ *is compact.*

(2) For all Galois subextensions $L/M/K$*, the restriction map* $\mathrm{Gal}(L/K) \to \mathrm{Gal}(M/K)$ *is surjective and continuous with kernel* $\mathrm{Gal}(L/M)$*.*

(3) For all finite Galois subextensions $L/M/K$*, the subgroup* $\mathrm{Gal}(L/M)$ *is normal, open, and closed.*

Proof. For (1), note that $\prod_M \mathrm{Gal}(M/K)$ is a product of compact groups (finite groups are always compact), and hence compact by Tychonoff's Theorem. Closed subsets of compact spaces are compact, giving (1).

Denote the restriction map of part (2) by θ. The proof of surjectivity is identical to the corresponding statement for *finite* extensions L/K, so we omit it.[2] However, we note that this critically uses that L/K is Galois. By definition, $\ker\theta = \mathrm{Gal}(L/M)$. For continuity, note that we have a commutative diagram

$$\begin{array}{ccc} \prod\limits_{\substack{L/N/K \\ N/K \text{ fn. Galois}}} \mathrm{Gal}(N/K) & \longrightarrow & \prod\limits_{\substack{M/N/K \\ N/K \text{ fn. Galois}}} \mathrm{Gal}(N/K) \\ \uparrow & & \uparrow \\ \varprojlim\limits_{\substack{L/N/K \\ N/K \text{ fn. Galois}}} \mathrm{Gal}(N/K) & \longrightarrow & \varprojlim\limits_{\substack{M/N/K \\ N/K \text{ fn. Galois}}} \mathrm{Gal}(N/K) \end{array}$$

where the upper arrow is the projection map and therefore continuous. As the bottom arrow corresponds to θ, we are done.

Part (3) follows from part (2) since $\{1\} \subset \mathrm{Gal}(M/K)$ is open and closed ($\mathrm{Gal}(M/K)$ has the discrete topology). □

Remark 1.10. $\mathrm{Gal}(L/K)$ is an example of a *topological group*, which is a topological space G with a compatible group structure. This means that G has multiplication and inversion maps

$$\begin{aligned} m : G \times G &\longrightarrow G \\ \iota : G &\longrightarrow G \end{aligned}$$

which are *continuous* and satisfy the usual group axioms. For example, there must exist an element $e \in G$ (the identity) such that

$$m(g, \iota(g)) = e$$

for all $g \in G$. In a topological group G, any subgroup H which is open is also closed (proof: $\bigcup_g g \cdot H$ is also open, where g runs through a set of left coset representatives for G/H, excluding the coset H itself). But closed subgroups are not necessarily open. So for subgroups, being open is a stronger condition than being closed.

Exercise 1.11. Let L/K be Galois.

(1) Show that $\mathrm{Gal}(L/K)$ is a topological group, i.e. show that the multiplication and inversion maps are continuous.

[2] To give a sketch, any $\sigma \in \mathrm{Gal}(M/K)$ gives a map $M \to \overline{L}$ by composing with $M \hookrightarrow L \hookrightarrow \overline{L}$. Using Zorn's lemma and the fact that L/M is algebraic, this extends to K-linear map $\overline{\sigma} : L \to \overline{L}$, and since L/K is Galois we have $\overline{\sigma}(L) \subseteq L$, giving an automorphism $\overline{\sigma} \in \mathrm{Gal}(L/K)$.

(2) Show that for $\sigma \in \mathrm{Gal}(L/K)$, the map $\tau \mapsto \sigma\tau$ is a homeomorphism of $\mathrm{Gal}(L/K)$ with itself.

(3) Show that $\{\mathrm{Gal}(L/M) : M/K \text{ finite Galois}\}$ is a basis of open sets at the identity. Conclude that $\mathrm{Gal}(L/K)$ is totally disconnected.

Now that we have endowed $\mathrm{Gal}(L/K)$ with a topology for any Galois extension L/K, we can extend theorem 1.1 to the case of L/K infinite.

Theorem 1.12. *Let L/K be a Galois extension with Galois group $G = \mathrm{Gal}(L/K)$. Then there is an inclusion-reversing bijection*

$$\{\textit{closed subgroups } H \leq G\} \longleftrightarrow \{\textit{subextensions } L/M/K\}$$

$$H \longmapsto L^H$$

$$\mathrm{Aut}(L/M) \longleftarrow\!\shortmid M$$

which furthermore restricts to bijections

$$\{\textit{normal closed subgroups } H \leq G\} \longleftrightarrow \{\textit{Galois subextensions } L/M/K\}$$
$$\{\textit{open subgroups } H \leq G\} \longleftrightarrow \{\textit{finite subextensions } L/M/K\}.$$

In particular, the normal open subgroups of proposition 1.9(3), given by $\mathrm{Gal}(L/M)$ for finite Galois M/K, are *all* of the open normal subgroups.

Proof. First we show that $\mathrm{Gal}(L/M)$ is open (resp. normal, resp. closed) if M/K is finite (resp. Galois, resp. arbitrary). Let M/K be finite. Then M is contained in some finite Galois extension N/K (e.g. the Galois closure of M). Hence $\mathrm{Gal}(L/M)$ contains the open subgroup $\mathrm{Gal}(L/N)$. But $\mathrm{Gal}(L/M)$ can be written as a union of cosets of $\mathrm{Gal}(L/M)$, all of which are open, so that $\mathrm{Gal}(L/M)$ is open as well. If M/K is Galois, then $\mathrm{Gal}(L/M)$ is normal by proposition 1.9(2). If M/K is arbitrary, then we can write $M = \bigcup M_i$ for a collection of finite subextensions M_i/K. Each $\mathrm{Gal}(L/M_i)$ is closed by proposition 1.9(3), hence

$$\mathrm{Gal}(L/M) = \bigcap \mathrm{Gal}(L/M_i)$$

is as well.

The maps $H \mapsto L^H$ and $M \mapsto \mathrm{Gal}(L/M)$ are clearly inclusion-reversing. We now show they are inverse to each other. If $L/M/K$ is a subextension, then L/M is Galois so that $L^{\mathrm{Gal}(L/M)} = M$. On the other hand, suppose that $H \leq G$ is closed. Clearly $H \subseteq \mathrm{Gal}(L/L^H)$. We will show that H is dense in $\mathrm{Gal}(L/L^H)$; since H is closed, equality will follow. Indeed, let $g \in \mathrm{Gal}(L/L^H)$. By exercise 1.11, any neighborhood of g contains some set of the form $g \cdot \mathrm{Gal}(L/M)$ for a finite Galois subextension $L/M/K$, so we'll be done if we show $g \cdot \mathrm{Gal}(L/M) \cap H$ is nonempty for any such M. Letting $\theta : \mathrm{Gal}(L/K) \to \mathrm{Gal}(M/K)$ be the restriction map, we see that $\theta(g)$ fixes $M^{\theta(H)}$, so that

$$\theta(g) \in \mathrm{Gal}(M/M^{\theta(H)}) = \theta(H)$$

by finite Galois theory. Hence there is some $h \in H$ with $\theta(h) = \theta(g)$. Thus $g^{-1}h \in \mathrm{Gal}(L/M)$, giving $h \in H \cap g \cdot \mathrm{Gal}(L/M)$ as desired.

