Automorphic lifting: Lecture 1-3

J'ignore • 3 Sep 2025

First we review some preliminary materials on algebraic number theory.

There are two isomorphisms (of $\mathbb{R}$-algebras) between $\mathbb{C} \to \mathbb{R}[x]/(x^2+1)$. They are Galois conjugates and no reason to prefer one over another. We can view $\overline{\mathbb{Q}}$ as living inside $\mathbb{C}$, or any other algebraic closures of $\mathbb{Q}$, the point is that it can be equipped with different topologies.

The absolute Galois group $G_{\mathbb{Q}}$ is defined to be the inverse limit of Galois group of $K/\mathbb{Q}$ for K finite Galois over $\mathbb{Q}$, so has a profinite topology. If we compare different constructions of $\overline{Q}$ sitting inside different algebraic closures, we see that $G_{\mathbb{Q}}$ is only pinned down up to conjugation.

$G_{\mathbb{Q}}$ is a very complicated group. For example, John Thompson showed that monster group (largest sporadic simple group) can be realized as a quotient of $G_{\mathbb{Q}}$ in infinitely many ways.

We next review the splitting of primes in quadratic extensions. For each prime p, $\mathcal{O}_{\mathbb{Q}(\sqrt{m})}/p\mathcal{O} \cong \mathbb{F}_p[X]/(f(x))$. If $m = 2, 3 \mod 4$, $f(x)$ can be taken to be $x^2 - m$; otherwise it is $x^2 - x + \frac{1-m}{4}$. The discriminant is $4m$ in the former and m in the latter. If p is odd and $p \mid \Delta$, then $f(x)$ has double root and the same holds for $p = 2$. If p doesn't divide Δ and p odd, then $f(x)$ is irreducible iff m is not a quadratic residue mod p. If $p = 2$, then $m = 1 \mod 4$ and $f(x) = x^2 - x + \frac{1-m}{4}$. Since $f'(x) = -1 \neq 0$, $f(x)$ doesn't have double root. It is irreducible iff $m = 5 \mod 8$.

The conclusion is there are three cases for the isomorphism types of the residue ring $\mathcal{O}_K/p\mathcal{O}_K$:

1. a nonreduced ring $\mathbb{F}_p[y]/(y^2)$ if $p \mid \Delta$;
2. $\mathbb{F}_p \times \mathbb{F}_p$, if p doesn't divide Δ and, either $(m/p) = 1$ if p is odd, or $m = 1 \mod 8$ if $p = 2$;
3. $\mathbb{F}_{p^2}$, remaining case

In case 1, $(p) = \mathfrak{p}^2$; case 2: $p = \mathfrak{p}_1\mathfrak{p}_2$; case 3: (p) is a prime.

We can reinterpret this in the language of schemes: $Spec(\mathbb{Q}(\sqrt{m})) \to Spec(\mathbb{Q})$ is etale morphism, but not very interesting, so we spread it out to one-dimension: $Spec(\mathcal{O}(\sqrt{m})) \to Spec(\mathbb{Z})$ is not etale. The fiber (base change to $Spec(\mathbb{F}_p)$) over (0) or split or inert primes is etale.

For more general $K/\mathbb{Q}$, we want to understand what happens over each prime systematically. To do this we look at the completion $\mathbb{Q}_p$ with the p-adic metric (or the valuation) and the unit disk $\mathbb{Z}_p$ which allows us to do analysis on it.

Over $\overline{\mathbb{Q}_p}$, v_p and $||_p$ uniquely extends but not longer discrete; $\mathcal{O}_{\overline{\mathbb{Q}_p}} = \{x \in \overline{\mathbb{Q}_p} : x \text{ integral over } \mathbb{Z}_p\}$ (if we take this idea further we get to Newton polygon). The open disk $\mathfrak{m}_{\overline{\mathbb{Q}_p}}$ is the set of topologically nilpotent elements. The quotient $\mathcal{O}/\mathfrak{m} \cong \overline{\mathbb{F}_p}$. This is not a Noetherian ring.

Fixing an embedding $\overline{\mathbb{Q}} \to \overline{\mathbb{Q}_p}$ gives a compatible choice of primes above (p) in each finite extension $K/\mathbb{Q}$. More precisely, it determines an extension $||_p$ to $\mathcal{O}_K$ known as a place v of $\mathcal{O}_K$ above p. The values of $||_p$ tells us about how ramified p is in $\mathcal{O}_K$. This also gives $G_{\mathbb{Q}_p} \to G_{\mathbb{Q}}$ by restriction, and we can further look at its image in every finite quotient $Gal(K/\mathbb{Q})$. The image of $I_{\mathbb{Q}_p}$ in $Gal(K/\mathbb{Q})$ is trivial iff p is unramified in K. The image $Gal(K_v/\mathbb{Q}_p)$ is the decomposition group.

