Modular Galois Representations and Applications

4 Lectures held at the Higher School of Economics in Moscow, 2–4 April 2013

Gabor Wiese
Université du Luxembourg
gabor.wiese@uni.lu

Version of 6th April 2013

Lecture 1

Representations of profinite groups

In this lecture we will

- recall finite Galois theory,
- prove infinite Galois theory,
- introduce profinite groups,
- introduce representations of profinite groups, and
- state some of their properties.

1 Profinite groups and infinite Galois theory

A good reference for profinite groups and infinite Galois theory is [Neukirch], Section IV.1.

Finite Galois theory

Let L/K be a field extension, that is, L is a field and K is a subfield of L. By restricting the multiplication map $L \times L \to L$ to $K \times L \to L$, we obtain a K-scalar multiplication on L, making L into a K-vector space. The *degree* of the field extension L/K is the K-dimension of L, notation:

$$[L : K] := \dim_K L.$$

A field extension is called *finite* if its degree is finite.

Let us look at some examples:

(a) $\mathbb{C}/\mathbb{R}$ is a field extension of degree 2 and an $\mathbb{R}$-basis of $\mathbb{C}$ is given by 1 and i.

(b) $\mathbb{F}_{p^n}/\mathbb{F}_p$ is a field extension of degree n, where $\mathbb{F}_{p^n}$ is the finite field with p^n elements (it is unique up to isomorphism as it is the splitting field of the polynomial $X^{p^n} - X \in \mathbb{F}_p[X]$ over $\mathbb{F}_p$).

(c) $\mathbb{C}/\mathbb{Q}$ is a field extension of infinite degree.

(d) $\overline{\mathbb{F}}_p/\mathbb{F}_p$ is an infinite field extension, where $\overline{\mathbb{F}}_p$ is an algebraic closure of $\mathbb{F}_p$.

We denote by $\mathrm{Aut}_K(L)$ the group of field automorphisms $\sigma : L \to L$ such that their restriction to K is the identity (note that any field homomorphism is automatically injective, since kernels are ideals and the only nontrivial ideals in a field L are (0) and L).

A field extension L/K is called *Galois* if it is normal and separable. Although you probably know what this means, we will not use it in these lectures and instead work with an equivalent description.

For warming up we first assume that $[L : K] < \infty$. Then one can show that one always has:

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

(This is not so difficult to show: Suppose $L = K[X]/(f)$, where f is an irreducible polynomial of degree $[L : K]$. Let us fix one root α (in $\overline{K}$) of f. Then every field automorphism $L \to L$ is uniquely determined by the image of α. But, this image must be another root of f, hence, there are at most $[L : K]$ different choices, proving the claim in this case. If L/K is separable, then any finite L/K is of that form; otherwise, one uses the multiplicativity of the 'separable degree'.)

A finite field extension L/K is *Galois* if and only if we have equality, i.e.

$$\#\,\mathrm{Aut}_K(L) = [L : K].$$

In that case we write $\mathrm{Gal}(L/K) := \mathrm{Aut}_K(L)$ and call this the *Galois group of* L/K.

The main result of *finite* Galois Theory states that the two maps

$$\big\{ \text{ fields } L/M/K \big\} \underset{\Psi}{\overset{\Phi}{\rightleftarrows}} \big\{ \text{ subgroups } H \leq \mathrm{Gal}(L/K) \big\}$$

given by $\Phi(M) = \mathrm{Gal}(L/M)$ and $\Psi(H) = L^H$ are inverses to each other and hence bijections. The *à priori* complicated world of field extensions can thus be completely described by the usually simpler world of groups.

We again look at some examples:

(a) $\mathbb{C}/\mathbb{R}$ is Galois and its Galois group has order 2 and consists of the identity and complex conjugation.

(b) $\mathbb{F}_{p^n}/\mathbb{F}_p$: Since we are in characteristic p, the *Frobenius* map $\mathrm{Frob}_p : x \mapsto x^p$ is a field automorphism of $\mathbb{F}_{p^n}$ (the point is that it is additive! That clearly fails over $\mathbb{C}$, for instance). Using that $\mathbb{F}_{p^n}^\times$ is a (cyclic) group of order $p^n - 1$, one immediately gets that $x^{p^n} = x$ in $\mathbb{F}_{p^n}$. This shows that $(\mathrm{Frob}_p)^n$ is the identity. But, it also shows that there is $x \in \mathbb{F}_{p^n}$ such that $(\mathrm{Frob}_p)^i(x) = x^{p^i} \neq x$ for all $i = 1, \ldots, n-1$. This shows that Frob_p has order n. Consequently, we have found n field automorphisms, namely, the powers of Frob_p. Thus, $\mathbb{F}_{p^n}/\mathbb{F}_p$ is a Galois extension and its Galois group is cyclic of order n generated by Frob_p.

(c) Let ζ be a primitive ℓ^n-th root of unity inside $\overline{\mathbb{Q}}$ (where ℓ is a prime number). Explicitly, we can take $\zeta = e^{2\pi i/\ell^n}$. We consider the field extension $\mathbb{Q}(\zeta)/\mathbb{Q}$. Here $\mathbb{Q}(\zeta)$ is the smallest subfield of $\mathbb{C}$ containing $\mathbb{Q}$ and ζ. It is not so difficult to show that one has

$$[\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(\ell^n) = (\ell - 1)\ell^{n-1}.$$

Let $\sigma \in \mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\zeta))$. Then we have

$$1 = \sigma(1) = \sigma(\zeta^{\ell^n}) = (\sigma(\zeta))^{\ell^n},$$

showing that $\sigma(\zeta)$ is another ℓ^n-th root of 1. As σ is invertible, $\sigma(\zeta)$ must also be primitive (i.e. have order ℓ^n). This means that there is an element $\overline{\chi}_{\ell^n}(\sigma) \in (\mathbb{Z}/\ell^n\mathbb{Z})^\times$ such that $\sigma(\zeta) = \zeta^{\overline{\chi}_{\ell^n}(\sigma)}$ (the complicated notation becomes clear below). Let us write this as a map:

$$\overline{\chi}_{\ell^n} : \mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\zeta)) \to (\mathbb{Z}/\ell^n\mathbb{Z})^\times.$$

Note that this map is surjective (for any $i \in (\mathbb{Z}/\ell^n\mathbb{Z})^\times$, define a field automorphism uniquely by sending ζ to ζ^i). Thus, $\mathbb{Q}(\zeta)/\mathbb{Q}$ is also a Galois extension. In fact, it is trivially checked that χ_{ℓ^n} is a group homomorphism. Thus, $\overline{\chi}_{\ell^n}$ is a group isomorphism between the Galois group of $\mathbb{Q}(\zeta)/\mathbb{Q}$ and $(\mathbb{Z}/\ell^n\mathbb{Z})^\times$.

Infinite Galois Theory

A (possibly infinite degree) field extension L/K is *Galois* if and only if L is the union of all finite Galois subextensions M/K, i.e.

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

In that case, we also write $\mathrm{Gal}(L/K) := \mathrm{Aut}_K(L)$.

If L/K is infinite, then $\mathrm{Gal}(L/K)$ is an infinite (even uncountable) group. In order to make it handable, we need to put a *topology* on it. We now describe how this works. If $L/M/K$ with M/K finite Galois, then restricting the K-automorphisms of L to M defines a group surjection with kernel $\mathrm{Gal}(L/M)$, that is, we have the exact sequence of groups

$$1 \to \mathrm{Gal}(L/M) \to \mathrm{Gal}(L/K) \xrightarrow{\sigma \mapsto \sigma|_M} \mathrm{Gal}(M/K) \to 1.$$

(One needs Galois theory to show that $\sigma|_M$ indeed belongs to $\mathrm{Gal}(M/K)$; I don't see how to derive this from $\#\,\mathrm{Aut}_K(M) = [M : K]$ in a simple way. It is, however, an immediate consequence – or even the definition in some presentations – of normality. The surjectivity is usually proved using an extension lemma of Artin.)

In order to define a topology on $G := \mathrm{Gal}(L/K)$ it suffices to give a *basis of open neighbourhoods* $\mathcal{U}_g$ (that is a nonempty collection of sets $Y \subseteq G$ all containing g such that for any $Y_1, Y_2 \in \mathcal{U}_g$

there is $Y_3 \in \mathcal{U}_g$ such that $Y_3 \subseteq Y_1 \cap Y_2$) for any $g \in G$. By definition, a set $X \subseteq G$ is then *open* if and only if for every $g \in X$, there is one $U \in \mathcal{U}_g$ such that $\mathcal{U}_g \subseteq X$.

For $g \in G$ we let $\mathcal{U}_g$ be the set consisting of all cosets $g\,\mathrm{Gal}(L/M)$, where M runs through the finite Galois extensions of K contained in L. We only need to check one condition:

$$g\,\mathrm{Gal}(L/M_1) \cap g\,\mathrm{Gal}(L/M_2) = g\,\mathrm{Gal}(L/(M_1M_2)) \in \mathcal{U}_g.$$

The topology on G thus defined is called the *Krull topology*. Note that if L/K is finite, then $g\,\mathrm{Gal}(L/L) = \{g\}$ is an open set for all $g \in G$, hence, the Krull topology is the discrete topology (every set is open).

The maps

$$m : G \times G \to G, \;\; (g,h) \mapsto gh, \text{ and } i : G \to G, \;\; g \mapsto g^{-1}$$

are continuous. It suffices to check that the preimage of any $Y \in \mathcal{U}_g$ is open: $i^{-1}(g\,\mathrm{Gal}(L/M)) = g^{-1}\,\mathrm{Gal}(L/M)$ and if $(\sigma,\tau) \in m^{-1}(g\,\mathrm{Gal}(L/M))$, then $(\sigma,\tau) \in \sigma\,\mathrm{Gal}(L/M) \times \tau\,\mathrm{Gal}(L/M) \subseteq m^{-1}(g\,\mathrm{Gal}(L/M))$. Thus, G is a topological group.

Definition 1.1. *A topological group G is called* profinite *if it is compact, Hausdorff, and totally disconnected (i.e. the connected component containing some x is equal to $\{x\}$).*

Theorem 1.2. *For any Galois extension L/K, the Galois group $G = \mathrm{Gal}(L/K)$ is a profinite group.*

Proof. **Hausdorff** Let $g \neq h$ be two elements of $\mathrm{Gal}(L/K)$. As gh^{-1} is not the identity, there is M/K Galois such that gh^{-1} is not the identity on M, thus $gh^{-1} \notin \mathrm{Gal}(L/M)$ and so $g\,\mathrm{Gal}(L/M) \cap h\,\mathrm{Gal}(L/M) = \emptyset$.

Compact Consider the map

$$\iota : \mathrm{Gal}(L/K) \to \prod_{K \subseteq M \subseteq L,\ M/K \text{ finite Galois}} \mathrm{Gal}(M/K) =: P$$

given by restricting σ to M on each component. If $\sigma|M = \mathrm{id}_M$ for all M, then σ is clearly the identity, thus, ι is injective. Note that the target space is compact by Tychonov (each $\mathrm{Gal}(L/M)$ is a finite group having the discrete topology). So, it suffices to prove that the image of ι is closed.