Finally, we show that L^H is finite (resp. Galois) if $H \leq G$ is open (resp. normal). If $H \leq G$ is open, then it contains $\mathrm{Gal}(L/M)$ for some large enough finite Galois M/K (exercise 1.11(3)). Thus $L^H \subseteq L^{\mathrm{Gal}(L/M)} = M$, so L^H/K is finite as well. If $H \leq G$ is normal and closed then for any finite Galois subextension $L/M/K$ we have M^H/K is Galois as well by finite Galois theory. Since $L^H = \bigcup_M M^H$, we see that L^H is Galois as well. $\square$

2 Representations of $G_{\mathbb{Q}}$

Applying the results of section 1 to $G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ endows it with a topology. When studying the representation theory of $G_{\mathbb{Q}}$, we want to only consider the *continuous* maps $G_{\mathbb{Q}} \to \mathrm{GL}_n(K)$ for a field K. The topology on $G_{\mathbb{Q}}$ was defined in section 1. For the topology on $\mathrm{GL}_n(K)$, we must assume that K is a *topological field*, meaning a field endowed with a topology such that addition and multiplication are continuous functions $K \times K \to K$ and inversion is a continuous function $K^\times \to K^\times$. Then $\mathrm{GL}_n(K)$ inherits its topology as a subset of K^{n^2} (using the matrix entries as coordinates in K^{n^2}). Since we only need the specific cases where K is $\mathbb{C}$ or a finite extension of $\mathbb{Q}_\ell$ for a prime number ℓ, we won't dwell on this point. This leads to the following definition.

Definition 2.1. A *Galois representation* of dimension n over a (topological) field F is a continuous group homomorphism

$$\rho : G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_n(F).$$

If F is an extension of $\mathbb{Q}_\ell$, we call ρ an *ℓ-adic Galois representation.*

Remark 2.2. We will sometimes consider representations of a subgroup $G_K \leq G_{\mathbb{Q}}$ for a Galois extension $K/\mathbb{Q}$, defined in exactly the same way. We'll call these *Galois representations* of G_K. But when we write that ρ is a Galois representation without specifying the domain, always assume it to be a representation of the full group $G_{\mathbb{Q}}$.

Example 2.3. The most important example of a Galois representation is the *ℓ-adic cyclotomic character*, defined as follows. Let

$$\mu_n = \left\{ \zeta \in \overline{\mathbb{Q}}^\times : \zeta^n = 1 \right\}$$

denote the set of nth roots of unity in $\overline{\mathbb{Q}}^\times$. Recall that we have an isomorphism

$$\begin{aligned} \mathrm{Gal}(\mathbb{Q}(\mu_n)/\mathbb{Q}) &\xrightarrow{\sim} (\mathbb{Z}/n\mathbb{Z})^\times \\ \sigma &\mapsto a \quad \text{such that } \sigma(\zeta_n) = \zeta_n^a \end{aligned}$$

for any $\zeta_n \in \mu_n$.

Let ℓ be a prime number. Writing $\mu_{\ell^\infty} = \bigcup_{n \geq 1} \mu_{\ell^n}$, we have

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

where the inverse limit is taken with respect to the natural restriction maps. Using the isomorphisms $\mathrm{Gal}(\mathbb{Q}(\mu_{\ell^n})/\mathbb{Q}) \cong (\mathbb{Z}/\ell^n\mathbb{Z})^\times$ we can describe the inverse limit a different way. Indeed, for $m \leq n$ we have a commutative diagram

$$\begin{array}{ccc} \mathrm{Gal}(\mathbb{Q}(\mu_{\ell^n})/\mathbb{Q}) & \longrightarrow & \mathrm{Gal}(\mathbb{Q}(\mu_{\ell^m})/\mathbb{Q}) \\ \wr \downarrow & & \wr \downarrow \\ (\mathbb{Z}/\ell^n\mathbb{Z})^\times & \xrightarrow{\bmod \ell^m} & (\mathbb{Z}/\ell^m\mathbb{Z}) \end{array}$$

since ℓ^mth roots of unity are also ℓ^nth roots of unity. Thus we have

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

where the last isomorphism is because

$$\varprojlim(\mathbb{Z}/\ell^n)^\times \subseteq \varprojlim \mathbb{Z}/\ell^n\mathbb{Z} \cong \mathbb{Z}_\ell$$

is the subset consisting of elements not congruent to 0 mod ℓ. The ℓ-adic cyclotomic character is defined via

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

Strictly speaking, this is not yet a Galois representation because $\mathbb{Z}_\ell$ is not a field. To fix this, we simply view $\mathbb{Z}_\ell^\times$ inside of $\mathbb{Q}_\ell^\times$:

$$G_\mathbb{Q} \longrightarrow \mathbb{Z}_\ell^\times \hookrightarrow \mathbb{Q}_\ell^\times = \mathrm{GL}_1(\mathbb{Q}_\ell).$$

Here is another way of viewing example 2.3. We have an inverse system of abelian groups $A_n = \mu_{\ell^n}$ with the "multiplication by ℓ" transition maps $\mu_{\ell^n} \xrightarrow{\times \ell} \mu_{\ell^{n-1}}$ (in this case "multiplication" really means "exponentiation"). Moreover, the A_n have two more compatible structures. First, the A_n all have an action of $G_\mathbb{Q}$ compatible with the transition maps. And second, each A_n is a $\mathbb{Z}/\ell^n\mathbb{Z}$-module, again compatibly with the inverse system $\{\mathbb{Z}/\ell^n\mathbb{Z}\}$; this means that if $\zeta \in \mu_{\ell^n}$ and $a \in \mathbb{Z}/\ell^n\mathbb{Z}$ we have

$$(\zeta^a)^\ell = \left(\zeta^\ell\right)^{(a \mod \ell^{n-1})}.$$

One can check that this makes $\varprojlim A_n$ a $Z_\ell \cong \varprojlim \mathbb{Z}/\ell^n\mathbb{Z}$-module of rank 1 with a compatible action of $G_\mathbb{Q}$. Tensoring this module with $\mathbb{Q}_\ell$ over $\mathbb{Z}_\ell$ then gives a one-dimensional $G_\mathbb{Q}$-representation over $\mathbb{Q}_\ell$.

This is a very good paradigm for how Galois reprsentations arise from geometry. In general, given an inverse system of finite-rank $\mathbb{Z}/\ell^n\mathbb{Z}$-modules with compatible Galois actions,taking the inverse limit gives a finite-rank $\mathbb{Z}_\ell$-module with a $G_\mathbb{Q}$-action. By tensoring with $\mathbb{Q}_\ell$, we obtain a representation of $G_\mathbb{Q}$ over $\mathbb{Q}_\ell$. The representations obtained in this way are called ℓ-adic *Tate modules.*[3]

Remark 2.4. Let $\rho : G_\mathbb{Q} \to \mathrm{GL}_n(\mathbb{C})$ be a complex n-dimensional Galois representation. The topologies on $G_\mathbb{Q}$ and $\mathbb{C}$ are very qualitatively different, and this puts strong restrictions on the possible ρ. For example, $G_\mathbb{Q}$ has arbitrarily small subgroups, in the sense that any open neighborhood of the identity contains some subgroup (because the open subgroups $\mathrm{Gal}(\overline{\mathbb{Q}}/K)$ for $K/\mathbb{Q}$ finite Galois form a basis of opens at the identity). On the other hand, $\mathrm{GL}_n(\mathbb{C})$ has no small subgroups: there is a neighborhood V of the identity such that the only subgroup contained in V is trivial (see exercise 2.6). This observation can be buffed into the following proposition, which implies that ρ can be studied via representation theory of finite groups.

