Seminar Talk: Galois Representations

Definition Let K be a field and $\overline{K}$ a fixed algebraic closure of K. Then we call the group $G_K := \mathrm{Gal}(\overline{K}/K)$ the *absolute Galois group* of K.

Note that for a different algebraic closure $\overline{K}'$, the corresponding group $\mathrm{Gal}(\overline{K}'/K)$ is isomorphic to G_K.

As the talk will treat different objects definded via limits, we recall the definition of an inductive limit:

Definition Let I be a small category (i. e. objects and morphisms are sets), $\mathcal{C}$ be an arbritary category, $F : I \to \mathcal{C}$ a functor and write X_i for the image of $i \in I$ under F. Then the *projective limit* of F (if it exists) is an object

$$\varprojlim_{i \in I} X_i$$

together with morphisms

$$(\rho_j : \varprojlim_{i \in I} X_i \to X_j)_{j \in I}$$

so that for every object $T \in \mathrm{Ob}(\mathcal{C})$ the map

$$\begin{aligned} \rho_j \circ : \mathrm{Hom}(T, \varprojlim_{i \in I} X_i) &\longrightarrow \{f_j : T \to X_j \mid F(\phi) \circ f_i = f_j \text{ for all } (\phi : i \to j) \in I\} \\ g &\longmapsto \rho_j \circ g \end{aligned}$$

is an isomorphism.

We can write the absolute Galois group as a limit:

$$\mathrm{Gal}(\overline{K}/K) = \varprojlim_{L/K} \mathrm{Gal}(L/K)$$

where $I = \mathrm{gal}_K^{\mathrm{op}}$ is the opposite category of finite galois extensions of K, i.e.

$$\begin{aligned} \mathrm{Ob}(I) &= \{L \text{ a field } \mid L/K \text{ Galois and finite } \}, \\ \mathrm{Mor}_I(L, L') &= \begin{cases} \{1\} & \text{if } L' \subseteq L \\ \emptyset & \text{otherwise} \end{cases} . \end{aligned}$$

Writing the Group as a projective limit endows it with a topology compatible with the group structure, called the *Krull topology*, so that it has the structure of a topological group, i. e. composition and the inverse map are continuous). The open subgroups are of the form $\mathrm{Gal}(\overline{K}/L)$, where L/K is a finite Galois extension.

As G_K is a fairly complicated group, we have to develop some tools to study it. One important approach is to use Galois representations.

Definition A *Galois representation* (of dimension n) is a continuous homomorphism

$$\rho : \mathrm{Gal}(\overline{K}/K) \longrightarrow \mathrm{GL}_n(F),$$

where F is a topological field (i. e. $(F,+)$ and $(F \setminus \{0\}, \cdot)$ are topological groups. The topology on $\mathrm{GL}_n(F)$ is induced by the topology F by considering $\mathrm{GL}_n(F)$ as the complement of the open subset

$\{M \mid det(M) = 0\} \subseteq \mathrm{Mat}_{n\times n}(F) \cong F^{n^2}$,

where F^{n^2} has the canonical topology.

Definition ρ is *unramified* at a prime $\mathfrak{p}$ of K if it factors as

$$\begin{tikzcd} \mathrm{Gal}(\overline{K}/K) \arrow[rr, "\rho"] \arrow[dr, "\mathrm{res}"'] & & \mathrm{GL}_n(F) \\ & \mathrm{Gal}(L/K) \arrow[ur] & \end{tikzcd}$$

for some Galois extension L/K (infinite extensions are allowed).

Recall the definition of the Frobenius automorphism:

For a Galois extension L/K, $\mathfrak{p}$ a prime of K taht is unramified in L, P a prime in L above $\mathfrak{p}$, we define $\mathrm{Frob}_{P|\mathfrak{p}}$ as

$$\mathrm{Frob}_{P|\mathfrak{p}}(x) \equiv x^{N_{\mathfrak{p}}} \mathrm{mod} P \text{ for all } x \in \mathcal{O}_L$$

and we can easily see that two Frobenius automorphisms for different primes P, P' above $\mathfrak{p}$ are conjugate in $\mathrm{Gal}(L/K)$, so that we get a well-defined conjugacy class $[\rho(\mathrm{Frob}_{\mathfrak{p}}]$.

If ρ is unramified, the class $[\rho(\mathrm{Frob}_{\mathfrak{p}}] \subseteq \mathrm{GL}_n(F)$ is well-defined.

This notion allows us to formulate a more general statement as question B:

Question C Given a Galios representation $\rho : G_K \to \mathrm{GL}_n(F)$, is there a rule to determine the conjugacy class of $\rho(\mathrm{Frob}_{\mathfrak{p}})$ for $\mathfrak{p}$ an unramified prime of K?