For any $M_1/M_2/K$ finite Galois inside L consider the closed subset

$$S_{M_1/M_2} := \{(\sigma_M)_M \in P \mid \sigma_{M_1}|_{M_2} = M_2\} \subseteq P.$$

It is clear that it is closed since only at M_1 and M_2 there is a condition and the topology on $\mathrm{Gal}(M/K)$ is discrete. But

$$\iota(\mathrm{Gal}(L/K)) = \bigcap_{M_1/M_2/K \text{ finite Galois}} S_{M_1/M_2}$$

is closed as an intersection of closed sets. The equality is easy: '$\subseteq$' is clear anyway and for '$\supseteq$' note that given $(\sigma_M)_M \in P$ one makes a unique $\sigma : L \to L$ by putting $\sigma(x) = \sigma_M(x)$ if $x \in M$.

Totally disconnected Let $x \in G$ and $x \in S \subseteq G$ a connected subset (that is, connected in the relative topology). Suppose there is $y \in S \setminus \{x\}$. Let (similarly as above) M/K be finite such that $xy^{-1} \notin \mathrm{Gal}(L/M)$. As $\mathrm{Gal}(L/K) = \bigsqcup_{g \in \mathrm{Gal}(M/K)} g \,\mathrm{Gal}(L/M)$ it follows that

$$S = \bigsqcup_{g \in \mathrm{Gal}(M/K)} (S \cap g \,\mathrm{Gal}(L/M))$$

is a partition into open and closed sets with x and y lying in two different subsets, contradicting the connectedness of S.

□

Note that any $H = \mathrm{Gal}(L/N)$ for N/K finite (not necessarily Galois) is an open subgroup of G because

$$H = \bigsqcup_{g \in H/\,\mathrm{Gal}(L/M)} g \,\mathrm{Gal}(L/M),$$

where M is the Galois closure of N/K in L. Moreover, any $H = \mathrm{Gal}(L/N)$ for N/K finite (not necessarily Galois) is also a closed subgroup of G because $H = G \setminus \bigcup_{H \neq gH \in G/H} gH$. The same reason shows that any closed subgroup $H \leq G$ is open if G/H is finite. Moreover, for any $L/N/K$ (not necessarily finite or Galois) the group

$$\mathrm{Gal}(L/N) = \bigcap_{N/F/K \text{ s.t. } F/K \text{ finite}} \mathrm{Gal}(L/F)$$

is closed.

Theorem 1.3 (Main theorem of Galois Theory)**.** *The two maps*

$$\big\{ \text{ fields } L/M/K \big\} \underset{\Psi}{\overset{\Phi}{\rightleftarrows}} \big\{ \text{ closed subgroups } H \leq \mathrm{Gal}(L/K) \big\}$$

given by $\Phi(M) = \mathrm{Gal}(L/M)$ *and* $\Psi(H) = L^H$ *are inverses to each other and hence bijections.*

Under these correspondences the open subgroups correspond to the finite extensions of K*, and the closed normal subgroups to the Galois extensions of* K*.*

Proof. We have seen that the maps are well-defined.

Let $L/M/K$ be given. We need to show

$$L^{\mathrm{Gal}(L/M)} = M.$$

The inclusion '$\supseteq$' is clear. For the other one '$\subseteq$' let $x \notin M$. We choose a finite Galois extension M_1/M such that $x \in M_1$. By the main theorem of finite Galois theory there is $\overline{\tau} \in \mathrm{Gal}(M_1/M)$ such that $\overline{\tau}(x) \neq x$. We now extend $\overline{\tau}$ to an element of $\mathrm{Gal}(L/M)$. This shows $x \notin L^{\mathrm{Gal}(L/M)}$.

Let $H \leq G$ be a closed subgroup. We need to show

$$H = \mathrm{Gal}(L/L^H).$$

The inclusion '$\subseteq$' is clear. To see equality, for any M/L^H finite Galois we consider the following diagram, whose first row is exact:

$$\begin{array}{ccccccc} 1 & \longrightarrow & \mathrm{Gal}(L/M) & \longrightarrow & \mathrm{Gal}(L/L^H) & \xrightarrow{\text{res}} & \mathrm{Gal}(M/L^H) \longrightarrow 1 \\ & & & & \uparrow & & \| \\ & & & & H & \xrightarrow{\text{res}} & H|_M \longrightarrow 1. \end{array}$$

The equality on the right is an immediate consequence of finite Galois theory noting $L^H = M^{H|_M}$, where by $H|_M$ we denote the group obtained by restricting the elements of H to M.

Let now $\sigma \in \mathrm{Gal}(L/L^H)$. By the diagram, for any M/L^H finite Galois there is $\tau \in H$ such that $\sigma|_M = \tau|_M$, whence $\sigma^{-1}\tau \in \mathrm{Gal}(L/M)$. Thus $\tau \in H \cap \sigma\,\mathrm{Gal}(L/M)$. We have thus proved that $H \cap \sigma\,\mathrm{Gal}(L/M) \neq \emptyset$ for any M/L^H finite Galois. This shows that H has non-empty intersection with any open neighbourhood of σ, hence, σ is in the closure of H. As H is closed, it follows $\sigma \in H$.

The rest is also easy. □

Definition 1.4. *A* directed set *is a set I together with a binary relation $\leq$ on I such that for any pair $i, j \in I$ there is $k \in I$ such that $i \leq k$ and $j \leq k$.*

A projective system of topological groups *for a directed set I is, for each $i \in I$, a topological group G_i and, for each pair $i \leq j$, a continuous group homomorphism $f_{i,j} : G_j \to G_i$ such that $f_{i,i} = \mathrm{id}_{G_i}$ for all $i \in I$ and $f_{i,j} \circ f_{j,k} = f_{i,k}$ for all $i \leq j \leq k$ in I.*

Example 1.5. *(a) Take I to be the set of all fields M such that $L/M/K$ with M/K finite Galois with order relation $M_1 \leq M_2$ if $M_1 \subseteq M_2$. Then $G_M := \mathrm{Gal}(L/M)$ together with $f_{M_1,M_2} : \mathrm{Gal}(M_2/K) \to \mathrm{Gal}(M_1/K)$, the restriction, whenever $M_1 \leq M_2$, forms a projective system of finite (hence topological groups for the discrete topology) groups.*

(b) Let p be a prime. Take $I = \mathbb{N}_{\geq 1}$ the set of natural numbers with the usual $\leq$ order relation. Then $G_n := \mathbb{Z}/p^n\mathbb{Z}$ together with $f_{n,m} : \mathbb{Z}/p^m\mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z}$, the natural projection, for $n \leq m$, forms a projective system of finite (hence topological groups for the discrete topology) groups.

(c) Take $I = \mathbb{N}_{\geq 1}$ the set of natural numbers for the divisibility relation as order relation. Then $G_n := \mathbb{Z}/n\mathbb{Z}$ together with $f_{n,m} : \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, the natural projection, for $n \mid m$, forms a projective system of finite (hence topological groups for the discrete topology) groups.

Proposition 1.6. *Let $(G_i, f_{i,j})$ be a projective system of topological groups for a directed set I. The projective limit of this system is defined as the topological group*

$$\varprojlim_{i \in I} G_i := \{(x_i)_{i \in I} \in \prod_{i \in I} G_i \mid f_{i,j}(x_j) = x_i \; \forall\, i \leq j\}.$$

If the G_i are finite groups with the discrete topology, then $\varprojlim_{i \in I} G_i$ is a profinite group.

Proof. Exercise. One should let oneself be inspired by the proof of Theorem 1.2. □

Example 1.7. *(a) One has*

$$\mathrm{Gal}(L/K) = \varprojlim_{K \subseteq M \subseteq L,\ M/K \text{ finite Galois}} \mathrm{Gal}(M/K).$$

We showed this in the proof of Theorem 1.2.

(b) The group $\varprojlim_{n\in\mathbb{N}} \mathbb{Z}/p^n\mathbb{Z}$ *is called the group of* p-adic integers, *it is denoted* $\mathbb{Z}_p$.

(c) The group $\varprojlim_{n\in\mathbb{N}} \mathbb{Z}/n\mathbb{Z}$ *is called* Z hat *and it is denoted* $\widehat{\mathbb{Z}}$. *By the Chinese remainder theorem one has* $\widehat{\mathbb{Z}} \cong \prod_{p \text{ prime}} \mathbb{Z}_p$.

(d) We now compute the Galois group of $\overline{\mathbb{F}}_p/\mathbb{F}_p$. *We clearly have*

$$\overline{\mathbb{F}}_p = \bigcup_{n\in\mathbb{N}} \mathbb{F}_{p^n},$$

since any element in $\overline{\mathbb{F}}_p$ *is contained in some finite extension* $\mathbb{F}_{p^n}$. *Hence, this is a Galois extension (in fact, for any field* F *the extension* $\overline{F}/F$, *where* $\overline{F}$ *is a separable closure of* F, *is a Galois extension). We thus have*

$$\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p) = \varprojlim_{n\in\mathbb{N}} \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) \cong \varprojlim_{n\in\mathbb{N}} \mathbb{Z}/(n) =: \hat{\mathbb{Z}} = \langle \mathrm{Frob}_p \rangle_{\text{top. gp.}}.$$

This means that the Galois group is a pro-cyclic group (by definition, this is the projective limit of cyclic groups), and, equivalently, that it is topologically generated by a single element, namely the Frobenius.

2 Representations

Definition 2.1. *Let* G *be a profinite group and let* k *be a topological field. By an* n-dimensional representation of G *we mean a continuous homomorphism of groups*

$$\rho : G \to \mathrm{GL}_n(k).$$

Example 2.2. *(1) If* G *is a finite group with the discrete topology and* k *are the complex numbers, then we are in the context of the standard theory of representations of finite groups.*

(2) $\varphi : \mathbb{Z}/N\mathbb{Z} \to \mathrm{GL}_1(\mathbb{C})$, $r + N\mathbb{Z} \mapsto \zeta_N^r = e^{2\pi i r/N}$.

(3) For a finite group G *the* regular representation *is defined by the natural left* G*-action on the group algebra* $\mathbb{C}[G]$.

(4) We have the augmentation exact sequence

$$0 \to I_G \to \mathbb{C}[G] \xrightarrow{g \mapsto 1} \mathbb{C} \to 0$$

with the aumentation ideal $I_G = (g-1) \lhd \mathbb{C}[G]$.

The left action of G *on* I_G *gives rise to the* augmentation representation.

(5) Let M *be any* $\mathbb{C}[G]$*-module. Then* G *also acts on* $\mathrm{End}_{\mathbb{C}}(M)$ *by* $(g.\sigma)(m) = g.(\sigma(g^{-1}.m))$ *for* $g \in G$, $m \in M$ *and* $\sigma \in \mathrm{End}_{\mathbb{C}}(M)$. *This representation is called the* adjoint representation of M. *Thinking about this representation in terms of matrices,* g *acts by conjugation. Hence, the augmentation representation can be restricted to the matrices of trace* 0.

We always consider $\overline{\mathbb{F}}_\ell$ with the discrete topology.

Definition 2.3. *Let* ρ *be an* n*-dimensional representation of* G *over* k.

(a) The representation ρ *is called*

- *an* Artin representation *if* $k \subseteq \mathbb{C}$ *(topological subfield),*
- *an* ℓ-adic representation *if* $k \subseteq \overline{\mathbb{Q}}_\ell$,
- *a* mod ℓ representation *if* $k \subseteq \overline{\mathbb{F}}_\ell$.