Proposition 2.5. *Let $\rho : G_\mathbb{Q} \to \mathrm{GL}_n(\mathbb{C})$ be a complex Galois representation. Then ρ factors as $G_\mathbb{Q} \twoheadrightarrow \mathrm{Gal}(K/\mathbb{Q}) \to \mathrm{GL}_n(\mathbb{C})$ for some finite Galois $K/\mathbb{Q}$.*

Proof. Let $V \subseteq \mathrm{GL}_n(\mathbb{C})$ be an open neighborhood of the identity so containing no nontrivial subgroups (see exercise 2.6). Then $\rho^{-1}(V) \subseteq G_\mathbb{Q}$ is an open neighborhood of the identity, hence contains some open normal subgroup $\mathrm{Gal}(\overline{\mathbb{Q}}/K)$ for a finite Galois $K/\mathbb{Q}$. But $\rho(\mathrm{Gal}(\overline{\mathbb{Q}}/K))$ is then a subgroup of $\mathrm{GL}_n(\mathbb{C})$ contained in V, so $\rho(\mathrm{Gal}(\overline{\mathbb{Q}}/K)) = \{1\}$. As $G_\mathbb{Q}/\mathrm{Gal}(\overline{\mathbb{Q}}/K) = \mathrm{Gal}(K/\mathbb{Q})$, we obtain the result. □

[3]Formally, the representation of example 2.3 is the ℓ-adic Tate module of the group scheme $\mathbb{G}_m$.

Exercise 2.6. This exercise proves the "no small subgroup" property of $\mathrm{GL}_n(\mathbb{C})$. The key input is the *exponential map* $\exp : M_n(\mathbb{C}) \to \mathrm{GL}_n(\mathbb{C})$, where $M_n(\mathbb{C})$ is the set of $n \times n$ matrices with entries in $\mathbb{C}$. The exponential is defined as a power series

$$\exp(X) = \sum_{n \geq 0} \frac{1}{n!} X^n \qquad \text{for } X \in M_n(\mathbb{C}).$$

You may assume that there is some neighborhood U of $0 \in M_n(\mathbb{C})$ so that exp is a diffeomorphism from U to its image.

(1) If $X, Y \in M_n(\mathbb{C})$ commute, show that $\exp(X+Y) = \exp(X)\exp(Y)$. Deduce that $\exp(nX) = \exp(X)^n$ for any $n \in \mathbb{Z}$.

(2) Show that there is a neighborhood V of $1 \in \mathrm{GL}_n(\mathbb{C})$ so that the only subgroup $H \leq \mathrm{GL}_n(\mathbb{C})$ contained in V is trivial.

2.1 Ramification

Let $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_n(K)$ be an n-dimensional Galois representation over a field K, and let p be a prime. In many cases, we would like to make sense of an element $\rho(\sigma_p) \in \mathrm{GL}_n(K)$ where $\sigma_p \in G_{\mathbb{F}_p} = \mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$ denotes the *Frobenius automorphism*

$$\sigma_p(a) = a^p$$

for all $a \in \overline{\mathbb{F}}_p$. Of course, $\rho(\sigma_p)$ is nonsense, since σ_p is not an element of $G_{\mathbb{Q}}$. Nevertheless, if ρ has good "local behavior" at p in a certain sense, then we can make sense of $\rho(\sigma_p)$ up to conjugacy in $\mathrm{GL}_n(K)$. In such a case, we say that ρ is *unramified* at p; otherwise it is *ramified*.

This terminology mirrors the case of a Galois extension of number fields $K/\mathbb{Q}$, which we briefly review here. If p is a prime number and $\mathfrak{p}$ is a prime of K lying over p, then we have a reduction map

$$D_{\mathfrak{p}} \to \mathrm{Gal}(\mathbb{F}_{\mathfrak{p}}/\mathbb{F}_p)$$

where $D_{\mathfrak{p}} = \{\sigma \in \mathrm{Gal}(K/\mathbb{Q}) : \sigma(\mathfrak{p}) = \mathfrak{p}\}$ and $\mathbb{F}_{\mathfrak{p}} = \mathcal{O}_K/\mathfrak{p}$ is the residue field at $\mathfrak{p}$. This map is surjective, and we write $I_{\mathfrak{p}}$ for the kernel. In other words, we have an exact sequence

$$1 \longrightarrow I_{\mathfrak{p}} \longrightarrow D_{\mathfrak{p}} \longrightarrow \mathrm{Gal}(\mathbb{F}_{\mathfrak{p}}/\mathbb{F}_p) \longrightarrow 1$$

As $\mathrm{Gal}(\mathbb{F}_{\mathfrak{p}}/\mathbb{F}_p)$ is generated by the Frobenius σ_p, we get a generator $\sigma_p \in D_{\mathfrak{p}}/I_{\mathfrak{p}}$. The extension $K/\mathbb{Q}$ is unramified at p if and only if $I_{\mathfrak{p}}$ is trivial, in which case σ_p generates $D_{\mathfrak{p}}$. The decomposition groups $D_{\mathfrak{p}}$ for varying primes $\mathfrak{p}$ over p are conjugate; hence, for an extension unramified at p, we get a Frobenius element $\sigma_p \in \mathrm{Gal}(K/\mathbb{Q})$ well-defined up to conjugacy.

Given a prime number p, we would like to define *absolute* decomposition and inertia groups in $G_{\mathbb{Q}}$ which fit into the exact sequence

$$1 \longrightarrow I_p \longrightarrow D_p \longrightarrow \mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p) \longrightarrow 1.$$

As before, there will be many possible choices for D_p, all of which are conjugate by an element of $G_{\mathbb{Q}}$. Again we have the Frobenius $\sigma_p \in \mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$; it is no longer a generator, but instead a *topological generator* for $\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$ in the sense of exercise 2.8. Thus, if $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_n(K)$ is a Galois representation with $I_p \subseteq \ker \rho$, we can make sense of an element $\rho(\sigma_p) \in \mathrm{GL}_n(K)$ which is well-defined up to conjugation. This is what it means to be unramified at p.

Definition 2.7. Let p be a prime number, $D_p \leq G_{\mathbb{Q}}$ be some choice of decomposition group, let $I_p \leq D_p$ be the inertia subgroup (I_p and D_p are defined below). A Galois representation $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_n(K)$ is *unramified at* p if $I_p \subseteq \ker \rho$.

