I. Galois Representations

We skip 9.1, and check there fore definitions

Definition I.0.1

Let ℓ be a prime. The ring of ℓ-adic integers is

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

along $\mathbb{Z}/\ell^m\mathbb{Z} \to \mathbb{Z}/\ell^n\mathbb{Z}$.

Explicitly, $a \in \mathbb{Z}_\ell$ si a sequence $a = (a_1, a_2, \ldots)$ with $a_n \in \mathbb{Z}/\ell^n\mathbb{Z}$ and $a_{n+1} \equiv a_n \pmod{\ell}^n$.

Note $\mathbb{Z}_\ell$ is an integral domain and the natural map

$$\mathbb{Z} \to \mathbb{Z}_\ell$$
$$a \mapsto (a + \ell\mathbb{Z}, a + \ell^2\mathbb{Z}, \ldots)$$

is injective. This inclusion induces

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

for every n. Then $\mathbb{Z}_\ell$ is profinite because $\mathbb{Z}/\ell^n\mathbb{Z}$ is finite for all n.

The group of units $\mathbb{Z}_\ell^\times$ is

$$\begin{aligned}\mathbb{Z}_\ell^\times &= \{(a_1, a_2, \ldots) \mid a_i \in (\mathbb{Z}/\ell^i\mathbb{Z})^\times\} \\ &= (a_1, a_2, \ldots) \mid a_1 \not\equiv 0\}.\end{aligned}$$

Also $\mathbb{Z}_\ell$ has a unique maximal ideal $\ell\mathbb{Z}_\ell$. Furthermore, it comes equipped with a topology with basis given by the sets

$$U_x(n) \coloneqq x + \ell^n\mathbb{Z}_\ell,$$

where $n \in \mathbb{Z}^+$.

Definition I.0.2

The field $\mathbb{Q}_\ell$ is the fraction field of $\mathbb{Z}_\ell$.

$\mathbb{Q}_\ell$ has a topology given in the same way. The basis is

$$U_x(n) = x + \ell^n\mathbb{Z}_\ell$$

for $x \in \mathbb{Q}_\ell, n \in \mathbb{Z}^+$. For any $d > 0$, $\mathbb{Q}_\ell^d$ is a topological $\mathbb{Q}_\ell$-vector space with the product topology. The group $\mathrm{GL}_d(\mathbb{Q}_\ell)$ inherits the subspace topology from $\mathbb{Q}_\ell^{d^2}$. Under this topology, matrix multiplication and inversion are continuous (i.e. $\mathrm{GL}_d(\mathbb{Q}_\ell)$ is a topological group).

Now let K be a number field ($K \subseteq \overline{\mathbb{Q}}, [K : \mathbb{Q}] < \infty$) with ring of integers $\mathcal{O}_K$. If λ is a prime in $\mathcal{O}_K$ over ℓ, then we can play the same game:

$$\mathcal{O}_{K,\lambda} = \varprojlim_n \mathcal{O}_K/\lambda^n\mathcal{O}_K,$$

and similarly define $K_\lambda = \mathrm{Frac}(\mathcal{O}_{k,\lambda})$. Then we have

$$\mathbb{Q}_\ell \hookrightarrow, \mathbb{Z}_\ell \hookrightarrow \mathcal{O}_{K,\lambda}, K \otimes_{\mathbb{Q}} \mathbb{Q}_\ell \cong \prod_{\lambda|\ell} K_\lambda,$$

with the proof in the book.

Galois Representations:

- Let $\overline{\mathbb{Q}}$ be the algebraic closure of $\mathbb{Q}$.
- Define $G_{\mathbb{Q}} = \mathrm{Aut}(\overline{\mathbb{Q}})$.
- We want to study representations of $G_{\mathbb{Q}}$ on $\mathbb{Q}_\ell$-vector spaces.
- Recall that

$$\overline{\mathbb{Q}} = \bigcup_{\substack{K/\mathbb{Q} \\ [K:\mathbb{Q}]<\infty \\ K \text{ Galois}}} K.$$

Then for any $\sigma \in G_{\mathbb{Q}}$ and any $K/\mathbb{Q}$ Galois of finite degree, we have $\sigma\big|_K \in \mathrm{Gal}(K/\mathbb{Q})$. This defines a compatible system of surjections

$$G_{\mathbb{Q}} \twoheadrightarrow \mathrm{Gal}(K/\mathbb{Q}),$$

compatible in the sense that if $K' \subseteq K$ we have a commutative diagram

$$\begin{array}{ccc} G_{\mathbb{Q}} & \twoheadrightarrow & \mathrm{Gal}(K/\mathbb{Q}) \\ & \searrow & \downarrow \\ & & \mathrm{Gal}(K'/\mathbb{Q}) \end{array}$$

So really we have that

$$G_{\mathbb{Q}} = \varprojlim_{\substack{K/\mathbb{Q} \\ \text{fin. Galois}}} \mathrm{Gal}(K/\mathbb{Q}).$$

This has a natural topology

Definition I.0.3

The Krull topology on $G_{\mathbb{Q}}$ has basis sets

$$U_\sigma(K) = \{\sigma\tau \mid \tau\big|_K = \mathrm{Id}_K\}.$$

Let's discuss some important elements of $G_{\mathbb{Q}}$. Fix a prime p, $\mathfrak{p} \subseteq \overline{\mathbb{Z}}$ lying over p.