(b) The representation ρ *is called*

- abelian *if* $\rho(G)$ *is an abelian group,*
- dihedral *if* $\rho(G)$ *is a dihedral group, etc.*

Definition 2.4. *Two* n*-dimensional representations* ρ_1 *and* ρ_2 *of* G *over* k *are called* equivalent *if there exists some* $M \in \mathrm{GL}_n(k)$ *such that for all* $g \in G$

$$\rho_1(g) = M\rho_2(g)M^{-1}.$$

Proposition 2.5. *Let* G *be a profinite group,* k *a topological field and* $\rho : G \to \mathrm{GL}_n(k)$ *a representation. The image of* ρ *is finite in any of the three cases:*

(a) ρ *is an Artin representation,*

(b) ρ *is a mod* ℓ *representation,*

(c) G *is a pro-*p*-group and* ρ *is an* ℓ*-adic representation with* $\ell \neq p$.

Proof. Exercise. □

Proposition 2.6. *Let k be a local field with complete discrete valuation ring $\mathcal{O}$, maximal ideal $\mathfrak{m}$ and residue field $\mathbb{F} = \mathcal{O}/\mathfrak{m}$ of characteristic ℓ. Let G be a profinite group and $\rho : G \to \mathrm{GL}_n(k)$ a representation. Then there exists a representation*

$$\rho_1 : G \to \mathrm{GL}_n(\mathcal{O})$$

such that

$$G \xrightarrow{\rho_1} \mathrm{GL}_n(\mathcal{O}) \xrightarrow{\text{inclusion}} \mathrm{GL}_n(k)$$

is equivalent to ρ.

Proof. Exercise. □

Definition 2.7. *Assume the set-up of Proposition 2.6. The composition*

$$\overline{\rho} : G \xrightarrow{\rho_1} \mathrm{GL}_n(\mathcal{O}) \xrightarrow{\text{natural projection}} \mathrm{GL}_n(\mathbb{F})$$

is called a mod ℓ reduction of ρ.

Definition 2.8. *Let ρ be an n-dimensional representation of G over k. Let $V = k^n$ the standard n-dimensional k-vector space. We make V into a $k[G]$-module by defining the G-action as*

$$g.v = \rho(g)v \text{ for } g \in G, v \in V.$$

We call ρ (semi-)simple if V is (semi-)simple in the category of $k[G]$-modules.

More explicitly, ρ is simple (other word: irreducible) if the only k-subspace $W \lneq V$ such that $gW \subseteq W$ for all $g \in G$ is the 0-space. Moreover, ρ is called semi-simple if V is the direct sum of simple $k[G]$-modules, that is, $V = W_1 \oplus \cdots \oplus W_n$, where the W_i are k-subspaces of V such that $gW_i \subseteq W_i$ for all $g \in G$.

We call ρ indecomposable if $V = W_1 \oplus W_2$ with $k[G]$-submodules $W_i \leq V$ is only possible if one of them is the 0-space.

Note that indecomposable does not imply irreducible if the characteristic of k is positive. For instance $\overline{\mathbb{F}}_2[\mathbb{Z}/2\mathbb{Z}]$ is indecomposable but not irreducible.

Moreover ρ is called absolutely irreducible (absolutely semi-simple, absolutely indecomposable, etc.) *if $\overline{k} \otimes_k V$ has this property, where $\overline{k}$ is an algebraic closure of k.*

By the semi-simplification of ρ we mean the direct sum of all Jordan-Hölder constituents of V as $k[G]$-module.

Theorem 2.9 (Brauer-Nesbitt)**.** *Let k be a field. Let $\rho_i : G \to \mathrm{GL}_n(k)$ with $i = 1, 2$ be continuous semi-simple representations. Assume that at least one of the following two conditions holds:*

(1) $\mathrm{charpoly}(\rho_1(g)) = \mathrm{charpoly}(\rho_2(g))$ *for all $g \in G$;*

(2) The characteristic of k is 0 or bigger than n and $\mathrm{Tr}(\rho_1(g)) = \mathrm{Tr}(\rho_2(g))$ for all $g \in G$.

Then ρ_1 and ρ_2 are equivalent.

Proposition 2.10 (Serre, Carayol)**.** *Let R be a local ring with maximal ideal $\mathfrak{m}$ and let $\rho_i : G \to \mathrm{GL}_n(R)$ be a continuous representation of a group G for $i = 1, 2$ such that ρ_1 is residually absolutely irreducible, that is, $G \to \mathrm{GL}_n(R) \twoheadrightarrow \mathrm{GL}_n(R/\mathfrak{m})$ is absolutely irreducible. Assume that all traces are equal: $\mathrm{Tr}(\rho_1(g)) = \mathrm{Tr}(\rho_2(g))$ for all $g \in G$.*

Then ρ_1 and ρ_2 are equivalent over R.

Lecture 2

Galois representations

In this lecture we will

- define Galois representations,
- introduce basic properties, such as the representation being unramified, and
- give some examples.

1 Definition and properties

Definition 1.1. *Let K be a field. We denote by G_K the absolute Galois group of K, i.e. the Galois group of a separable closure of G.*

Let k be a topological field. A representation of G_K over k is called a Galois representation.

If K is a global field (e.g. a number field), then a representation of G_K is called a global Galois representation*. If K is a local field, then we speak of a* local Galois representation.

Remark 1.2. *One often hears about ℓ-*adic Galois representations *(or even* elladic *ones) as compared to p-*adic Galois representations*. In that case, what people usually mean the following: Let*

$$G_K \to \mathrm{GL}_n(k)$$

be an n-dimensional Galois representation with K a finite extension of $\mathbb{Q}_p$ and k a finite extension of $\mathbb{Q}_l$. The situation $l \neq p$ is referred to as ℓ-adic, and the situation $l = p$ as p-adic.

The behaviour is fundamentally different! Wild inertia (to be explained in a second), which is a pro-p group, has a finite image in the first case (by Proposition 2.5), but it can have a very large image in the second case.

Before we can go on, we need to recall some algebraic number theory. We start by the finite situation. Let K be a number field and $\mathfrak{p}$ a prime. Then we can complete K at $\mathfrak{p}$ (with respect to the non-archimedean absolute value attached to $\mathfrak{p}$ or by completing the ring of integers of K at $\mathfrak{p}$ in the

sense of commutative algebra) to obtain $K_{\mathfrak{p}}$, a finite extension of $\mathbb{Q}_p$, where $(p) = \mathbb{Z} \cap \mathfrak{p}$ is the rational prime number lying under $\mathfrak{p}$. Then $K_{\mathfrak{p}}$ is a local field with a non-archimedean absolute value $|\cdot|$, discrete valuation ring

$$\mathcal{O}_{K_{\mathfrak{p}}} = \mathcal{O}_{\mathfrak{p}} = \{x \in K_{\mathfrak{p}} \mid \ |x| \leq 1\}$$

and valuation ideal

$$\widehat{\mathfrak{p}} = \{x \in K_{\mathfrak{p}} \mid \ |x| < 1\}.$$

We shall also write $\mathfrak{p}$ for $\widehat{\mathfrak{p}}$. In the sequel we need and assume that the absolute value $|\cdot|$ is *correctly normalized*. For the residue fields, we shall use the notation

$$\mathbb{F}(\mathfrak{p}) = \mathbb{F}(K_{\mathfrak{p}}) := \mathcal{O}_{\mathfrak{p}}/\widehat{\mathfrak{p}}.$$

The residue field can also be seen as the quotient of the ring of integers of K by $\mathfrak{p}$.

Now we move on to discuss finite Galois extensions. Let L/K be a finite Galois extension of number fields and $\mathfrak{P}/\mathfrak{p}/p$ prime ideals in these fields. The *decomposition group of* $\mathfrak{P}$ is defined as

$$D(\mathfrak{P}/\mathfrak{p}) = \{\sigma \in \mathrm{Gal}(L/K) | \sigma(\mathfrak{P}) = \mathfrak{P}\}.$$

It is naturally isomorphic to the local Galois group

$$D(\mathfrak{P}/\mathfrak{p}) \cong \mathrm{Gal}(L_{\mathfrak{P}}/K_{\mathfrak{p}}).$$

Indeed, recall that L is dense in $L_{\mathfrak{P}}$ and K in $K_{\mathfrak{p}}$. An automorphism $\sigma \in D(\mathfrak{P}/\mathfrak{p})$ can be uniquely extended by continuity to an automorphism in the local Galois group. To go in the converse direction, one just restricts the automorphism to L.

Whenever we have a Galois extension of local fields $L_{\mathfrak{P}}/K_{\mathfrak{p}}$, we can consider the reduction mod $\mathfrak{P}$ of all field automorphisms in $\mathrm{Gal}(L_{\mathfrak{P}}/K_{\mathfrak{p}})$, since each of them fixes the valuation rings. The reduction map

$$\pi(L_{\mathfrak{P}}/K_{\mathfrak{p}}) = \pi(\mathfrak{P}/\mathfrak{p}) : \mathrm{Gal}(L_{\mathfrak{P}}/K_{\mathfrak{p}}) \to \mathrm{Gal}(\mathbb{F}(\mathfrak{P})/\mathbb{F}(\mathfrak{p}))$$

is surjective. To see the surjectivity, we consider $L_{\mathfrak{P}}$ as $K_{\mathfrak{p}}[X]/(f(X))$ with f an irreducible polynomial (monic and with coefficients in $\mathcal{O}_{\mathfrak{p}}$) of degree equal to $[L_{\mathfrak{P}} : K_{\mathfrak{p}}]$. Let us fix a root α of f. An element in the Galois group is uniquely given by the image of α, i.e. the Galois group consists of the elements σ_β with $\sigma_\beta(\alpha) = \beta$. The factorization of f mod $\mathfrak{p}$ is of the form $g(X)^e$ and the reduction $\overline{\alpha}$ of α is a root of g. An element $\overline{\sigma} \in \mathrm{Gal}(\mathbb{F}(\mathfrak{P})/\mathbb{F}(\mathfrak{p}))$ is uniquely given by the image $\overline{\sigma}(\overline{\alpha})$, which is of the form $\overline{\beta}$ with β a root of f. Hence, σ_β reduces to $\overline{\sigma}$, showing the surjectivity.