Exercise 2.8. Let $\sigma_p \in \mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$ be the Frobenius automorphism. Show that the subgroup $\langle \sigma_p \rangle$ generated by σ_p is dense in $\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$. An element with this property is called a *topological generator*.

Exercise 2.9. Check that definition 2.7 does not depend on the choice of D_p. That is, show that if ρ is unramified with respect to some choice of D_p, then it is ramified with respect to every choice.

We now turn to the task of defining D_p and I_p. There are two equivalent ways of doing so. The first is very similar to the approach in the case of finite extensions, but uses some nontrivial facts about the extension $\overline{\mathbb{Q}}/\mathbb{Q}$. The second is more unfamiliar, but uses nontrivial facts about extensions of $\mathbb{Q}_p$ (which are easier to deal with). To emphasize the central concepts, we omit the proofs of the nontrivial facts used in the first method, and relegate the proofs of the nontrivial facts for the second method to exercises 2.13 through 2.16. Note that there is a notational ambiguity: D_p might represent either the absolute decomposition group or the decomposition group of the trivial extension $\mathbb{Q}/\mathbb{Q}$. Since the latter is trivial, we always take D_p to mean the former.

For the first approach, let $\mathfrak{p} \subseteq \mathcal{O}_{\overline{\mathbb{Q}}}$ be a prime lying over p. Then as before, we have the decomposition group

$$D_p = \{\sigma \in G_{\mathbb{Q}} : \sigma(\mathfrak{p}) = \mathfrak{p}\}$$

and a reduction map $D_p \to \mathrm{Gal}(\mathbb{F}_{\mathfrak{p}}/\mathbb{F}_p)$, where in fact $\mathbb{F}_{\mathfrak{p}} = \overline{\mathbb{F}}_p$. As in the case of finite extensions, the reduction map is surjective, and we define I_p to be its kernel. And as in the case of finite extensions, all of the primes of $\mathcal{O}_{\overline{\mathbb{Q}}}$ over p are conjugate, so that the choices of D_p are conjugate as well.

For the second approach, consider the embedding $\mathbb{Q} \hookrightarrow \mathbb{Q}_p \hookrightarrow \overline{\mathbb{Q}}_p$. This extends (non-uniquely) to an embedding $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$, and any two such extensions are conjugate by an element of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. This gives a continuous map

$$\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p) \hookrightarrow \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}) \to \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$$

which is injective by exercise 2.16. The image of this injection is a closed subgroup $D_p \leq G_{\mathbb{Q}}$, the decomposition group, and different choices of $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$ give conjugate decomposition groups. The residue field of $\overline{\mathbb{Q}}_p$ is $\overline{\mathbb{F}}_p$ (exercise 2.14), and we have a map $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p) \to \mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$ defined in the usual way. This map is continuous and surjective (exercise 2.15), thereby inducing a continuous surjection $D_p \twoheadrightarrow G_{\mathbb{F}_p}$. The inertia group $I_p \leq D_p$ is the kernel of this map.

Remark 2.10. This second approach works just as well for a finite extension $K/\mathbb{Q}$. Indeed, let $\mathfrak{p}$ be a prime of K over p. (The following remark explains why this is equivalent to choosing an embedding $K \hookrightarrow \overline{\mathbb{Q}}_p$.) As above we have a map

$$\mathrm{Gal}(K_{\mathfrak{p}}/\mathbb{Q}_p) \longrightarrow \mathrm{Gal}(K/\mathbb{Q}).$$

By exercise 2.13, σ and $\sigma^{-1} \in \mathrm{Gal}(K_{\mathfrak{p}}/\mathbb{Q}_p)$ are continuous, so that $\sigma(\mathfrak{p}) = \mathfrak{p}$. Thus this map has image in $D_{\mathfrak{p}}$, giving a map

$$\mathrm{Gal}(K_{\mathfrak{p}}/\mathbb{Q}_p) \longrightarrow D_{\mathfrak{p}} = \{\sigma \in \mathrm{Gal}(K/\mathbb{Q}) : \sigma(\mathfrak{p}) = \mathfrak{p}\}.$$

This map is an isomorphism. Indeed, any $\sigma \in D_{\mathfrak{p}}$ is continuous for the $\mathfrak{p}$-adic topology on K, thereby extending to an automorphism of $K_{\mathfrak{p}}$. By exercise 2.13 this automorphism fixes $\mathbb{Q}_p$. Hence we have an inverse map $D_{\mathfrak{p}} \to \mathrm{Gal}(K_{\mathfrak{p}}/\mathbb{Q}_p)$.

Remark 2.11. Let $K/\mathbb{Q}$ be a finite extension. Then a choice of prime $\mathfrak{p}$ of K over p induces an embedding $K \hookrightarrow K_{\mathfrak{p}} \hookrightarrow \overline{\mathbb{Q}}_p$. Conversely, an embedding $K \hookrightarrow \overline{\mathbb{Q}}_p$ induces a nonarchimedean valuation on K by restricting the valuation of $\overline{\mathbb{Q}}_p$. Ostrowski's theorem says that this valuation is equivalent to the $\mathfrak{p}$-adic valuation for a unique prime $\mathfrak{p}$ of K over p. Thus picking a prime $\mathfrak{p}$ over p is equivalent to picking an embedding $K \hookrightarrow \overline{\mathbb{Q}}_p$.

Remark 2.11 has the following important consequence. Fix an embedding $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$. Then for any finite Galois $K/\mathbb{Q}$ we have a commutative diagram

$$\begin{array}{ccc} G_{\mathbb{Q}_p} & \hookrightarrow & G_{\mathbb{Q}} \\ \downarrow & & \downarrow \\ \mathrm{Gal}(K_{\mathfrak{p}}/\mathbb{Q}_p) & \hookrightarrow & \mathrm{Gal}(K/\mathbb{Q}) \end{array}$$

where $\mathfrak{p}$ is the prime of K induced by the embedding $K \hookrightarrow \overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$. It follows that a choice of absolute decomposition group restricts to a decomposition group of the finite extension $K/\mathbb{Q}$ under the map $G_{\mathbb{Q}} \twoheadrightarrow \mathrm{Gal}(K/\mathbb{Q})$. The same is true of the absolute inertia group.

Example 2.12. The ℓ-adic cyclotomic character $\chi_\ell : G_{\mathbb{Q}} \to \mathbb{Q}_\ell^\times$ is unramified at all primes $p \neq \ell$. Indeed, χ_ℓ factors through the map

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

and each extension $\mathbb{Q}(\mu_{\ell^n})/\mathbb{Q}$ is unramified at all $p \neq \ell$. Hence the absolute inertia group I_p has trivial image in $\mathrm{Gal}(\mathbb{Q}(\mu_{\ell^\infty})/\mathbb{Q})$ by the preceding discussion. We can also compute the action of Frobenius:

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

$$\left(\frac{p}{\mathbb{Q}(\mu_{\ell^\infty})/\mathbb{Q}}\right) \longmapsto \left(\left(\frac{p}{\mathbb{Q}(\mu_{\ell^n})/\mathbb{Q}}\right)\right)_{n \geq 1} \longmapsto (p)_{n \geq 1} \longmapsto p \longmapsto p$$

where we denote the Frobenius of the extension L/K at p by $\left(\frac{p}{L/K}\right)$. Thus $\chi_\ell(\sigma_p) = p$ for $p \neq \ell$. The fact that χ_ℓ is unramified at almost every prime is no fluke – this is the typical behavior of Galois representations we'll encounter.