Definition If the field F is equal to the complex numbers equipped with the discrete topology, a Galois representation $\rho : G_K \to \mathrm{GL}_n(\mathbb{C})$ is called *Artin representation*.

Note that images of Artin representations are finite, as $\rho^{-1}(\mathrm{id})$ is open. Therefore they factor through representations of finite groups $\mathrm{Gal}(L/K)$, where L/K is a finite Galois extension.

Finding an answer for Question C would also answer Question B, als for L/K finite and Galois, we can find an Artin representation ρ with $\mathrm{Ker}(\rho) = \mathrm{Gal}(\overline{K}/L)$, so that $\mathfrak{p}$ splits in L if and only if $[\rho(\mathrm{Frob}_{\mathfrak{p}}]$ is trivial.

Example If $n = 1$, we have $\mathrm{GL}_1(\mathbb{C}) = \mathbb{C}^*$, so an Artin representation of dimension one is just a continuous homomorphism $\rho : G_K \to \mathbb{C}^*$. By the Kronecker-Weber Theorem (every number field is contained in a cyclotomic field) we know that there ist some m so that ρ factors through $\mathrm{Gal}\mathbb{Q}(\zeta_m)/\mathbb{Q}) \cong (\mathbb{Z}/m\mathbb{Z})^*$. Thus we get a corresponence

$$\{\text{one-dimensional artin representations}\} \longleftrightarrow \{\text{Dirlichet Characters}\}\chi : (\mathbb{Z}/m\mathbb{Z})^*$$
$$\rho \longmapsto \chi \textit{ with } \chi(\mathfrak{p}) = \rho(\mathrm{Frob}_{\mathfrak{p}}).$$

Example For $L = \mathbb{Q}(i, \sqrt[4]{2})$, the splitting field of the polynomial $x^4 - 2$ oder $\mathbb{Q}$, we know that the Galois group is isomorphis to the dihedral group D_8 that is generated by the two elements r and s, with

$$\begin{aligned} r(\sqrt[4]{2})) &= i\sqrt[4]{2}), \\ r(i) &= i, \\ s(\sqrt[4]{2})) &= \sqrt[4]{2}), \\ s(i) &= -i. \end{aligned}$$

We have $r^4 = 1, s^2 = 1, srs^{-1} = r^{-1}$. We get a two-dimensional Artin representation

$$\begin{tikzcd} \mathrm{Gal}(\overline{\mathbb{Q}}/Q) \arrow[rr, "\rho"] \arrow[dr, "\mathrm{res}"] & & \mathrm{GL}_2(\mathbb{C}) \\ & \mathrm{Gal}(L/\mathbb{Q}) \cong D_8 \arrow[ur] & \end{tikzcd}$$

via $\rho(r) = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \rho(s) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.

Fact We have

$$[\rho(\mathrm{Frob}_{\mathfrak{p}}] = \begin{cases} 1 & \text{if } p = a^2 64 b^2 \\ r^2 & \text{if } p = a^2 + 16b^2, b \text{ odd} \\ rs & \text{if } p \equiv 3(8) \\ r & \text{if } p \equiv 5(8) \\ s & \text{if } p \equiv 7(8) \end{cases},$$

so that

$$tr(\rho(\mathrm{Frob}_{\mathfrak{p}}) = \begin{cases} 2 & \text{if } p = a^2 64 b^2 \\ -2 & \text{if } p = a^2 + 16b^2, b \text{ odd} \\ 0 & \text{otherwise} \end{cases}.$$

Example If we take some prime $p \equiv 1(8)$, we know by the quartic reciproctiy law that 2 is a quadratic, but not biquadratic residue mod p, so we get the following splitting behaviour:

$\mathbb{Q}(i, \sqrt[4]{2})$	$\mathfrak{p}_1$	$\mathfrak{p}_2$
$\mathbb{Q}(i, \sqrt{2})$	$\mathfrak{p}_1$	$\mathfrak{p}_2$
$\mathbb{Q}(i)$	$\mathfrak{p}_1$	$\mathfrak{p}_2$
$\mathbb{Q}$	p	

The fact stated above can be proven by using the quadratic reciprocity law.

Recall The set of rational primes p so that a polynomial $f \in \mathbb{Q}[x]$ irreducible splits completely has a density that is $(\#G)^{-1}, G = \mathrm{Gal}(\mathbb{Q}[x]/(f)/\mathbb{Q})$. If we define $G_0 := \{\sigma \in G \mid \sigma \text{ has no sulutions mod } p\}$ has a density equal to $\#G_0/\#G$.

For $f \in \mathbb{Z}[x]$, p prime, we denote by $N_p(f)$ the number of zeros of f in $\mathbb{F}_p$ (counted without multiplicity).