A canonical generator of $\mathrm{Gal}(\mathbb{F}(\mathfrak{P})/\mathbb{F}(\mathfrak{p}))$ is given by the (arithmetic) *Frobenius endomorphism* (or *Frobenius element*) $\mathrm{Frob}(L_{\mathfrak{P}}/K_{\mathfrak{p}}) = \mathrm{Frob}(\mathfrak{P}/\mathfrak{p})$ which is defined as $x \mapsto x^q$ with $q = \#\mathbb{F}(\mathfrak{p}) = N(\mathfrak{p})$. The integer $N(\mathfrak{p})$ is called the *norm of* $\mathfrak{p}$. The kernel of the reduction map is called the *inertia group* $I(L_{\mathfrak{P}}/K_{\mathfrak{p}}) = I(\mathfrak{P}/\mathfrak{p})$, so that we have the exact sequence

$$0 \to I(L_{\mathfrak{P}}/K_{\mathfrak{p}}) \to \mathrm{Gal}(L_{\mathfrak{P}}/K_{\mathfrak{p}}) \xrightarrow{\pi(L_{\mathfrak{P}}/K_{\mathfrak{p}})} \mathrm{Gal}(\mathbb{F}(\mathfrak{P})/\mathbb{F}(\mathfrak{p})) \to 0.$$

The field extension $L_{\mathfrak{P}}/K_{\mathfrak{p}}$ (or the prime $\mathfrak{P}$ above $\mathfrak{p}$) is *unramified* if and only if $I(L_{\mathfrak{P}}/K_{\mathfrak{p}})$ is trivial, i.e. if and only if the reduction map $\pi(L_{\mathfrak{P}}/K_{\mathfrak{p}})$ is an isomorphism. The inertia group $I(L_{\mathfrak{P}}/K_{\mathfrak{p}})$ has a unique p-Sylow group $P(L_{\mathfrak{P}}/K_{\mathfrak{p}}) = P(\mathfrak{P}/\mathfrak{p})$, which is called the *wild inertia group*. The field extension $L_{\mathfrak{P}}/K_{\mathfrak{p}}$ (or the prime $\mathfrak{P}$ above $\mathfrak{p}$) is *tamely ramified* if $P(L_{\mathfrak{P}}/K_{\mathfrak{p}})$ is trivial; otherwise, it is called *wildly ramified*.

Now we investigate what happens if we change the prime $\mathfrak{P}$ lying above a fixed $\mathfrak{p}$ in the Galois extension L/K. One knows that any other prime is of the form $\sigma(\mathfrak{P})$ with $\sigma \in \mathrm{Gal}(L/K)$. Then we clearly have

$$D(\sigma(\mathfrak{P})/\mathfrak{p}) = \sigma \circ D(\mathfrak{P}/\mathfrak{p}) \circ \sigma^{-1}$$

and, consequently, similar statements for $I(L_{\mathfrak{P}}/K_{\mathfrak{p}})$ and $P(L_{\mathfrak{P}}/K_{\mathfrak{p}})$. Hence, if the extension L/K is unramified (or tamely ramified) at one $\mathfrak{P}$, then so it is at all $\sigma(\mathfrak{P})$, whence we say that L/K is unramified (or tamely ramified) at the 'small' ideal $\mathfrak{p}$.

Suppose L/K is unramified at $\mathfrak{p}$, so that the reduction map $\pi(\mathfrak{P}/\mathfrak{p})$ is an isomorphism. We can thus consider $\mathrm{Frob}(L_{\mathfrak{P}}/K_{\mathfrak{p}})$ as an element of $D(\mathfrak{P}/\mathfrak{p})$. We have

$$\mathrm{Frob}(\sigma(\mathfrak{P})/\mathfrak{p}) = \sigma \circ \mathrm{Frob}(\mathfrak{P}/\mathfrak{p}) \circ \sigma^{-1},$$

so that the Frobenius elements of the primes lying over $\mathfrak{p}$ form a conjugacy class in $\mathrm{Gal}(L/K)$. We will often write $\mathrm{Frob}_{\mathfrak{p}}$ for either this conjugacy class or any element in it.

Our next goal is to pass to infinite Galois extensions. For that it is often useful to take an *embedding point of view* on primes. We fix once and for all algebraic closures $\overline{\mathbb{Q}}$ and $\overline{\mathbb{Q}}_p$ for all p. The field $\overline{\mathbb{Q}}_p$ also has an absolute value $|\cdot|$ which is chosen such that the restriction of $|\cdot|$ to any finite extension of $\mathbb{Q}_p$ contained in $\overline{\mathbb{Q}}_p$ gives the standard absolute value on that field.

Let $K \subset \overline{\mathbb{Q}}$ be a number field (even if we do not write the inclusion into our fixed $\overline{\mathbb{Q}}$, we often mean it). Let us choose an embedding $\iota : \overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$. It determines a prime $\mathfrak{p}$ lying above p, namely we take $\mathfrak{p} = K \cap \iota^{-1}(\{x \in \overline{\mathbb{Q}}_p \mid |x| < 1\})$. Moreover, in the same way it gives prime ideals above $\mathfrak{p}$ for *every* extension $K \subseteq L \subset \overline{\mathbb{Q}}$, which are compatible with intersection. Conversely, if we are given a prime $\mathfrak{p}$ of K lying above p, we can first pass to the completion $K_{\mathfrak{p}}$ of K at $\mathfrak{p}$ and then choose any embedding of $K_{\mathfrak{p}}$ into $\overline{\mathbb{Q}}_p$; this defines an embedding $K \hookrightarrow K_{\mathfrak{p}} \hookrightarrow \overline{\mathbb{Q}}_{\mathfrak{p}}$, which by Artin's extension lemma of Galois theory can be extended to an embedding $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$. From now on we are going to take this point of view of embeddings. It allows us to generalize the above discussion and it also enables us to view $\overline{\mathbb{Q}}_p$ and $\mathbb{C}$ on an equal footing (what we mean becomes clear below: Frobenius elements and complex conjugation are defined in a very similar way: the former at finite places, the latter at infinite ones).

Let still K be a number field (inside $\overline{\mathbb{Q}}$) and fix an embedding $\iota_{\mathfrak{p}} : K \hookrightarrow \overline{\mathbb{Q}}_p$, which we extend to $\iota : \overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$ as before. It gives rise to an embedding of absolute Galois groups

$$\mathrm{Gal}(\overline{\mathbb{Q}}_p/K_{\mathfrak{p}}) \hookrightarrow \mathrm{Gal}(\overline{\mathbb{Q}}/K), \quad \sigma \mapsto \iota^{-1} \circ \sigma \circ \iota.$$

Note that this definition makes sense, since $\overline{\mathbb{Q}}/K$ is a normal extension. If we have two such embeddings ι_1 and ι_2, then the two embeddings of Galois groups are conjugate by $\iota_1 \circ \iota_2^{-1}$, just as in the case of finite primes.

Let $K_\mathfrak{p} \subset L_\mathfrak{P} \subset M_{\tilde{\mathfrak{P}}}$ be finite degree subfields of $\overline{\mathbb{Q}}_p$. We obtain a projective system of short exact sequences:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & I(M_{\tilde{\mathfrak{P}}}/K_\mathfrak{p}) & \longrightarrow & \mathrm{Gal}(M_{\tilde{\mathfrak{P}}}/K_\mathfrak{p}) & \xrightarrow{\pi(M_{\tilde{\mathfrak{P}}}/K_\mathfrak{p})} & \mathrm{Gal}(\mathbb{F}(\tilde{\mathfrak{P}})/\mathbb{F}(\mathfrak{p})) & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & I(L_\mathfrak{P}/K_\mathfrak{p}) & \longrightarrow & \mathrm{Gal}(L_\mathfrak{P}/K_\mathfrak{p}) & \xrightarrow{\pi(L_\mathfrak{P}/K_\mathfrak{p})} & \mathrm{Gal}(\mathbb{F}(\mathfrak{P})/\mathbb{F}(\mathfrak{p})) & \longrightarrow & 0.
\end{array}$$

The projective limit over compact sets is exact, hence, we obtain the exact sequence

$$0 \to I_{K_\mathfrak{p}} \to G_{K_\mathfrak{p}} \xrightarrow{\pi_\mathfrak{p}} G_{\mathbb{F}(\mathfrak{p})} \to 0,$$

where $I_{K_\mathfrak{p}} = I_\mathfrak{p}$ is the projective limit over the inertia groups. With the same reasoning we obtain that the projective limit $P_{K_\mathfrak{p}} = P_\mathfrak{p}$ over the wild inertia groups is equal to the (necessarily unique) pro-p Sylow group of $I_{K_\mathfrak{p}}$. We again call $I_{K_\mathfrak{p}}$ and $P_{K_\mathfrak{p}}$ the *inertia (group)* respectively the *wild inertia (group) of $K_\mathfrak{p}$ (or of $\mathfrak{p}$)*. By $\mathrm{Frob}_\mathfrak{p}$ we denote the Frobenius element in $\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}(\mathfrak{p}))$.

We can see complex conjugation as a variant of this. Suppose there is an embedding τ_∞ of K into $\mathbb{R}$. Then for any embedding $\tau : \overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$ extending τ_∞, the map

$$\tau^{-1} \circ \text{ (complex conjugation in } \mathbb{C}/\mathbb{R}) \circ \tau$$

defines an element of G_K. It is called *a complex conjugation*. Again, all complex conjugations are conjugate.

Now we come to the very important definition of unramified and tamely ramified Galois representations. We start with the local case.

Definition 1.3. *Let $K_\mathfrak{p}$ be a finite extension of $\mathbb{Q}_p$ and let k be any topological field. Consider a local Galois representation $\rho : G_{K_\mathfrak{p}} \to \mathrm{GL}_n(k)$. It is called*

- unramified *if* $\rho(I_{K_\mathfrak{p}}) = 0$,
- tamely ramified *if* $\rho(P_{K_\mathfrak{p}}) = 0$.

Let ρ be a representation as in the definition and let V be the k-vector space underlying it, i.e. such that $\rho : G_{K_\mathfrak{p}} \to \mathrm{GL}_n(k) = \mathrm{GL}(V)$. Denote by $V^{I_{K_\mathfrak{p}}}$ the sub-vector space $V^{\rho(I_{K_\mathfrak{p}})}$ of V consisting of the elements fixed by $I_{K_\mathfrak{p}}$. We obtain the unramified representation

$$\rho^{I_{K_\mathfrak{p}}} : G_{K_\mathfrak{p}} \to \mathrm{GL}(V^{I_{K_\mathfrak{p}}}) = \mathrm{GL}_m(k)$$

for some $m \leq n$. Clearly, ρ is unramified if and only if $\rho = \rho^{I_{K_\mathfrak{p}}}$.

Evaluating an unramified representation at the Frobenius element makes sense, since any preimage under $\pi_{K_\mathfrak{p}}$ of $\mathrm{Frob}_{K_\mathfrak{p}}$ is uniquely determined up to a trivially acting element from $I_{K_\mathfrak{p}}$.

Definition 1.4. *The* characteristic polynomial of Frobenius of ρ *is defined as*

$$\Phi(\rho)(X) := \mathrm{charpoly}(\rho^{I_{K_\mathfrak{p}}}(\mathrm{Frob}_{K_\mathfrak{p}})) = \det(X - \mathrm{Frob}_{K_\mathfrak{p}} \mid V^{I_{K_\mathfrak{p}}}) \in k[X].$$

Very often one sees a slightly different version, namely

$$\tilde{\Phi}(\rho)(X) := \det(1 - X\,\mathrm{Frob}_{K_\mathfrak{p}} \mid V^{I_{K_\mathfrak{p}}}) \in k[X].$$

We have the relation

$$\tilde{\Phi}(\rho)(X) = X^n \cdot \Phi(\rho)(X^{-1}).$$

Now we treat the global situation.