The following exercises tie together the ends we've left loose.

Exercise 2.13. Recall that the topology on $\overline{\mathbb{Q}}_p$ is defined via the unique absolute value $|\cdot|$ on $\overline{\mathbb{Q}}_p$ extending the p-adic absolute value $|\cdot|_p$ on $\mathbb{Q}_p$. Explicitly, for any $\alpha \in \overline{\mathbb{Q}}_p$ we have

$$|\alpha| = \left|N_{\mathbb{Q}_p(\alpha)/\mathbb{Q}_p}(\alpha)\right|_p^{1/[\mathbb{Q}_p(\alpha):\mathbb{Q}_p]}.$$

Show that if $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ and $\alpha \in \overline{\mathbb{Q}}_p$ then $|\sigma(\alpha)| = |\alpha|$. Conclude that if $K/\mathbb{Q}_p$ is an algebraic extension, then any field automorphism of K is automatically *continuous*. In particular, show that the only automorphism of $\mathbb{Q}_p$ is the identity.

Exercise 2.14. This exercise defines the map $G_{\mathbb{Q}_p} \to G_{\mathbb{F}_p}$ and establishes its basic properties (not including surjectivity). The following exercise 2.15 gives a more sophisticated (albeit conceptually cleaner) perspective on this map, which automatically shows it is surjective.

(1) Show that the residue field of $\overline{\mathbb{Q}}_p$ is $\overline{\mathbb{F}}_p$.

(2) Use exercise 2.13 to show that any $\sigma \in G_{\mathbb{Q}_p}$ preserves the valuation ring $\mathcal{O}_{\overline{\mathbb{Q}}_p}$ and maximal ideal $\mathfrak{p}$ of $\overline{\mathbb{Q}}_p$.

(3) Use parts (1) and (2) to define a homomorphism $G_{\mathbb{Q}_p} \to G_{\mathbb{F}_p}$.

(4) Show that the homomorphism $G_{\mathbb{Q}_p} \to G_{\mathbb{F}_p}$ is continuous.

Exercise 2.15. This exercise uses unramified extensions to give a conceptually cleaner perspective on the map $G_{\mathbb{Q}_p} \to G_{\mathbb{F}_p}$. Specifically, we show there is a canonical isomorphism $G_{\mathbb{F}_p} \cong \mathrm{Gal}(\mathbb{Q}_p^{ur}/\mathbb{Q}_p)$ where $\mathbb{Q}_p^{ur}$ is the maximal unramified extension of $\mathbb{Q}_p$, and this isomorphism identifies the map $G_{\mathbb{Q}_p} \to G_{\mathbb{F}_p}$ with the restriction $G_{\mathbb{Q}_p} \twoheadrightarrow \mathrm{Gal}(\mathbb{Q}_p^{ur}/\mathbb{Q}_p)$, which is automatically surjective.

Recall that a finite extension $K/\mathbb{Q}_p$ is *unramified* if

$$[K : \mathbb{Q}_p] = [\kappa : \mathbb{F}_p]$$

where $\kappa = \mathcal{O}_K/\mathfrak{p}$ is the residue field of K. Equivalently, $K/\mathbb{Q}_p$ is unramified if $\mathfrak{p} = p\mathcal{O}_K$.

(1) Let K, K' be unramified extensions of $\mathbb{Q}_p$. Show that a $\mathbb{Q}_p$-linear map $f : K \to K'$ has $f(\mathcal{O}_K) \subseteq \mathcal{O}_{K'}$ and $f(\mathfrak{p}_K) \subseteq \mathfrak{p}_{K'}$.

(2) Deduce that we have a functor

$$\mathcal{F} : \left\{ \begin{array}{c} \text{finite unramified extensions} \\ K/\mathbb{Q}_p \end{array} \right\} \longrightarrow \left\{ \begin{array}{c} \text{finite extensions} \\ \kappa/\mathbb{F}_p \end{array} \right\}$$

via $\mathcal{F}(K) = \mathcal{O}_K/\mathfrak{p}_K$, the residue field of K. The morphisms on both sides are field homomorphisms (which automatically fix $\mathbb{Q}_p$ on the left or $\mathbb{F}_p$ on the right).

(3) Use the primitive element theorem and Hensel's lemma to show that the functor $\mathcal{F}$ is essentially surjective, i.e. for every finite extension $\kappa/\mathbb{F}_p$ there is a finite unramified $K/\mathbb{Q}_p$ with residue field κ.

(4) Again use the primitive element theorem and Hensel's lemma to show that $\mathcal{F}$ is fully faithful, i.e. if K, K' are unramified extensions with residue fields κ, κ' then the map

$$\mathrm{Hom}(K, K') \longrightarrow \mathrm{Hom}(\kappa, \kappa')$$

via $f \mapsto \mathcal{F}(f)$ is a bijection.

(5) By parts (3) and (4), the functor $\mathcal{F}$ is an equivalence of categories. Deduce that we have a natural isomorphism $\mathrm{Gal}(K/\mathbb{Q}_p) \cong \mathrm{Gal}(\kappa/\mathbb{Q}_p)$ where κ is the residue field of the finite unramified extension $K/\mathbb{Q}_p$.

(6) As the compositum of two finite unramified extensions is again finite unramified, we can let the *maximal unramified extension* $\mathbb{Q}_p^{ur}/\mathbb{Q}_p$ be the union of all finite unramified extensions. Show that the residue field of $\mathbb{Q}_p^{ur}$ is $\overline{\mathbb{F}}_p$. Also show that $\mathrm{Gal}(\mathbb{Q}_p^{ur}/\mathbb{Q}_p) \cong G_{\mathbb{F}_p}$ and that the map $G_{\mathbb{Q}_p} \to G_{\mathbb{F}_p}$ factors as

$$G_{\mathbb{Q}_p} \twoheadrightarrow \mathrm{Gal}(\mathbb{Q}_p^{ur}/\mathbb{Q}_p) \xrightarrow{\sim} G_{\mathbb{F}_p}.$$

Hence this map is automatically surjective and continuous.

Exercise 2.16. This exercise shows that the map $G_{\mathbb{Q}_p} \to G_{\mathbb{Q}}$ is injective. The key input is *Krasner's lemma*. Part (5) also uses Krasner's lemma to show that the completion of $\overline{\mathbb{Q}}_p$ is still algebraically closed; we denote this field by $\mathbb{C}_p$.

(1) Let $\alpha, \beta \in \overline{\mathbb{Q}}_p$ such that
$$|\alpha - \beta| < |\sigma(\alpha) - \alpha|$$
for all $\sigma \in G_{\mathbb{Q}_p}$ such that $\sigma(\alpha) \neq \alpha$. In other words, suppose that β is closer to α than any of α's conjugates are. Prove that $\mathbb{Q}_p(\alpha) \subseteq \mathbb{Q}_p(\beta)$. This is Krasner's lemma.