Example We want to compute $N_p(f)$ for $f(x) = x^n - x - 1$.

In the case $n = 2$, the discriminant of f is 5, so we can conclude $N_5(f) = 1$.

If $p \neq 5$, we have

$$N_p(f) = \begin{cases} 2 & \text{if 5 is a square mod } p \\ 0 & \text{otherwise} \end{cases} = \begin{cases} 2 & \text{if } p \equiv \pm 1 \text{ mod } p \\ 0 & \text{if } p \equiv \pm 2 \text{ mod } p \end{cases}$$

because for $p \neq 2$, the roots of f in $\overline{\mathbf{F}_p}$ are $(1 \pm \sqrt{p})/2$. The second equality is just quadratic reciprocity.

In the case $n = 3$, we write $E = \mathbb{Q}[x]/(f)$, L a Galois closure of E. The Galois group is $\mathrm{Gal}(L/\mathbb{Q}) = S_3$. We know the discriminant of f is -23, so that L contains the field $K = \mathbb{Q}(\sqrt{-23})$ and L is a cubic extension of K.

If $p \neq 23$, let Frob_p be the Frobenius substitution of p in S_3. As we know there is a unique quadratic character associated to $K/\mathbb{Q}$, we know $\mathrm{sgn}(\mathrm{Frob}_p) = \varepsilon$, where $\varepsilon(q) = \left(\frac{q}{23}\right)$. This implies that Frob_p is a transposition if $\left(\frac{p}{23}\right) = -1$, so we have $N_p(f) = 1$ in this case.

If $\left(\frac{p}{23}\right) = 1$, Frob_p has either order 1 or 3, so $N_p(f) = 1$ or 3.

To distinguish these cases, we decompose $p = \mathfrak{p}_1\mathfrak{p}_2 \in K$. By the coresondence between ideal classes and binary quadratic forms we know that $\mathfrak{p}_1$ is principial if and only if we can write $p = a^2 + ab + 6b^2$ with $a, b \in \mathbb{Z}$. In the other case we can write $p = 2a^2 + ab + 3b$, and as a result we get

$$N_p(f) = \begin{cases} 3 & \text{if } p = a^2 + ab + 6b^2 \\ 0 & \text{if } p = 2a^2 + ab + 3b \\ 1 & \text{if } \left(\frac{p}{23}\right) = -1 \end{cases}.$$

Definition If F is the field of the $p-$adic numbers, equipped with the p-adic topology, a Galois representation $\rho : G_K \to \mathrm{GL}_n(\mathbb{Q}_p)$ is called *p-adic Galois representatnion.*

Recall The p-adic integers are defined as the projective limit

$$\varprojlim_{m \in \mathbb{N}} \mathbb{Z}/p^m\mathbb{Z},$$

where the limit runs over all positive integers and we have a morphism from $\mathbb{Z}/p^m\mathbb{Z}$ to $\mathbb{Z}/p^{m'}\mathbb{Z}$ if and only if $m \leq m'$, and that morphism is just the inclusion.

Alternatively, they can be defined as the completion of $\mathbb{Z}$ with respect to the p-adic absolute value

$$\mid n \mid_p := \begin{cases} \max\{k : p^k \mid n\} & \text{if } n \neq 0 \\ 0 & \text{if } n = 0 \end{cases}.$$

We then define the p-adic numbers to be the fraction field of the p-adic integers. On those we define the p-adic norm: For any $x \in \mathbb{Q}_p \setminus \{0\}$ there is a unique n so that $x = p^n \frac{a}{b}$, so that p does not divide a and b, and we define

$$\mid x \mid_p := \begin{cases} p^{-n} & \text{if } x \neq 0 \\ 0 & \text{if } x = 0 \end{cases} .$$

Remark Every nonzero p-adic integer a can be written uniquely as

$$a = a_0 + a_1 p + ... + a_{n-1} p^{n-1} \in \mathbb{Z}_p^*$$

with $a_i < p$ for all i.

Example The p-adic cyclotomic character is the one-dimensional representation

$$\begin{tikzcd} \mathrm{Gal}(\overline{\mathbb{Q}}/Q) \arrow[rr, "\rho_{\mathrm{cycl}}"] \arrow[dr, "\mathrm{res}"'] & & \mathbb{Q}_p^* \cong \mathrm{GL}_1(\mathbb{Q}_p) \\ & \mathrm{Gal}(\mathbb{Q}_p/\mathbb{Q}) \cong \mathbb{Z}_p^* \arrow[ur] & \end{tikzcd}$$

given by $\rho_{\mathrm{cycl}}(\sigma) = a = a_0 + a_1 p + ... + a_{n-1} p^{n-1}$ for

$$\sigma(\zeta_{p^n}) = \zeta_{p^n}^{a_0 + a_1 p + ... + a_{n-1} p^{n-1}}$$

We know that the only prime ramified in $\mathbb{Q}_p/\mathbb{Q}$ is p. For $l \neq p$ prime, we have

$$\mathrm{Frob}_l(\zeta_{p^n}) = \zeta_{p^n}^l$$

and therefore $\rho_{\mathrm{cy\,cl}}(\mathrm{Frob}_p = l$.