Definition 1.5. *Let K be a number field (inside $\overline{\mathbb{Q}}$), and k any topological field. Consider a global Galois representation $\rho : G_K \to \mathrm{GL}_n(k)$. Let $\mathfrak{p}$ be a prime of K corresponding to an embedding $\iota_\mathfrak{p} : K \hookrightarrow \overline{\mathbb{Q}}_p$. Choose any embedding $\iota : \overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$ extending $\iota_\mathfrak{p}$, giving rise to an embedding of $G_{K_\mathfrak{p}}$ into G_K. The Galois representation ρ is called* unramified (respectively, tamely ramified) at $\mathfrak{p}$ *if the restriction of ρ to $G_{K_\mathfrak{p}}$ is unramified (respectively, tamely ramified).*

We also define the characteristic polynomial of Frobenius at $\mathfrak{p}$ *as*

$$\Phi_\mathfrak{p}(\rho) := \Phi(\rho|_{G_{K_\mathfrak{p}}}) \in k[X]$$

and

$$\tilde{\Phi}_\mathfrak{p}(\rho) := \tilde{\Phi}(\rho|_{G_{K_\mathfrak{p}}}) \in k[X].$$

Note that these properties do not depend on the choice of ι (for the statement on the characteristic polynomial we use that conjugate matrices have the same characteristic polynomial).

Definition 1.6. *Let ρ be as in the previous definition with $n = 1, 2$. Then ρ is called* odd *if the image of all complex conjugations has determinant -1.*

There are generalisations of odd representations for $n > 2$.

The Frobenius elements play a very special role in the theory. Their images determine the Galois representation uniquely. This is a consequence of Chebotarev's density theorem.

Recall that the norm of an ideal is denoted as $N(\mathfrak{p}) = \#\mathbb{F}(\mathfrak{p})$.

Definition 1.7. *Let K be a number field and S a set of primes of K.*

(a) The Dirichlet density of S *is defined as*

$$d(S) := \lim_{s \to 1,\, s>1} \frac{\sum_{\mathfrak{p} \in S} N(\mathfrak{p})^{-s}}{\sum_{\mathfrak{p}} N(\mathfrak{p})^{-s}},$$

if the limit exists.

(b) The natural density of S *is defined as*

$$\delta(S) := \lim_{x\to\infty} \frac{\#\{\mathfrak{p} \in S \mid N(\mathfrak{p}) < x\}}{\#\{\mathfrak{p} \mid N(\mathfrak{p}) < x\}},$$

if the limit exists.

The existence of the natural density implies the existence of the Dirichlet density, but the converse does not hold in general.

Theorem 1.8 (Chebotarev's density theorem)**.** *Let L/K be a finite Galois extension of number fields with Galois group $G = \mathrm{Gal}(L/K)$. Let $\sigma \in G$ be any element. We use the notation $[\sigma]$ to denote the conjugacy class of σ in G. Define the set of primes*

$$P_{L/K}(\sigma) = \{\mathfrak{p} \mid [\mathrm{Frob}_\mathfrak{p}] = [\sigma]\}.$$

The Dirichlet density of this set is

$$d(P_{L/K}(\sigma)) = \frac{\#[\sigma]}{\#G}.$$

In other words, the Frobenius elements are uniformly distributed over the conjugacy classes of the Galois group.

We will at least give a precise sketch of the proof later this lecture and we will also present important applications. Here we provide a first one concerning Galois representations.

Corollary 1.9. *Let K be a number field, k a topological field and $\rho : G_K \to \mathrm{GL}_n(k)$ a global Galois representation that ramifies at most at finitely many primes of K. Then the set*

$$\{\rho(\mathrm{Frob}_\mathfrak{p}) | \mathfrak{p} \text{ unramified } \}$$

is a dense subset of the image $\rho(G_K)$. In other words, the Frobenius elements topologically generate the image of the Galois representation.

Moreover, the Galois representation is uniquely determined by the images of the Frobenius elements.

Proof. In a profinite group G a subset $X \subset G$ is dense in G if and only if the image of X under all natural projections $G \twoheadrightarrow G_i$ is equal to G_i.

We apply this with $G = \rho(G_K)$ and X the set of Frobenius images. All the finite quotients of G correspond to finite Galois extensions and, consequently, Chebotarev's density theorem (Theorem 1.8) implies that the image of X in any finite quotient hits all conjugacy classes and because of $\mathrm{Frob}(\sigma(\mathfrak{P}/\mathfrak{p})) = \sigma \circ \mathrm{Frob}(\mathfrak{P}/\mathfrak{p}) \circ \sigma^{-1}$ is all of it. □

2 Examples

Cyclotomic character

We now give a very important example of a Galois representation in dimension 1: the *ℓ-adic cyclotomic character*. Recall from above that we found the group isomorphism:

$$\overline{\chi}_{\ell^n} : \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) = \mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\zeta)) \to (\mathbb{Z}/\ell^n\mathbb{Z})^\times.$$

Let us rewrite this, using the group surjection $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$:

$$\overline{\chi}_{\ell^n} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_1(\mathbb{Z}/\ell^n\mathbb{Z}).$$

We can now take the projective limit to obtain the *ℓ-adic cyclotomic character*

$$\chi_\ell : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathbb{Z}_\ell^\times \cong \mathrm{GL}_1(\mathbb{Z}_\ell).$$

Its properties are summarised in the following proposition.

Proposition 2.1. *Let χ_ℓ be the cyclotomic character over $\overline{\mathbb{Q}}$. It is a 1-dimensional global Galois representation, which is unramified at all primes $p \neq \ell$ and is characterized there by*

$$\chi_\ell(\mathrm{Frob}_p) = p.$$

More generally, we have

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

for all $\zeta \in \mu_{\ell^n}(\overline{\mathbb{Q}})$, all n and all $\sigma \in G_{\mathbb{Q}}$. In particular, the image of any complex conjugation is equal to -1.

Proof. Exercise. □

Abelian varieties

Let K be a field and A an abelian variety of dimension g over K. Let

$$A(\overline{K})[m] = \ker\left(A(\overline{K}) \xrightarrow{P \mapsto m \cdot P} A(\overline{K})\right)$$

be the m-torsion points of $A(\overline{K})$. One defines the *ℓ-adic Tate module of A* by

$$T_\ell(A) := \varprojlim_n A(\overline{K})[\ell^n]$$

with respect to the projective system

$$A(\overline{K})[\ell^n] \twoheadrightarrow A(\overline{K})[\ell^{n-1}], \quad P \mapsto \ell \cdot P.$$

If ℓ is not the characteristic of K, then, as is well known, one can compatibly identify $A(\overline{K})[\ell^n]$ with $(\mathbb{Z}/\ell^n\mathbb{Z})^{2g}$, yielding an isomorphism

$$T_\ell(A) \cong (\mathbb{Z}_\ell)^{2g}.$$

One often puts

$$V_\ell(A) := T_\ell(A) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell \cong (\mathbb{Q}_\ell)^{2g}.$$

The absolute Galois group G_K acts on $T_\ell(A)$ and on $V_\ell(A)$, since it compatibly acts on all the $A(\overline{K})[\ell^n]$. This yields the *Galois representation attached to* A:

$$\rho_A : G_K \to \mathrm{Aut}_{\mathbb{Q}_\ell}(V_\ell(\overline{K})) \cong \mathrm{GL}_{2g}(\mathbb{Q}_\ell).$$

Theorem 2.2 (Serre, Tate)**.** *Let K be a number field. Then ρ_A is unramified at all primes $\mathfrak{p}$ of K at which A has good reduction.*

Here is a more precise theorem for the special case of elliptic curves.

Theorem 2.3. *Let K be a number field and E an elliptic curve over K. Let $\mathfrak{p}$ be a prime of K at which E has good reduction. Then ρ_E is unramified at $\mathfrak{p}$ and we have*

$$\Phi_\mathfrak{p}(\rho_E) = X^2 - a_\mathfrak{p} X + N(\mathfrak{p})$$

and

$$\tilde{\Phi}_\mathfrak{p}(\rho_E) = 1 - a_\mathfrak{p} X + N(\mathfrak{p}) X^2$$

where $a_\mathfrak{p} \in \mathbb{Z}$ such that

$$\#E(\mathbb{F}(\mathfrak{p})) = N(\mathfrak{p}) + 1 - a_\mathfrak{p} = \Phi_\mathfrak{p}(\rho_E)(1).$$

Furthermore, the determinant of ρ_E is equal to the cyclotomic character of K.

Lecture 3

Galois representations attached to modular forms

In this lecture we will

- recall the definition of modular forms and Hecke operators,
- describe the Galois representation attached to a Hecke eigenform,
- define the conductor and the Serre weight of a 2-dimensional residual Galois representation,
- state Serre's modularity conjecture, and
- in an appendix sketch the construction of the Galois representation attached to a Hecke eigenform.

1 Modular forms

Congruence subgroups

We first we recall the standard congruence subgroups of $\mathrm{SL}_2(\mathbb{Z})$. By N we shall always denote a positive integer.

$$\begin{aligned}\Gamma(N) &:= \{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z}) \mid \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \equiv \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) \mod N\} \\ \Gamma_1(N) &:= \{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z}) \mid \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \equiv \left(\begin{smallmatrix} 1 & * \\ 0 & 1 \end{smallmatrix}\right) \mod N\} \\ \Gamma_0(N) &:= \{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z}) \mid \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \equiv \left(\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix}\right) \mod N\}\end{aligned}$$

These groups are all called the *congruence subgroups of level* N, and $\Gamma(N)$ the *principal* one.

Remark 1.1. *We describe a more conceptual point of view on congruence subgroups. The following observations are at the base of defining level structures for elliptic curves (which we won't do in these lectures).*

(a) The group homomorphism

$$\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$$

given by reducing the matrices modulo N is surjective with kernel $\Gamma(N)$.

(b) The group $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ acts on $(\mathbb{Z}/N\mathbb{Z})^2$ (by multiplying the matrix with a vector). In particular, the homomorphism $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}) \to (\mathbb{Z}/N\mathbb{Z})^2$ given by $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \mapsto \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right) = \left(\begin{smallmatrix} a \\ c \end{smallmatrix}\right)$ takes all $\left(\begin{smallmatrix} a \\ c \end{smallmatrix}\right) \in (\mathbb{Z}/N\mathbb{Z})^2$ as image such that a, c generate $\mathbb{Z}/N\mathbb{Z}$. Moreover, the image is equal to set of elements in $(\mathbb{Z}/N\mathbb{Z})^2$ which are of precise (additive) order N. The kernel is the stabiliser of $\left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right)$.

(c) The group $\Gamma_1(N)$ is the preimage in $\mathrm{SL}_2(\mathbb{Z})$ of the stabiliser subgroup of $\left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right)$.

(d) The group $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ also acts on $\mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})$, the projective line over $\mathbb{Z}/N\mathbb{Z}$ which one can define as the tuples $(a : c)$ with $a, c \in \mathbb{Z}/N\mathbb{Z}$ such that $\langle a, c\rangle = \mathbb{Z}/N\mathbb{Z}$ modulo the equivalence relation given by multiplication by an element of $(\mathbb{Z}/N\mathbb{Z})^\times$. The action is the natural one (we should actually view $(a : c)$ as a column vector, as above). The preimage in $\mathrm{SL}_2(\mathbb{Z})$ of the stabiliser group of $(1 : 0)$ is equal to $\Gamma_0(N)$.

(e) The quotient of $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ modulo the stabiliser group of $(1 : 0)$ is in bijection with the set of cyclic subgroups of precise order N in $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$. These observations, which may seem unimportant at this point, are at the base of defining level structures for elliptic curves (see the section on modular curves).