(2) Let $P(X) = \sum p_i X^i \in \mathbb{Q}_p[X]$ be a monic irreducible polynomial of degree n with roots $\alpha_1, \ldots, \alpha_n$. Using part (1), show that there is an $\epsilon > 0$ so that if $Q(X) = \sum q_i X^i \in \mathbb{Q}_p[X]$ is a monic irreducible polynomial of degree n with roots $\beta_1, \ldots, \beta_n$ such that
$$|p_i - q_i|_p < \epsilon \qquad \text{for all } i = 0, \ldots, n-1,$$
then (possibly after reordering the β_i) we have $\mathbb{Q}_p(\alpha_i) = \mathbb{Q}_p(\beta_i)$ for all $i = 1, \ldots, n$. In other words, if two polynomials are "sufficiently close" then they generate the same extensions of $\mathbb{Q}_p$.

(3) Use the primitive element theorem and part (2) to show that if $K/\mathbb{Q}_p$ is a finite extension, then there is a number field $L/\mathbb{Q}$ and an absolute value $|\cdot|$ on L so that K is the completion of L with respect to $|\cdot|$.

(4) Fix an embedding $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$. Arguing as in part (3), show that $\mathbb{Q}_p\overline{\mathbb{Q}} = \overline{\mathbb{Q}}_p$. Deduce that the map $G_{\mathbb{Q}_p} \to G_{\mathbb{Q}}$ induced by our choice of embedding is injective.

(5) Show that the completion $\mathbb{C}_p$ of $\overline{\mathbb{Q}}_p$ with respect to the canonical absolute value on $\overline{\mathbb{Q}}_p$ is algebraically closed.

3 L-functions

In this section, we discuss L-functions, which conveniently package the essential information contained in a Galois representation into an analytic function. Familiar examples of L-functions include the Riemann zeta function $\zeta(s)$ and the Dirichlet L-functions $L(\chi, s)$ for a Dirichlet character $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$:
$$\zeta(s) = \sum_{n \geq 1} n^{-s}, \qquad L(\chi, s) = \sum_{n \geq 1} \chi(n) n^{-s}.$$
These are convergent on the half-plane $\{s \in \mathbb{C} : \mathrm{Re}(s) > 1\}$. An important fact about these L-functions is that they have *Euler products*
$$\zeta(s) = \prod_p \frac{1}{1 - p^{-s}}, \qquad L(\chi, s) = \prod_{p \nmid N} \frac{1}{1 - \chi(p) p^{-s}}.$$
This is no coincidence: in this section we will *define* L-functions by an Euler product of this form. These L-functions also have meromorphic continuations to $\mathbb{C}$ and functional equations; these are properties that we *hope* will hold for general L-functions, but are conjectural in many cases.

There are two ways basic ways of forming L-functions. First, given a complex Galois representation $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_n(\mathbb{C})$, one can form an *Artin L-function*. These L-functions are known to have meromorphic continuations and functional equations. The two examples above are both Artin L-functions. The second way of forming L-functions is more complicated: it comes from a *compatible system* of ℓ-adic Galois representations $\{\rho_\ell\}$ varying over primes ℓ. These L-functions are much subtler and less is known about them. Since the most interesting Galois representations are ℓ-adic, we would like to understand these L-functions as well as we understand the Artin L-functions.

3.1 Artin L-functions

The L-functions in this section will not be directly important for this course, though they give important context for what L-functions are and what sorts of properties we expect them to have.

Let $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_n(\mathbb{C})$ be a complex n-dimensional Galois representation. By proposition 2.5, ρ factors as $G_{\mathbb{Q}} \to \mathrm{Gal}(K/\mathbb{Q}) \to \mathrm{GL}_n(\mathbb{C})$ for some finite Galois $K/\mathbb{Q}$, so we replace the study of ρ with the study of the induced representation of the finite group $\mathrm{Gal}(K/\mathbb{Q})$. Slightly more generally, Artin L-functions come from representations of Galois groups $\mathrm{Gal}(L/K)$ for a Galois extension of number fields L/K.

Let $\mathfrak{p}$ be a prime of K lying under a prime $\mathfrak{P}$ of L. Denote by $N\mathfrak{p} = \#\mathbb{F}_{\mathfrak{p}}$ the norm of $\mathfrak{p}$. As before, we say that a representation $\rho : \mathrm{Gal}(L/K) \to \mathrm{GL}_n(\mathbb{C})$ is *unramified* at $\mathfrak{p}$ if $I_{\mathfrak{P}} \subseteq \ker \rho$. In this case, we have an element $\rho(\sigma_{\mathfrak{p}}) \in \mathrm{GL}_n(\mathbb{C})$ where $\sigma_{\mathfrak{p}} = (x \mapsto x^{N\mathfrak{p}}) \in \mathrm{Gal}(\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}})$ is the Frobenius.

Definition 3.1. Let L/K be a Galois extension of number fields, and let $\rho : \mathrm{Gal}(L/K) \to \mathrm{GL}(V)$ be a representation on an n-dimensional $\mathbb{C}$-space.

(1) If $I_{\mathfrak{P}}$ is some choice of inertia group at the prime $\mathfrak{p}$ of K, let

$$V^{I_{\mathfrak{P}}} = \{v \in V : \rho(\sigma)v = v \text{ for all } \sigma \in I_{\mathfrak{P}}\}$$

be the subspace of V fixed by $I_{\mathfrak{P}}$. Note that ρ then gives a representation ρ^{I_p} of $\mathrm{Gal}(L/K)$ on $V^{I_{\mathfrak{P}}}$ which is unramified at $\mathfrak{p}$.

(2) For each prime $\mathfrak{p}$ of K, the *local L-factor* is

$$L_{\mathfrak{p}}(\rho, T) = \frac{1}{\det(1 - T\sigma_p | \rho^{I_p})} \in \mathbb{C}(T)$$

where $\det(1-T\sigma_p|\rho^{I_p})$ denotes the determinant of $1-T\sigma_p$ acting on V^{I_p} by the representation ρ^{I_p}. Note that this polynomial is $\chi_{\rho^{I_p}(\sigma_p)}(1/T)$ for the characteristic polynomial $\chi_{\rho^{I_p}(\sigma_p}(T) \in \mathbb{C}[T]$ of $\rho^{I_p}(\sigma_{\mathfrak{p}})$. As the characteristic polynomial of a matrix is invariant under conjugation, the local L-factor does not depend on the choice of $\mathfrak{P}$ lying over $\mathfrak{p}$.

(3) The *(global) L-function* is

$$L(\rho, s) = \prod_{\mathfrak{p}} L_{\mathfrak{p}}(\rho, N\mathfrak{p}^{-s})$$

for $s \in \mathbb{C}$ such that the infinite product converges. The product is over all primes $\mathfrak{p}$ of K.