Artin representations coming from geometry Let $f(x) = x^3 + ax + b \in \mathbb{Q}[x]$, E the elliptic curve given by $y^2 = f(x)$, i.e.

$$E = \mathrm{Proj}\mathbb{Q}[X, Y, Z]/(Y^2 Z - X^3 - aXZ^2 - bZ^3)$$

E is an abelian scheme with the well-known group law on $E(L)$ for any field extension L/K. The multiplication by $m \in \mathbb{Z}$, denoted by $[m]$ is a group homomorphism.

We define the m-torsion points to be

$$E[m] = \{P \in E(\overline{\mathbb{Q}} \mid [m](P) = \mathcal{O}\} = \mathrm{Ker}([m]),$$

where $\mathcal{O} = (0 : 1 : 0)$ is the point at infinity. $E[m]$ is a subgroup of $E(\mathbb{Q}$ as it is the kernel of a homomorpism.

We have $E \cong (Z/m\mathbb{Z})^2$ as groups because $E[m]$ is a free $\mathbb{Z}/M\mathbb{Z}$-module of rank two.

Why is this the case?

We know that over $\mathbb{C}$, every elliptic curve can be written as

$$(E[m], +) \cong (\mathbb{C}/L, +),$$

where $L \subseteq \mathbb{C}$ is a lattice, i. e. a free abelian group of rank two, so that $\mathbb{C}/L$ is compact.

For a class of complex numbers $[z]$ corresponding to a point $P \in E$ we have $[m]P = [m][z] = [mz]$, because

$$\mathrm{Ker}(\mathbb{C}/L \to \mathbb{C}/L) = \{z \in \mathbb{C} \mid [m]z \in L\} = (\frac{1}{m}L)/L \cong L/mL \cong \mathbb{Z}^2/m\mathbb{Z}^2 \cong (\mathbb{Z}/m\mathbb{Z})^2,$$

because $L \cong \mathbb{Z}^2$.

This implies $E[m](\mathbb{C}) = E[m](\overline{\mathbb{Q}}) \cong (\mathbb{Z}/m\mathbb{Z})^2$ because all points on the curve satisfy an algebraic equation.

Consider the action of G_K on $E[p^n]$:

$$G_Q \times E[p^n] \longrightarrow E[p^n](\sigma, P) \quad \longmapsto P^\sigma := (\sigma(x), \sigma(y)) \text{ for } P = (x, y)\mathcal{O} \longmapsto \mathcal{O}$$

This action is well-defined because $(\sigma x)^3 = a(\sigma x) + b = \sigma(x^3 + ax + b) = \sigma(y^2) = \sigma(y)^2$.

This action gives us a Galois representation $\rho_m : G_K \to \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$ and we have a chain

$$... \longrightarrow E[p^r] \xrightarrow{[p]} E[p^{r+1}] \longrightarrow ...$$

We define the *Tate module* to be the projective limit

$$\varprojlim_{m \in \mathbb{N}} (E[p^m], [p]).$$

It is a free module over

$$\varprojlim_{m \in \mathbb{N}} \mathbb{Z}/m\mathbb{Z} = \mathbb{Z}_p.$$

We write

$$T_pE := \varprojlim_{m \in \mathbb{N}} E[p^m] \cong \mathbb{Z}_p^2$$

The Tate module acts on $G_\mathbb{Q}$ and we obtain a Galois representation

$$\begin{tikzcd}
\mathrm{Gal}(\overline{\mathbb{Q}}/K) \arrow[rr, "\rho"] \arrow[dr, "\mathrm{act}"'] & & \mathrm{GL}_2(\mathbb{Q}_p) \\
& \mathrm{Aut}(T_pE) \cong \mathrm{GL}_2(\mathbb{Z}_p) \arrow[ur] &
\end{tikzcd}$$

This ρ is unramified at all primes l not dividing $p\Delta$, $\Delta = \mathrm{disc}(f(x))$. The caracteristic polynomial of $\rho\mathrm{Frob}_l$ is

$$\det(x\mathrm{Id} - \rho(\mathrm{Frob}_l)) = x^2 - (l + 1 + N_l)x + l,$$

where $N_l = \#E(\mathbf{F}_l)$.