One can prove these assertions as an exercise.

It is clear that

$$\Gamma_0(N)/\Gamma_1(N) \xrightarrow{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \mapsto a + N\mathbb{Z}} (\mathbb{Z}/N\mathbb{Z})^\times$$

is a group isomorphism. We also let

$$\chi : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$$

denote a character, i.e. a group homomorphism. We shall extend χ to a map $(\mathbb{Z}/N\mathbb{Z}) \to \mathbb{C}$ by imposing $\chi(r) = 0$ if $(r, N) \neq 1$. The simplest instance of class field theory (here a simple exercise; by ζ_N we mean any primitive N-th root of unity) tells us that

$$\mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q}) \xrightarrow{\mathrm{Frob}_\ell \mapsto \ell} (\mathbb{Z}/N\mathbb{Z})^\times$$

(for all primes $\ell \nmid N$) is an isomorphism. We shall later on also consider χ as a character of $\mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$. The name *Dirichlet character* (here of *modulus* N) is common usage for both.

Modular forms

We now recall the definitions of modular forms. We denote by $\mathbb{H}$ the upper half plane, i.e. the set $\{z \in \mathbb{C} | \mathrm{Im}(z) > 0\}$. The set of cusps is by definition $\mathbb{P}^1(\mathbb{Q}) = \mathbb{Q} \cup \{\infty\}$. Fix integers k and $N \geq 1$. A function

$$f : \mathbb{H} \to \mathbb{C}$$

given by a convergent power series (the $a_n(f)$ are complex numbers)

$$f(z) = \sum_{n=0}^{\infty} a_n(f)(e^{2\pi i z})^n = \sum_{n=0}^{\infty} a_n q^n \quad \text{with } q(z) = e^{2\pi i z}$$

is called a *modular form of weight k for $\Gamma_1(N)$* if

(i) the function $f(\frac{az+b}{cz+d})(cz+d)^{-k}$ is a holomorphic function (still from $\mathbb{H}$ to $\mathbb{C}$) for all $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ and it is bounded when $\mathrm{Im}(z)$ tends to infinity (this condition is called *f is holomorphic at the cusp a/c*), and

(ii) $f(\frac{az+b}{cz+d}) = (cz+d)^k f(z)$ for all $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_1(N)$.

We use the notation $\mathrm{M}_k(\Gamma_1(N)\,;\,\mathbb{C})$. If we replace (i) by

(i)' the function $f(\frac{az+b}{cz+d})(cz+d)^{-k}$ is a holomorphic function and the limit $f(\frac{az+b}{cz+d})(cz+d)^{-k}$ is 0 when $\mathrm{Im}(z)$ tends to ∞ for all $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$,

then f is called a *cusp form*. For these, we introduce the notation $\mathrm{S}_k(\Gamma_1(N)\,;\,\mathbb{C})$.

Let us now suppose that we are given a Dirichlet character χ of modulus N as above. Then we can also consider a variant of (ii) as follows:

(ii)' $f(\frac{az+b}{cz+d}) = \chi(d)(cz+d)^k f(z)$ for all $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(N)$.

Functions satisfying this condition are called *modular forms* (respectively, *cusp forms* if they satisfy (i)') *of weight k, character χ and level N*. The notation $\mathrm{M}_k(N, \chi\,;\,\mathbb{C})$ (respectively, $\mathrm{S}_k(N, \chi\,;\,\mathbb{C})$) will be used.

All these are finite dimensional $\mathbb{C}$-vector spaces and for $k \geq 2$, there are dimension formulae, which one can look up in [Stein]. We, however, point the reader to the fact that for $k = 1$ nearly nothing about the dimension is known (except that it is smaller than the respective dimension for $k = 2$; it is believed to be much smaller, but only very weak results are known to date).

A very famous example of a modular form is Ramanujan's Delta function

$$\Delta(z) = q \prod_{n=1}^{\infty} (1-q^n)^{24}.$$

It belongs to $\mathrm{S}_{12}(1, 1\,;\,\mathbb{C})$.

Hecke operators

At the base of everything that we will do with modular forms are the Hecke operators. One should really define them conceptually. Here is a definition by formulae.

Definition 1.2. *Suppose $f \in \mathrm{M}_k(N, \chi\,; \mathbb{C})$. Recall that we have extended χ so that $\chi(\ell) = 0$ if ℓ divides N. Then the formula*

$$a_n(T_\ell f) = a_{\ell n}(f) + \ell^{k-1}\chi(\ell)a_{n/\ell}(f),$$

where $a_{n/\ell}(f)$ is to be read as 0 if ℓ does not divide n, defines a linear map $T_\ell : \mathrm{M}_k(N, \chi\,; \mathbb{C}) \to \mathrm{M}_k(N, \chi\,; \mathbb{C})$, called the ℓ-th Hecke operator.

The Hecke operators for composite n can be defined as follows (we put T_1 to be the identity):

- $T_{\ell^{r+1}} = T_\ell \circ T_{\ell^r} - \ell^{k-1}\chi(\ell)T_{\ell^{r-1}}$ *for all primes ℓ and $r \geq 1$,*
- $T_{uv} = T_u \circ T_v$ *for coprime positive integers u, v.*

We point out the very important formula (valid for every n)

$$a_1(T_n f) = a_n(f), \tag{1.1}$$

which is a direct consequence of the preceding formulae. From the above formulae it is also evident that the Hecke operators commute among one another. Consequently, the Hecke algebra $\mathbb{T} = \mathbb{T}(\mathrm{M}_k(N, \chi\,; \mathbb{C}))$ which is defined as the $\mathbb{C}$-subalgebra of $\mathrm{End}_{\mathbb{C}}(\mathrm{M}_k(N, \chi\,; \mathbb{C}))$ generated by the Hecke operators T_n for all $n \in \mathbb{N}$ is commutative. Formula (1.1) can be used to show (as an Exercise) that the pairing

$$\mathbb{T} \times \mathrm{M}_k(N, \chi\,; \mathbb{C}) \to \mathbb{C}, \quad (T, f) \mapsto a_1(Tf)$$

is non-degenerate. Thus, the modular forms space is the $\mathbb{C}$-dual of the Hecke algebra.

Moreover, the commutativity of the Hecke operator also implies that eigenspaces for a collection of operators (i.e. each element of a given set of Hecke operators acts by scalar multiplication) are respected by all Hecke operators. Hence, it makes sense to consider modular forms which are eigenvectors for every Hecke operator. These are called *Hecke eigenforms*, or often just *eigenforms*. Such an eigenform f is called *normalised* if $a_1(f) = 1$. Ramanujan's Delta function is an example of a normalised Hecke eigenform.

2 Galois representations

The great importance of modular forms for modern number theory is due to the fact that one may attach a 2-dimensional representation of the Galois group of the rationals to each normalised cuspidal eigenform. The following theorem is due to Shimura for $k = 2$ and due to Deligne for $k \geq 2$.

Theorem 2.1. *Let $k \geq 2$, $N \geq 1$, ℓ a prime, and $\epsilon : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$ a character.*

Then to any normalised eigenform $f \in \mathrm{S}_k(N, \epsilon\,; \mathbb{C})$ with $f = \sum_{n\geq 1} a_n(f)q^n$ one can attach a Galois representation of the rationals

$$\rho_f : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{Q}}_\ell)$$

such that

(i) ρ_f *is irreducible,*

(ii) ρ_f *is odd,*

(iii) for all primes $p \nmid N\ell$ the representation ρ_f is unramified at p and

$$\Phi_p(\rho_f)(X) = X^2 - a_p(f)X + \epsilon(p)p^{k-1}.$$

By reduction and semi-simplification one obtains the following consequence.

Theorem 2.2. *Let $k \geq 2$, $N \geq 1$, ℓ a prime, and $\epsilon : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$ a character.*

Then to any normalised eigenform $f \in \mathrm{S}_k(N, \epsilon\,; \mathbb{C})$ with $f = \sum_{n\geq 1} a_n(f)q^n$ and to any prime ideal Λ of the ring of integers of $\mathbb{Q}_f = \mathbb{Q}(a_n(f) : n \in \mathbb{N})$ with residue characteristic ℓ, one can attach a mod ℓ Galois representation

$$\overline{\rho}_f : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$$

such that

(i) $\overline{\rho}_f$ *is semi-simple,*

(ii) $\overline{\rho}_f$ *is odd,*

(iii) for all primes $p \nmid N\ell$ the representation $\overline{\rho}_f$ is unramified at p and

$$\Phi_p(\rho_f)(X) \equiv X^2 - a_p(f)X + \epsilon(p)p^{k-1} \mod \Lambda.$$

There is also a weight one version of these theorems due to Deligne and Serre.

Theorem 2.3. *Let $N \geq 1$ and $\epsilon : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$ a character.*

Then to any normalised eigenform $f \in \mathrm{S}_1(N, \epsilon\,; \mathbb{C})$ with $f = \sum_{n\geq 1} a_n(f)q^n$ one can attach a Galois representation of the rationals

$$\rho_f : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{C})$$

such that

(i) ρ_f *is odd,*

(ii) for all primes $p \nmid N$ the representation ρ_f is unramified at p and

$$\Phi_p(\rho_f)(X) = X^2 - a_p(f)X + \epsilon(p).$$

Example 2.4. *We present a toy example: $Q(X) = X^6 - 6X^4 + 9X^2 + 23$. Compute factorisations modulo p of $Q(X)$ for some small p with the computer and try to find a pattern describing how many irreducible factors there are. It won't be easy at all (I'd be astonished if you found one without reading on)! But, there is one: There is a unique Hecke eigenform f in $S_1(23)(\mathbb{F}_7)$ (this is with a certain quadratic Dirichlet character); you can also see it in weight 7 or in weight 2 for level $7 \cdot 23$. The pattern is the following. Let p be a prime. Then (with finitely many exceptions):*

- *Q has 2 factors modulo $p \Leftrightarrow a_p(f) = 6$.*
- *Q has 3 factors modulo $p \Leftrightarrow a_p(f) = 0$.*
- *Q has 6 factors modulo $p \Leftrightarrow a_p(f) = 2$.*

This comes from the attached Galois representation $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F}_7)$. There are only the following matrices in the image of ρ:

$$\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right), \quad \left(\begin{smallmatrix}2&0\\0&4\end{smallmatrix}\right), \quad \left(\begin{smallmatrix}4&0\\0&2\end{smallmatrix}\right), \quad \left(\begin{smallmatrix}0&1\\1&0\end{smallmatrix}\right), \quad \left(\begin{smallmatrix}0&2\\4&0\end{smallmatrix}\right), \quad \left(\begin{smallmatrix}0&4\\2&0\end{smallmatrix}\right).$$

The first one has order 1 and trace 2, the second and third have order 3 and trace 6, and the final ones have order 2 and trace 0.

The polynomial Q is Galois over $\mathbb{Q}$. For a given p, $\rho(\mathrm{Frob}_p)$ must be one of these matrices. If the trace is 2, then $\rho(\mathrm{Frob}_p)$ must be the identity and thus have order 1. That means that Q factors completely modulo p (there's a small issue with primes dividing the index of the equation order generated by Q in the maximal order – these primes are next to 7 and 23 the finitely many exceptions mentioned above). If the trace is 0, then the order has to be 2, leading to a factorisation of Q into three fractors modulo p. In the remaining case the trace is 6 and the order is 3, so that Q has three factors modulo p.