Remark 3.2. Though it is traditional to define Artin L-functions as above, it is perhaps more natural to view them as being associated to a Galois representation $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_n(\mathbb{C})$ of the full absolute Galois group (or of a subgroup G_K). By the discussion above, any such ρ factors through the Galois group of a finite extension, so we get exactly the same thing. Given a Galois representation $\rho : G_K \to \mathrm{GL}_n(\mathbb{C})$, we will sometimes write $L(\rho, s)$ for the Artin L-function associated to any representation $\mathrm{Gal}(L/K) \to \mathrm{GL}_n(\mathbb{C})$ such that $G_L \subseteq \ker \rho$. It is worth checking that this is well defined.

Exercise 3.3. Given a Galois representation $\rho : G_K \to \mathrm{GL}_n(\mathbb{C})$, check that $L(\rho, s)$ depends only on ρ and not on the choice of L/K such that $G_L \subseteq \ker \rho$, as in remark 3.2. In particular, show that if $M/L/K$ are Galois extensions and $\rho : \mathrm{Gal}(L/K) \to \mathrm{GL}_n(\mathbb{C})$ is a representation, then

$$L(\rho, s) = L(\rho', s)$$

where ρ' is the representation $\mathrm{Gal}(M/K) \twoheadrightarrow \mathrm{Gal}(L/K) \xrightarrow{\rho} \mathrm{GL}_n(\mathbb{C})$.

Example 3.4. Let $\rho : \mathrm{Gal}(\mathbb{Q}/\mathbb{Q}) \to \mathrm{GL}_1(\mathbb{C})$ be the trivial representation. Then ρ is unramified at every p, and we have $L_p(\rho, T) = \frac{1}{1-T}$. This gives the global L-function

$$L(\rho, s) = \prod_p \frac{1}{1 - p^{-s}} = \zeta(s).$$

More generally, if K is a number field and ρ is the trivial representation $\rho : \mathrm{Gal}(K/K) \to \mathrm{GL}_1(\mathbb{C})$ then

$$L(\rho, s) = \prod_{\mathfrak{p}} \frac{1}{1 - N\mathfrak{p}^{-s}} = \sum_I NI^{-s}$$

where the sum is over ideals of K. This is the *Dedekind zeta function* $\zeta_K(s)$ of K.

Example 3.5. Let $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$ be a Dirichlet character. Via the isomorphism $\mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q}) \cong (\mathbb{Z}/N\mathbb{Z})^\times$, we can view χ as a Galois representation. Specifically, define ρ_χ by the composition

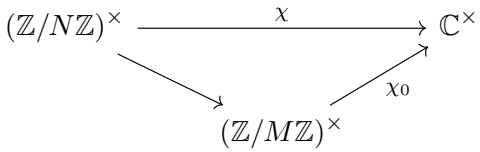
$$G_\mathbb{Q} \twoheadrightarrow \mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q}) \xrightarrow{\sim} (\mathbb{Z}/N\mathbb{Z})^\times \xrightarrow{\chi} \mathrm{GL}_1(\mathbb{C}).$$

Since the extension $\mathbb{Q}(\zeta_N)/\mathbb{Q}$ is unramified at all $p \nmid N$, so also is ρ_χ. The local L-factor at such a prime is

$$L_p(\rho_\chi, T) = \frac{1}{1 - \rho_\chi(\sigma_p)T} = \frac{1}{1 - \chi(p)T}$$

just as for the Dirichlet L-function.

The situation is slightly trickier for $p|N$. Recall that a Dirichlet character χ mod N is *imprimitive* if it factors through some $(\mathbb{Z}/M\mathbb{Z})^\times$ for $M|N$, i.e. if we have a commutative diagram



for some Dirichlet character χ_0 mod M. On the level of Galois representations, this is equivalent to ρ_χ factoring through $\mathrm{Gal}(\mathbb{Q}(\zeta_M)/\mathbb{Q})$ for some subfield $\mathbb{Q}(\zeta_M) \subseteq \mathbb{Q}(\zeta_N)$. If χ and χ_0 are as in the above commutative diagram, then they define the same Galois representation $\rho_\chi = \rho_{\chi_0}$. But if there is some prime dividing N but not M, then the Dirichlet L-functions of χ and χ_0 will differ (look at the Euler products). Thus, if we want $L(\rho_\chi, s)$ and $L(\chi, s)$ to be the same, we must assume that χ is *primitive*.

Doing so, we have extensions of fields $\mathbb{Q}(\zeta_N)/L/\mathbb{Q}$ where $L = \overline{\mathbb{Q}}^{\ker \rho_\chi}$, and by assumption $\mathbb{Q}(\zeta_N)$ is the smallest cyclotomic field containing L. By construction, χ defines an *injective* map $\mathrm{Gal}(L/\mathbb{Q}) \to \mathbb{C}^\times$. At this point, we must use a simple fact from class field theory: the ramified primes in L are exactly the same as the ramified primes in $\mathbb{Q}(\zeta_N)$.[4] Hence if p ramifies in $\mathbb{Q}(\zeta_N)$, then it ramifies in L; since the map $\mathrm{Gal}(L/\mathbb{Q}) \to \mathbb{C}^\times$ induced by χ is injective, $\rho(I_p) \supsetneq \{1\}$, so that $\mathbb{C}^{I_p} = \{0\}$. This shows that

$$L_p(\rho_\chi, T) = 1.$$

In summary, we have shown that if χ is primitive, then $L(\rho_\chi, s) = L(\chi, s)$.

Exercise 3.6. How does $L(\rho_\chi, s)$ relate to $L(\chi, s)$ if χ is imprimitive?

[4]This is because a prime p ramifies in L if and only if it divides the conductor of L.

Remark 3.7. Viewed differently, example 3.5 shows there is a bijection

$$\left\{ \begin{array}{c} \text{primitive} \\ \text{Dirichlet characters} \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \text{1-dimensional complex} \\ \text{Galois representations} \end{array} \right\}$$

which preserves L-functions. Using class field theory, one shows a similar bijection

$$\{\text{finite order Hecke characters}\} \longleftrightarrow \{\text{Dirichlet characters}\}$$

which preserves L-functions. Hecke characters have a notion of primitivity which is compatible with that of Dirichlet characters, so in total we have an L-function preserving bijection

$$\left\{ \begin{array}{c} \text{primitive finite order} \\ \text{Hecke characters} \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \text{1-dimensional complex} \\ \text{Galois representations} \end{array} \right\}.$$

This bijection is part of an $n = 1$ analogue of the modularity theorem. The Hecke characters provide the *automorphic* side, which modular forms provide in the $n = 2$ case. And the right-hand side is the Galois representation theoretic side, which will become 2-dimensional Galois representations when $n = 2$.

What about the non-finite order Hecke characters? They still correspond to Galois representation theoretic data, but the representations cannot be complex since all such representations are finite order. Instead we will need the compatible systems of ℓ-adic representations of section 3.2.

The following exercises compute some examples of Artin L-functions.

Exercise 3.8. Let $K/\mathbb{Q}$ be a quadratic extension. Write down $L(\rho, s)$ for all irreducible representations ρ of $\mathrm{Gal}(K/\mathbb{Q})$. Multiply these functions together – is the result familiar?

Exercise 3.9. Repeat exercise 3.8 for $K = \mathbb{Q}(\zeta_7)$. Formulate a conjecture that should hold for any abelian extension L/K.