Thus to understand ramification and splitting of p in a finite Galois extension $K/\mathbb{Q}$ we can always complete at p. We don't just want to understand the structure of $G_{\mathbb{Q}}$ we should understand the whole collection of subgroups $\{I_p \subseteq G_{\mathbb{Q}_p}\}$, as well as the archimedean place (different ways of embedding K into $\mathbb{C}$ and the absolute value it inherits), and also how $G_{\mathbb{R}} = \{1, c\}$ acts. All of these subgroups are defined up to conjugacy by $G_{\mathbb{Q}}$.

When studying actions of $G_{\mathbb{Q}}$ on topological spaces, we can study the restrictions of the action to these subgroups. The action is unramified at p if it is trivial on $I_{\mathbb{Q}_p}$ and most of the time it is unramified at almost all primes.

The goal of the course is to understand what the following big conjecture is saying:

Big conjecture

> Fix an field-isomorphism $r : \overline{\mathbb{Q}_p} \xrightarrow{\cong} \mathbb{C}$, then there is a bijection from the set of
>
> $$\{\text{Irreeducible algebraic cuspidal automorphic representations of } G = GL_n\}$$
>
> to that of
>
> $$\{\text{Irreducible algebraic continuous representation of } G_{\mathbb{Q}} \to GL_n(\overline{Q_p})\}$$

> where algebraic on the left means π_∞ has Harish-Chandra parameters in $W \setminus (\rho + X^*(T))$; algebraic on the right means 1. unramified at all but finitely many (nonarchimedean) places 2. de Rham at p (condition from p-adic Hodge theory). This bijection is characterised by the 'local-global compatibility' at almost all unramified places. More precisely, at unramified places, we want to match Hecke eigenvalues (Satake paramters) to Frobenius eigenvalues (via r). This match the L-factors.

We can also talk about this conjecture over $F/\mathbb{Q}$, then we need to replace GL_n by $Res_{F/\mathbb{Q}}GL_n$ and $G_\mathbb{Q}$ by G_F.

This specializes to quadratic reciprocity: Take $n = 1$, suppose q is an odd prime, set $q^* := (-1)^{(q-1)/2}q$, note that $q^* = 1 \mod 4$. Note that $\mathbb{Q}(\sqrt{q^*})/\mathbb{Q}$ is ramified only at q, and it is the unique quadratic extension of $\mathbb{Q}$ with this property. We can write down another quadratic extension with this property: Let ζ_q be a primitive q-th root of unity, the cyclotomic extension $\mathbb{Q}(\zeta_q)$ is ramified only at q as well, and if we take the subfield K corresponding to the unique index 2 subgroup of $Gal(\mathbb{Q}(\zeta_q)/\mathbb{Q})$, it will be a quadratic extension K ramified only at q, so it is $\mathbb{Q}(\sqrt{q^*})$. Note that $r \mod q$ is in $Gal(\mathbb{Q}(\zeta_q)/K)$ (the index 2 subgroup) iff $(r/q) = 1$. Equivalently, we can look at the character $\gamma : Gal(\mathbb{Q}(\zeta_q)/\mathbb{Q}) \to Gal(K/\mathbb{Q}) \cong \{\pm 1\}$ which comes from restriction, and the above essentially says that this is $r \mod q \mapsto (r/q)$. Viewing it as a Dirichlet character, it induces an automorphic representation π of GL_1. This π match with γ just by checking on cyclotomic extensions (Kronecker-Weber). The local-global compatibility is the only nontrivial part: The Hecke eigenvalue of π at ℓ is (ℓ/q); on the other hand, this is the Frobenius eigenvalue or γ at ℓ, which is just $\gamma(Frob_\ell)$. Recalling $K = \mathbb{Q}(\sqrt{q^*})$, so for $\ell \neq q$ (unramified places) and $\ell \neq 2$, it will be $+1$ if ℓ splits in $\mathbb{Q}(\sqrt{q^*})$ (since ℓ-th power map is trivial on $\mathbb{F}_\ell \times \mathbb{F}_\ell$) and -1 otherwise. Whether ℓ splits in the quadratic extension depends on whether q^* is a quadratic residue mod ℓ if $\ell \neq 2$ and something else for $\ell = 2$. From this we can get the quadratic reciprocity.