3 Serre's Modularity Conjecture

Artin conductor

Let $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$ be a Galois representation. For every prime $p \neq \ell$ define the field

$$K_{\rho,p} := \overline{\mathbb{Q}}_p^{\ker(\rho|_{G_{\mathbb{Q}_p}})}.$$

It is a finite Galois extension of $\mathbb{Q}_p$ with Galois group

$$G^{(p)} := \mathrm{Gal}(K_{\rho,p}/\mathbb{Q}_p) \cong \rho(G_{\mathbb{Q}_p}).$$

It comes equipped with the ramification filtration (in lower numbering):

$$G_i^{(p)} := \{\sigma \in G^{(p)} \mid \forall\, x \in \mathcal{O}_{\rho,p} :\ \sigma(x) - x \in (\pi_{\rho,p})^{i+1}\},$$

where $\mathcal{O}_{\rho,p}$ is the valuation ring of $K_{\rho,p}$ with uniformiser $\pi_{\rho,p}$. We define the integer (it is nontrivial but true that it is an integer!)

$$n_{\rho,p} := \sum_{i=0}^{\infty} \frac{1}{(G_0^{(p)} : G_i^{(p)})} \dim_{\overline{\mathbb{F}}_\ell} \left(V/V^{G_i^{(p)}}\right),$$

called the *conductor exponent of ρ at p.*

Definition 3.1. *The* Artin conductor *of ρ is defined as*

$$N(\rho) := \prod_{p \neq \ell} p^{n_{\rho,p}}.$$

Note that ρ is unramified at $p \neq \ell$ if and only if $p \nmid N(\rho)$.

Fundamental characters

Here we give a description of fundamental characters based on local class field theory (that can be treated as a black box if necessary). One can also develop them in a nice way just using Kummer theory.

Let $K/\mathbb{Q}_p$ be a finite extension with residue field $\mathbb{F}_q$ with $q = p^n$. By local class field theory the Galois group of the maximal totally tamely ramified abelian extension $K^{\mathrm{t.t.r.}}$ of K is isomorphic to $\mathbb{F}_q^\times$.

Definition 3.2. *A character*

$$\phi : G_K \twoheadrightarrow \mathrm{Gal}(K^{\mathrm{t.t.r.}}/K) \to \mathbb{F}_q^\times \overset{\tau}{\hookrightarrow} \overline{\mathbb{F}}_p^\times$$

is said to be a fundamental character (for K) of level n *if $\tau \in \{\tau_1, \ldots, \tau_n\}$, the set of the n field embeddings of $\mathbb{F}_{p^n}$ into $\overline{\mathbb{F}}_p$.*

Remark 3.3. *The fundamental characters of level n are $\{\psi, \psi^p, \psi^{p^2}, \ldots, \psi^{p^{n-1}}\}$ for some fixed fundamental character ψ, since the embeddings τ_i are given by the p-power Frobenius.*

Every character of $\mathrm{Gal}(K^{\mathrm{t.t.r.}}/K)$ is the i-th power of ψ for a unique $0 \leq i < p^n - 1$, since the definition of ϕ only differs from ψ by the fact that $\mathbb{F}_{p^n}^\times \hookrightarrow \overline{\mathbb{F}}_p^\times$ need not come from a field embedding but is allowed to be any group homomorphism. As $\mathbb{F}_{p^n}^\times$ is cyclic, it is uniquely determined by the image of a generator, which has order $p^n - 1$.

The level 1 fundamental character for $K = \mathbb{Q}_p$ is the cyclotomic character (Exercise).

Serre weight

Now we define the weight in Serre's modularity conjecture. We point out that what we present here is the *minimal weight* discussed by Edixhoven [EdixWeight], i.e. the weight that one should use when formulating Serre's conjecture with Katz modular forms over $\overline{\mathbb{F}}_p$ rather than reductions of holomorphic modular forms.

Definition 3.4. *Denote by ψ, ψ^p the two fundamental characters of level 2 and by χ the cyclotomic character.*

Let $\rho_p : G_p \to \mathrm{GL}(V)$ be a Galois representation with V a 2-dimensional $\overline{\mathbb{F}}_p$-vector space. The restriction of ρ_p to the inertia group at p is of the form $\begin{pmatrix} \phi_1 & * \\ 0 & \phi_2 \end{pmatrix}$. The minimal weight $k(\rho_p)$ *of ρ_p is defined as follows.*

(I) Suppose ϕ_1, ϕ_2 are of level 2. After interchanging ϕ_1 and ϕ_2 there are unique integers $0 \leq a < b \leq p-1$ such that

$$\phi_1 = \psi^{a+pb} \text{ and } \phi_2 = \psi^{b+ap}.$$

Let

$$k(\rho_p) = 1 + pa + b.$$

(II) Suppose ϕ_1, ϕ_2 are of level 1.

(1) Suppose that ρ_p is tamely ramified, i.e. $\rho_p(P_p) = 0$. There are unique integers $0 \leq a \leq b \leq p-2$ such that $\phi_1 = \chi^a$ and $\phi_2 = \chi^b$. Let

$$k(\rho_p) = 1 + pa + b.$$

(2) Suppose that ρ_p is not tamely ramified. Then there are unique integers $0 \leq \alpha \leq p-2$ and $1 \leq \beta \leq p-1$ such that

$$\rho_p|_{I_p} \cong \begin{pmatrix} \chi^\beta & * \\ 0 & \chi^\alpha \end{pmatrix}.$$

Let $a = \min(\alpha, \beta)$ and $b = \max(\alpha, \beta)$.

(a) Suppose $\beta \neq \alpha + 1$. Let

$$k(\rho_p) = 1 + pa + b.$$

(b) Suppose $\beta = \alpha + 1$. Let K be the extension of $\mathbb{Q}_p$ such that $G_K = \ker(\rho_p)$.

(i) Suppose K is little ramified. Let

$$k(\rho_p) = 1 + pa + b.$$

(ii) Suppose K is very ramified. Let

$$k(\rho_p) = 1 + pa + b + (p-1).$$

The conjecture and level raising

We finish this course by giving the full statement of Serre's conjecture.

Theorem 3.5 (Serre's modularity conjecture: Khare, Wintenberger, Kisin, Taylor, et al.)**.** *Given any irreducible odd Galois representation $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_p)$. There is a (Katz) modular form on $\Gamma_1(N(\rho))$ of weight $k(\rho|_{G_{\mathbb{Q}_p}})$ such that its attached mod p Galois representation is isomorphic to ρ.*

Remark 3.6. *Serre's modularity conjecture implies, for instance, the following strong finiteness result:*

Fix a prime ℓ and an integer N. Then there are only finitely many odd irreducible Galois representations

$$\overline{\rho} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$$

of conductor dividing $N(\overline{\rho})$.

Reason: Since there are only finitely many values for $k(\overline{\rho})$, each $\overline{\rho}$ must come from one of the finitely many newforms in levels dividing n and weights less than or equal to the maximum value that $k(\overline{\rho})$ can take (that is $\ell^2 - 1$).

There is currently no other way to prove this result!

Remark 3.7. *We point out the following consequence, which is known as* level/weight lowering. *It had been known long before Serre's conjecture due to work of, in particular, Ken Ribet. In fact, it is an essential ingredient in the proof of Serre's conjecture.*

Let $f \in \mathrm{S}_k(N, \epsilon\,; \mathbb{C})$ be an eigenform and consider $\overline{\rho}_f$, the mod ℓ reduction of ρ_f. Then there is an eigenform in $g \in \mathrm{S}_{k(\rho)}(N, \epsilon\,; \mathbb{C})$ (if $k(\overline{\rho}_f) = 1$, one has to use Katz modular forms over $\overline{\mathbb{F}}_\ell$) such that $\overline{\rho}_f \cong \overline{\rho}_g$.

Since in general $N(\overline{\rho})|N$ and $k(\overline{\rho}) \leq k$ will be strictly inequalities, we have lowered the level and the weight in the sense that g is an eigenform in the lower level and the lower weight whose coefficients (at least away from ℓN) are congruent modulo (a prime above) p to those of f.

Theorem 3.8 (Diamond, Taylor: *Level Raising*)**.** *Let $N \in \mathbb{N}$, $k \geq 2$ and let $\ell > k + 1$ be a prime not dividing N. Let $f \in \mathrm{S}_k(N, \epsilon\,; \mathbb{C})$ be a newform such that $\overline{\rho}_f$ is irreducible. Let, furthermore, $q \nmid N$ be a prime such that $q \equiv -1 \bmod \ell$ and $\mathrm{Tr}(\overline{\rho}_f(\mathrm{Frob}_q)) = 0$.*

Then there exists a newform $g \in \mathrm{S}_k(Nq^2, \tilde{\epsilon}\,; \mathbb{C})$ such that $\overline{\rho}_g \cong \overline{\rho}_f$.

Appendix: Sketch of the construction

In this appendix we sketch the construction of these Galois representations.

Let $f = \sum_{n \geq 1} a_n q^n \in S_k(\Gamma_1(N))$ be a Hecke eigenform. Let $\mathbb{T}$ be the sub-$\mathbb{Q}$-algebra inside $\mathrm{End}_{\mathbb{C}}(S_k(\Gamma_1(N)))$ generated by all Hecke operators T_n with $(n, N) = 1$. It is an Artin $\mathbb{Q}$-algebra and hence decomposes as the direct product over the localizations at its maximal ideals:

$$\mathbb{T} \cong \prod_{\mathfrak{m}} \mathbb{T}_{\mathfrak{m}}.$$

Recall that

$$\mathfrak{m} = \ker(\mathbb{T} \xrightarrow{T_n \mapsto a_n} \mathbb{C})$$

is such a maximal ideal. The residue field $\mathbb{T}/\mathfrak{m}$ is equal to the coefficient field $\mathbb{Q}_f := \mathbb{Q}(a_n | (n, N) = 1)$, as one easily sees. If one assumes that f is a newform, then $\mathbb{T}_{\mathfrak{m}} \cong \mathbb{Q}_f$. We shall do that from now on.

From the Eichler-Shimura theorem it follows that the localization $\mathrm{H}^1_{\mathrm{par}}(\Gamma_1(N), \mathbb{Q}[X,Y]_{k-2})_{\mathfrak{m}}$ is a $\mathbb{T}_{\mathfrak{m}} = \mathbb{Q}_f$-vector space of dimension 2. This we will explain now. We compute its dimension after tensoring it over $\mathbb{Q}$ with $\mathbb{C}$:

$$\mathbb{C} \otimes_{\mathbb{Q}} \mathrm{H}^1_{\mathrm{par}}(\Gamma_1(N), \mathbb{Q}[X,Y]_{k-2})_{\mathfrak{m}} \cong \prod_{\sigma : \mathbb{Q}_f \hookrightarrow \mathbb{C}} \mathrm{H}^1_{\mathrm{par}}(\Gamma_1(N), \mathbb{C}[X,Y]_{k-2})_{\sigma(\tilde{\mathfrak{m}})},$$

with $\tilde{\mathfrak{m}} = \ker(\mathbb{C} \otimes_{\mathbb{Q}} \mathbb{T} \xrightarrow{T_n \mapsto a_n} \mathbb{C})$ (this is not so difficult to check). Hence, it suffices to show that the $\mathbb{C}$-dimension of $\mathrm{H}^1_{\mathrm{par}}(\Gamma_1(N), \mathbb{C}[X,Y]_{k-2})_{\sigma(\tilde{\mathfrak{m}})}$ is equal to 2. This is an easy consequence of the Eichler-Shimura isomorphism

$$\mathrm{H}^1_{\mathrm{par}}(\Gamma_1(N), \mathbb{C}[X,Y]_{k-2})_{\sigma(\tilde{\mathfrak{m}})} \cong S_k(\Gamma_1(N))_{\mathfrak{m}} \oplus \overline{S_k(\Gamma_1(N))}_{\mathfrak{m}}.$$

From the q-expansion pairing it follows that the dimension of $S_k(\Gamma_1(N))_{\mathfrak{m}}$ is equal to the dimension of $(\mathbb{C} \otimes_{\mathbb{Q}} \mathbb{T})_{\sigma(\tilde{\mathfrak{m}})}$, which is 1 for a newform.