Exercise 3.10. Repeat exercise 3.8 for K your favorite non-abelian extension. How do you need to refine your conjecture from exercise 3.9 to apply to non-abelian extensions?

Students who enjoy representation theory should also like the following exercise.

Exercise 3.11. Let L/K be Galois.

(1) If ρ, ρ' are representations of $\mathrm{Gal}(L/K)$ then show

$$L(\rho \oplus \rho', s) = L(\rho, s)L(\rho', s).$$

(2) Let $L/K'/K$ be a Galois subextension, and let ρ be a representation of $\mathrm{Gal}(L/K')$. Show that

$$L(\rho, s) = L(\mathrm{Ind}_{\mathrm{Gal}(L/K')}^{\mathrm{Gal}(L/K)} \rho, s)$$

where $\mathrm{Ind}_{\mathrm{Gal}(L/K')}^{\mathrm{Gal}(L/K)} \rho$ is the induced representation.

(3) Prove that that

$$\zeta_L(s) = \zeta_K(s) \prod_{\text{irrep } \rho \neq 1} L(\rho, s)^{\dim \rho}$$

where the product runs over the nontrivial irreducible representations of $\mathrm{Gal}(L/K)$.

Before moving on to the second type of L-function, we state some deeper properties of Artin L-functions, namely that they have a meromorphic continuation and functional equation. These properties are emblematic of the sorts of properties we expect other L-functions to have.

Theorem 3.12. *Let $\rho : \mathrm{Gal}(L/K) \to \mathrm{GL}_n(\mathbb{C})$ be a Galois representation. Then there is a function $L_\infty(\rho, s)$ (discussed below) and an integer $c(\rho)$ such that the completed L-function*

$$\Lambda(\rho, s) = c(\rho)^{s/2} L(\rho, s) L_\infty(\rho, s)$$

has a meromorphic continuation to $\mathbb{C}$, and

$$\Lambda(\rho, s) = W(\rho)\Lambda(\overline{\rho}, 1 - s)$$

where $\overline{\rho}$ is complex conjugate of ρ and $W(\rho) \in S^1 \subseteq \mathbb{C}^\times$ is a complex number of modulus 1.

Why is $\Lambda(\rho, s)$ called the completed L-function? We'll give a brief explanation here without any details. The idea is that $L(\rho, s)$ is missing some factors. Primes of K correspond to absolute values $|\cdot|_{\mathfrak{p}}$ on K, but they give only the nonarchimedean ones. There are also some archimedean absolute values on K, and they are all induced by the absolute value on $\mathbb{C}$ via embeddings $K \hookrightarrow \mathbb{C}$. We thus define an *infinite prime* $\mathfrak{p}$ of K to be an archimedean absolute value on K. We then define local factors $L_{\mathfrak{p}}(\rho, s)$ at each infinite prime to be certain functions involving powers of π and gamma functions, and $L_\infty(\rho, s)$ is the product of these. On the other hand, the conductor is a measure of ramification that's needed to make the functional equation work.

Remark 3.13. The proof of theorem 3.12 goes by reducing to the case $n = 1$, in which case the L-function is a Dirichlet L-function. By remark 3.7, such an L-function is also associated to a Hecke character. Then in the case of an L-function associated to a Hecke character, more tools are available that enable a proof of the theorem. More generally, L-functions of automorphic objects are easier to study, and more is known about them. So when studying a Galois representation, it is useful to show that its L-function comes from an automorphic object. The Modularity Theorem says that this works for any Galois representation coming from an elliptic curve over $\mathbb{Q}$, where the automorphic object is a cusp form.

3.2 L-functions of compatible systems of ℓ-adic representations

Before defining compatible systems of ℓ-adic representations, we observe some compatibility properties of the ℓ-adic cyclotomic characters χ_ℓ as ℓ varies.

- χ_ℓ is unramified at all primes $p \nmid \ell$.
- For $\ell \neq p$, the value $\chi_\ell(\sigma_p) = p \in \mathbb{Q}_\ell^\times$ actually lies in $\mathbb{Q}^\times$ and is independent of ℓ. In particular, the characteristic polynomial $\det(1 - T\chi_\ell(\sigma_p)) = 1 - pT \in \mathbb{Q}_\ell[T]$ lies in $\mathbb{Q}[T]$ and is independent of $\ell \neq p$.

A compatible system of ℓ-adic representations is a system $\{\rho_\ell\}_\ell$ of Galois representations satisfying these properties.

Definition 3.14. Fix $n \geq 1$. For each prime ℓ, let $\rho_\ell : G_{\mathbb{Q}} \to \mathrm{GL}_n(\mathbb{Q}_\ell)$ be an ℓ-adic Galois representation. We say that $\{\rho_\ell\}_\ell$ is a *compatible system of ℓ-adic representations* if the following conditions are satisfied.

(1) There is a finite set S of primes so that each ρ_ℓ is unramified at all $p \notin S \cup \{\ell\}$.

(2) For each prime p, polynomial $\det(1 - T\sigma_p|\rho_\ell^{I_p}) \in \mathbb{Q}_\ell[T]$ lies in $\mathbb{Q}[T]$ and does not depend on $\ell \neq p$.

If $\rho = \{\rho_\ell\}$ is a compatible system of ℓ-adic representations, then we have associated local L-factors

$$L_p(\rho, T) = \frac{1}{\det(1 - T\sigma_p|\rho_\ell^{I_p})}$$

independent of the choice of $\ell \neq p$, and an L-function

$$L(\rho, s) = \prod_p L_p(\rho, p^{-s}).$$

Example 3.15. As observed above, $\chi = \{\chi_\ell\}$ provides a compatible system of ℓ-adic representations. The L-function is

$$L(\chi, s) = \prod_p \frac{1}{1 - p^{1-s}} = \zeta(s - 1).$$

Remark 3.16. What we would really like is a so-called *global* Galois representation $\rho : G_\mathbb{Q} \to \mathrm{GL}_n(\mathbb{Q})$. This is global in the sense that it gives rise to ℓ-adic Galois representations via $G_\mathbb{Q} \xrightarrow{\rho} \mathrm{GL}_n(\mathbb{Q}) \hookrightarrow \mathrm{GL}_n(\mathbb{Q}_\ell)$, which are clearly compatible in the sense of part (2) of definition 3.14. Thus if ρ is unramified at all but finitely many primes, it gives rise to a compatible system of ℓ-adic Galois representations. However, we can not run this process in reverse: compatible systems do not all come from global representations.

Compatible systems of ℓ-adic Galois representations are interesting objects that arise naturally from geometry. For example, the *Tate modules* $V_\ell(E)$ of an elliptic curve $E/\mathbb{Q}$ give such a system, and the L-function of E is the L-function of said compatible system. As mentioned earlier, the L-functions of compatible systems are also much more difficult to study; it is not known that they have meromorphic continuations and functional equations. As in remark 3.13, our best strategy of studying such L-functions is to show that they also arise as L-functions of automorphic objects (like Hecke characters or modular forms), and use the general theory for these easier-to-study L-functions. The Modularity Theorem says that this approach works for elliptic curves $E/\mathbb{Q}$.