Definition I.0.4

The decomposition group of $\mathfrak{p}$ is

$$D_{\mathfrak{p}} = \{\sigma \in G_{\mathbb{Q}} \mid \mathfrak{p}^\sigma = \sigma\}.$$

We then have a surjective map $D_{\mathfrak{p}} \twoheadrightarrow \mathrm{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p)$ given by

$$\sigma \mapsto (x + \mathfrak{p} \mapsto x^\sigma + \mathfrak{p}).$$

Definition I.0.5

An absolute Frobenius over p is any preimage $\text{Frob}_\mathfrak{p} \in D_\mathfrak{p}$ of the Frobenius map $\sigma_p \in G_{\mathbb{F}_p}$, where $\sigma_p(x) = x^p$.

This is well-defined up to $I_\mathfrak{p} \coloneqq \ker(D_\mathfrak{p} \to G_{\mathbb{F}_p})$, which we call the inertia group of $\mathfrak{p}$.

Explicitly,

$$I_\mathfrak{p} \coloneqq \{\sigma \in D_\mathfrak{p} \mid x^\sigma \equiv x \pmod{\mathfrak{p}}, \text{ for all } x \in \overline{\mathbb{Z}}\}.$$

Theorem I.0.1

Fix a finite set of primes $S \subseteq \mathbb{Z}$. For each prime $\mathfrak{p}$ lying over $p \notin S$, choose an absolute Frobenius $\text{Frob}_\mathfrak{p}$. Then the set

$$\{\text{Frob}_\mathfrak{p} \mid p \notin S\}$$

is dense for the Krull topology.

Proof. We use Tchebotarov Density Theorem (stated below) to prove this theorem.

take $U_\sigma(K)$ for some $\sigma \in G_\mathbb{Q}$ and K some number field. We want to show $\text{Frob}_\mathfrak{p} \in U_\sigma(K)$.

Consider $\sigma\big|_L \in \text{Gal}(K/\mathbb{Q})$. By Tchebotarov, σ is a Frobenius for some $\mathfrak{p}_K$. Lift $\mathfrak{p}_K$ to $\mathfrak{p} \subseteq \overline{\mathbb{Z}}$.

Then $\text{Frob}_\mathfrak{p} \in U_\sigma(K)$.

Theorem I.0.2 (Tchebotarov Density Theorem 9.1.2 in [DS05])

Let K be a Galois number field. Then every element of $\text{Gal}(K/\mathbb{Q})$ is a Frobenius for $\mathfrak{p}$ for infinitely many maximal ideals $\mathfrak{p}$ of $\mathcal{O}_K$.

Here we mean $x^\sigma \equiv x \pmod{\mathfrak{p}}$ for all $x \in \mathcal{O}_K$.

Definition I.0.6

Let $d > 0$. A d-dimensional Galois representation is a continuous homomorphism

$$\rho : G_\mathbb{Q} \to \text{GL}_d(L)$$

for L a finite extension of $\mathbb{Q}_\ell$.

Remark I.0.1

$L = K_\lambda$ for some λ, K works. If ρ, ρ' are two Galois representations then we say $\rho \sim \rho'$ if there exists some $g \in \text{GL}_d(L)$ so that

$$\rho'(\sigma) = g^{-1}\rho(\sigma)g$$

for all $\sigma \in G_\mathbb{Q}$. One can think of this as a commutative diagram.

Example I.0.1

Fix $n > 0$, let μ_{ℓ^n} be a primitive ℓ^n-th root of unity (say $e^{2\pi i/\ell^n}$). Then $\mathbb{Q}(\mu_{\ell^n})$ is a Galois number field of degree $\phi(\ell^n)$ over $\mathbb{Q}$, and we have a canonical isomorphism

$$\text{Gal}(\mathbb{Q}(\mu_{\ell^n})/\mathbb{Q}) \xrightarrow{\sim} (\mathbb{Z}/\ell^n\mathbb{Z})^\times$$

$$(\mu_{\ell^n} \xrightarrow{\sigma} \mu_{\ell^n}^a) \mapsto a \pmod{\ell^n}.$$

If we define

$$\mathbb{Q}(\mu_{\ell^\infty}) = \bigcup_{n=1}^{\infty} \mathbb{Q}(\mu_{\ell^n})$$

then

$$G_{\mathbb{Q},\ell} := \mathrm{Aut}(\mathbb{Q}(\mu_{\ell^\infty})) \xrightarrow{s} \varprojlim (\mathbb{Z}/\ell^n\mathbb{Z})^\times = \mathbb{Z}_\ell^\times.$$

The inclusion $\mathbb{Q}(\mu_\ell^\infty) \subseteq \overline{\mathbb{Q}}$ induces $G_\mathbb{Q} \twoheadrightarrow G_{\mathbb{Q},\ell}$ by restriction.