The Galois representation comes from a $G_{\mathbb{Q}} := \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-action on

$$\mathbb{Q}_\ell \otimes_{\mathbb{Q}} \mathrm{H}^1_{\mathrm{par}}(\Gamma_1(N), \mathbb{Q}[X,Y]_{k-2})_{\mathfrak{m}}.$$

Since

$$\mathbb{Q}_\ell \otimes_{\mathbb{Q}} \mathbb{Q}_f \cong \prod_{\lambda | \ell} \mathbb{Q}_{f,\lambda},$$

we obtain for every $\lambda \mid \ell$ a map

$$G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{Q}_{f,\lambda}) \hookrightarrow \mathrm{GL}_2(\overline{\mathbb{Q}}_\ell).$$

We shall try to motivate why there is a Galois action. One needs to get geometry into the business. Using that $\mathbb{H}$, the upper half plane, is simply connected and, since $\Gamma_1(N)$ acts with finite stabilizers on it (for $N \geq 4$ even with trivial stabilizers), one can identify

$$\mathrm{H}^1(\Gamma_1(N), \mathbb{Q}[X,Y]_{k-2}) \cong \mathrm{H}^1(Y_1(N), \underline{\mathbb{Q}[X,Y]_{k-2}}),$$

where $\underline{\mathbb{Q}[X,Y]_{k-2}}$ is the locally constant sheaf on $Y_1(N)$ (seen as a Riemann surface) which in small enough neighbourhoods looks like $\mathbb{Q}[X,Y]_{k-2}$. Formally, this sheaf can be obtained as the direct image sheaf $(\pi_* \underline{\mathbb{Q}[X,Y]_{k-2}})^{\Gamma_1(N)}$, where $\pi : \mathbb{H} \twoheadrightarrow Y_1(N)$ is the natural projection and now $\underline{\mathbb{Q}[X,Y]_{k-2}}$ stands for the constant sheaf on $\mathbb{H}$ with a suitable $\Gamma_1(N)$-action (we do not go into details here). By a suitable extension to the cusps one finds an isomorphism

$$\mathrm{H}^1_{\mathrm{par}}(\Gamma_1(N), \mathbb{Q}[X,Y]_{k-2}) \cong \mathrm{H}^1(X_1(N), \underline{\mathbb{Q}[X,Y]_{k-2}}).$$

It is very important to note that the Hecke operators respect this isomorphism.

In general, one now has the comparison theorem

$$\mathbb{Q}_\ell \otimes_{\mathbb{Q}} \mathrm{H}^1(X_1(N)(\mathbb{C}), \underline{\mathbb{Q}[X,Y]_{k-2}})_{\mathfrak{m}} \cong \prod_{\lambda|\ell} \mathrm{H}^1_{\mathrm{et}}(X_1(N)_{\mathbb{Q}} \otimes_{\mathbb{Q}} \overline{\mathbb{Q}}, \underline{\mathbb{Q}_\ell[X,Y]_{k-2}})_{\mathfrak{m}_\lambda}$$

with a suitable étale sheaf and the decomposition $\mathbb{Q}_\ell \otimes_{\mathbb{Q}} \prod_{\lambda|\ell} \mathbb{T}_{\mathfrak{m}} \cong \mathbb{T}_{\mathfrak{m}_\lambda} \cong \prod_{\lambda|\ell} \mathbb{Q}_{f,\lambda}$. On the right hand side, one finds the desired $G_{\mathbb{Q}}$-action.

If $k = 2$, there is a slightly more down to earth description, which avoids the use of étale cohomology. We explain this version now. Let $X = X_1(N)(\mathbb{C})$ the modular curve as a Riemann surface. Consider the exact sequence of sheaves:

$$0 \to \underline{\mu_{n,X}} \to \mathcal{O}_X^\times \xrightarrow{x \mapsto x^n} \mathcal{O}_X^\times \to 0.$$

We explain. Exactness of a sequence of sheaves is tested on the stalks. Taking an n-th root of a non-zero holomorphic function in some small enough neighbourhood is always possible, giving the surjectivity. We define $\underline{\mu_{n,X}}$ as the kernel. We claim that it is a locally constant sheaf, which in small enough neighbourhoods looks like μ_n, the n-th roots of unity. This is very easy to see: the n-th power of a function $\phi : U \to \mathbb{C}$ with $U \subset X$ open and connected is identically 1 if and only if $\phi(x) = \zeta$ for some $\zeta \in \mathbb{C}$ with $\zeta^n = 1$ and all $x \in X$. We now pass to the long exact sequence in cohomology

$$0 \to \mu_n(\mathbb{C}) \to \mathbb{C}^\times \xrightarrow{x \mapsto x^n} \mathbb{C}^\times \to \mathrm{H}^1(X, \underline{\mu_{n,X}}) \to \mathrm{H}^1(X, \mathcal{O}_X^\times) \xrightarrow{x \mapsto x^n} \mathrm{H}^1(X, \mathcal{O}_X^\times),$$

using $\mathcal{O}_X(X) = \mathbb{C}$, since X is connected. We obtain

$$\mathrm{H}^1(X, \underline{\mu_{n,X}}) \cong \ker\big(\mathrm{H}^1(X, \mathcal{O}_X^\times) \xrightarrow{x \mapsto x^n} \mathrm{H}^1(X, \mathcal{O}_X^\times)\big).$$

Since $\underline{\mu_{n,X}}$ is locally constant, one finds

$$\mathrm{H}^1(X, \underline{\mu_{n,X}}) \cong \mathrm{H}^1_{\mathrm{par}}(\Gamma_1(N), \mu_n) \cong \mathrm{H}^1_{\mathrm{par}}(\Gamma_1(N), \mathbb{Z}/n\mathbb{Z}),$$

subject to some identification between the n-th roots of unity and $\mathbb{Z}/n\mathbb{Z}$.

Next, we identify $\ker\big(\mathrm{H}^1(X, \mathcal{O}_X^\times) \xrightarrow{x \mapsto x^n} \mathrm{H}^1(X, \mathcal{O}_X^\times)\big)$ with $\mathrm{Jac}(X)(\mathbb{C})[n]$. One has an isomorphism

$$\mathrm{Pic}(X) \cong \mathrm{H}^1(X, \mathcal{O}_X^\times)$$

(see e.g. [Liu]), under which $x \mapsto x^n$ on the right becomes multiplication by n on the left. All together, we now have

$$\mathrm{H}^1_{\mathrm{par}}(\Gamma_1(N), \mathbb{Z}/n\mathbb{Z}) \cong \ker\big(\mathrm{Pic}(X) \xrightarrow{P \mapsto nP} \mathrm{Pic}(X)\big).$$

Elements in the n-torsion of $\mathrm{Pic}(X)$ are necessarily of degree 0, whence

$$\mathrm{H}^1_{\mathrm{par}}(\Gamma_1(N), \mathbb{Z}/n\mathbb{Z}) \cong \mathrm{Pic}(X)[n] = \mathrm{Pic}^0(X)[n] = \mathrm{Jac}(X)[n].$$

Recall that, so far, we have taken X over $\mathbb{C}$ (a Riemann surface), so that $\mathrm{Jac}(X)$ is a complex abelian variety. But, every torsion point is defined over the algebraic numbers, whence we finally get

$$\mathrm{H}^1_{\mathrm{par}}(\Gamma_1(N), \mathbb{Z}/n\mathbb{Z}) \cong \mathrm{Jac}(X_{\mathbb{Q}})(\overline{\mathbb{Q}})[n],$$

which carries a natural $G_{\mathbb{Q}}$-action. Now we replace n everywhere by ℓ^n and pass to the projective limit:

$$\mathrm{H}^1_{\mathrm{par}}(\Gamma_1(N), \mathbb{Z}_\ell) \cong T_\ell(\mathrm{Jac}(X_{\mathbb{Q}}))$$

and

$$\mathrm{H}^1_{\mathrm{par}}(\Gamma_1(N), \mathbb{Q}_\ell) \cong V_\ell(\mathrm{Jac}(X_{\mathbb{Q}})).$$

Of course, these identifications are compatible with the Hecke action, so that we indeed get a $G_{\mathbb{Q}}$-action as desired.

Lecture 4

Applications

In this lecture we will

- sketch the proof of Fermat's Last Theorem (using the validity of Serre's Modularity Conjecture),
- and report on applications of modular Galois representations to the inverse Galois problem.

These notes are not typed. The proof of Fermat's Last Theorem as a consequence of Serre's Modularity Conjecture was one motivation for Serre to formulate the precise version of his conjectures. For details we can refer to Serre's article [Serre] or to the survey article on Fermat's Last Theorem by Darmon, Diamond and Taylor [DDT].

The application to the inverse Galois problem whose proof was sketched in the lecture is part of the joint work with Dieulefait [DiWi]. The other two theorems are proved in [Wi1] and [Wi2].

Bibliography

[Neukirch] Neukirch. *Algebraische Zahlentheorie/Algebraic Number Theory*, Springer.

[DDT] H. Darmon, F. Diamond, R. Taylor. *Fermat's Last Theorem*.

[DiWi] Luis Dieulefait, Gabor Wiese. *On Modular Forms and the Inverse Galois Problem*. Trans. Amer. Math. Soc. 363 (2011), 4569–4584.

[EdixWeight] S. J. Edixhoven. *The weight in Serre's conjectures on modular forms*, Invent. math. **109** (1992), no. 3, 563–594.

[Liu] Q. Liu. *Algebraic geometry and arithmetic curves.* Translated from the French by Reinie Erné. Oxford Graduate Texts in Mathematics, 6. Oxford Science Publications. Oxford University Press, Oxford, 2002.

[Serre] J.-P. Serre. *Sur les représentations modulaires de degré* 2 *de* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Duke Mathematical Journal **54**, No. 1 (1987), 179–230.

[Stein] Stein, W. A. *Modular Forms. A Computational Approach.* AMS, 2007.

[Wi1] Gabor Wiese. *On projective linear groups over finite fields as Galois groups over the rational numbers.* In: 'Modular Forms on Schiermonnikoog' edited by Bas Edixhoven, Gerard van der Geer and Ben Moonen. Cambridge University Press, 2008, 343–350.

[Wi2] Gabor Wiese. *An Application of Maeda's Conjecture to the Inverse Galois Problem.* arXiv:1210.7157, 2012.