Then we have a representaiton

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

This is a Galois representation (check continuity). This is called the ℓ-adic cyclotomic character χ_ℓ.

Claim

χ_ℓ is continuous.

Proof. Since χ_ℓ is a group homomorphism, it suffices to show that $\chi_\ell^{-1}(U_1(n))$ is open (aka look at neighborhoods of identity). Explicitly we see that

$$\begin{aligned}\chi_\ell^{-1}(U_1(n)) &= \{\sigma \mid \chi_\ell(\sigma) \in 1 + \ell^n\mathbb{Z}_\ell\} \\ &= \{\sigma \in G_\mathbb{Q} \mid \sigma\big|_{\mathbb{Q}(\mu_{\ell^n})} = \mathrm{Id}\}.\end{aligned}$$

But this is simply $U_{\mathrm{Id}}(\mathbb{Q}(\mu_{\ell^n}))$ which is open.

Exercise I.0.2

Compute that $\chi_\ell(\mathrm{Frob}_\mathfrak{p}) = p$. In [DS05] This is 9.3.6.

We want to think more generally about $\rho(\mathrm{Frob}_\mathfrak{p})$

Problem: $\mathrm{Frob}_\mathfrak{p}$ is only well-defined up to inertia.

Definition I.0.7

Let ρ be a Galois representaton and p a prime. Then ρ is unramified at p if $I_\mathfrak{p} \subseteq \ker \rho$ for any $\rho \subseteq \overline{\mathbb{Z}}$ lying over p.

Example I.0.3

χ_ℓ is unramified at p since p is unramified in $\mathbb{Q}(\mu_{\ell^n})$, so $I_\mathfrak{p}$ acts trivially on $\mathbb{Q}(\mu_{\ell^n})$.

We can give an equivalent definition of Galois representation

Definition I.0.8

Let $d > 0$. A d-dimensional Galois representation is a d-dimensional topological vector space V over L, where $[L : \mathbb{Q}_\ell] < \infty$ that is also a $G_\mathbb{Q}$-module such that the map

$$\begin{aligned}V \times G_\mathbb{Q} &\to V \\ (v, \sigma) &\mapsto v^\sigma\end{aligned}$$

is continuous.

Remark I.0.2

We say $V \sim V'$ if there exists a continuous $G_{\mathbb{Q}}$-module isomorphism $V \to V'$ of L-vector spaces.

We can realize χ_ℓ in this way. Define

$$C = \mathrm{Spec}(\mathbb{Q}[x,y]/(xy-1))$$

This is a curve, and for any $\mathbb{Q}$-algebra R, the R-points of C are $C(R) = \{(a,b) \in R^2 \mid ab = 1\}$. This is isomorphic to $R^\times$.

Thus C has the structure of a "$\mathbb{Q}$-group scheme." For $n \in \mathbb{Z}^+$, define

$$C[\ell^n] = \{a \in C(\overline{\mathbb{Q}}) \mid a^{\ell^n} - 1 = 0\} \subseteq \overline{\mathbb{Q}}^\times.$$

Then we have an isomorphism

$$C[\ell^n] \xrightarrow{\sim} \mathbb{Z}/\ell^n\mathbb{Z}$$
$$\mu_{\ell^n}^a \mapsto a.$$

Furthermore $\mathrm{Aut}(C[\ell^n]) \cong (\mathbb{Z}/\ell^n\mathbb{Z})^\times$ in the natural way.

Definition I.0.9

The ℓ-adic Tate module of C is

$$T_\ell(C) = \varprojlim_n C[\ell^n].$$

We have an induced isomorphism ψ from $T_\ell(C)$ to $\mathbb{Z}_\ell$. $T_\ell(C)$ carries an action of $G_{\mathbb{Q},\ell}$ because $\mathrm{Aut}(C[\ell^n]) = \mathrm{Gal}(\mathbb{Q}(\mu_{\ell^n})/\mathbb{Q})$ as $C[\ell^n] = \mathbb{Q}(\mu_{\ell^n})$.

We can also define

$$V_\ell(C) \coloneqq T_\ell(C) \otimes_{\mathbb{Z}} \mathbb{Q}.$$

We get

$$V_\ell(C) \times G_{\mathbb{Q}} \to V_\ell(C)$$

which is compatible with our previous construction.