Lecture 1: The Kronecker-Weber Theorem

August 6

§1 Abelian Extensions of $\mathbb{Q}$

Def'n An abelian ext'n of a field is a Galois ext'n with abelian Gal-grp.

E.g. $\mathbb{Q}(\zeta_n)/\mathbb{Q}$, the cyclotomic field, with $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$.

primitive n-th root of unity.

Amazingly: there're NO OTHER examples!

Theorem (Kronecker-Weber) If $K/\mathbb{Q}$ finite abelian,
then $K \subseteq \mathbb{Q}(\zeta_n)$ for some $n \in \mathbb{N}$.

- The smallest n s.t. $K/\mathbb{Q}(\zeta_n)$ is called the conductor of $K/\mathbb{Q}$.

it plays an important role in the splitting behavior of $p \in \mathbb{Q}$ in K.
(will see it a bit later)

Theorem (Local K-W) $K/\mathbb{Q}_p$ finite abelian $\Rightarrow \exists n$ s.t. $K \subseteq \mathbb{Q}_p(\zeta_n)$.

Comment: L/K Gal ext'n with $G = \mathrm{Gal}(L/K)$, $\mathfrak{q} \mid \mathfrak{p}$.

$$\begin{tikzcd} L \arrow[d, dash] & \mathfrak{q} \arrow[d, dash] & \mathfrak{q}' \arrow[dl, dash] \\ K & \mathfrak{p} & \end{tikzcd} \qquad G$$

$G_\mathfrak{q}$ = decomp grp, $I_\mathfrak{q}$ = inertia grp

$\Rightarrow \forall \mathfrak{q}' \mid \mathfrak{p}$, $\mathfrak{q}' = \mathfrak{q}^g$ for some $g \in G$ and $I_{\mathfrak{q}'} = g^{-1} I_\mathfrak{q} g$. $G_{\mathfrak{q}'} = g^{-1} G_\mathfrak{q} g$

(When L/K abelian, conjugations have no effect.)

So it make sense to talk about $I_\mathfrak{p}$ & $G_\mathfrak{p}$.

§2 A Reciprocity Law

Suppose $K/\mathbb{Q}$ abelian with conductor m. Then

$$(\mathbb{Z}/m\mathbb{Z})^\times \cong \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \longrightarrow\!\!\!\!\!\rightarrow \mathrm{Gal}(K/\mathbb{Q}).$$

Constructing the "Artin map": $p \nmid m \Rightarrow p \nmid \Delta_{K/\mathbb{Q}} \Rightarrow p$ unramifies in $K \Rightarrow I_{\mathfrak{p}} = \{1\}$.

(Recall that $|I_{\mathfrak{p}}| = e$, $|G_{\mathfrak{p}}| = ef$.)

⇝ $G_{\mathfrak{p}}$ is generated by $\mathrm{Frob}_{\mathfrak{p}} = F_{\mathfrak{p}} : x \longmapsto x^{p} \bmod \mathfrak{p}$, $\mathfrak{p} | p$.

We can formally extend $p \longmapsto F_p$ to

$$\begin{array}{ccc} \mathrm{Art}_{K/\mathbb{Q}} : S_m & \xrightarrow{\quad \text{Artin} \quad} & \mathrm{Gal}(K/\mathbb{Q}) \\ \parallel & & \cup\!\mid \\ \{p \in \mathbb{Q} \text{ prime}, \ p \nmid m\} & & G_p = \langle F_p \rangle \end{array}$$

Punchline: $\mathrm{Art}_{K/\mathbb{Q}}$ factors through $(\mathbb{Z}/m\mathbb{Z})^* \longrightarrow \mathrm{Gal}(K/\mathbb{Q})$!!

Namely, $r \in (\mathbb{Z}/m\mathbb{Z})^* \longmapsto \boxed{(\zeta_m \mapsto \zeta_m^r) \overset{?}{=} F_p} \Leftrightarrow \zeta_m^r = \zeta_m^p \bmod \mathfrak{p}$, $\mathfrak{p} | p$.

(but $\zeta_m^r(1 - \zeta_m^{p-r}) \equiv 0 \bmod \mathfrak{q}$, $\mathfrak{q} | m$ unless $r - p \equiv 0 \bmod m$)

Artin Reciprocity Laws: Frob_p is governed by ($p \bmod m$).

Some obstructions: (1) Prime ideals in a general number field may not be principal so we can't always take a generator and reduce it modulo sth.

(2) There can be lots of units in a general number field, so even when a prime ideal is principal, it's unclear which generator to choose.

(3) How to explicitly construct generators for all of the abelian ext'ns.

§3 Reduction to the Local Case

Theorem (Minkowski) There are no nontrivial ext'ns of $\mathbb{Q}$ which are unramified everywhere.

Proof of Kronecker-Weber

p ramifies in $K/\mathbb{Q}$ with $\mathfrak{p} | p \Rightarrow K_{\mathfrak{p}} \subseteq \mathbb{Q}_p(\zeta_{n_p})$, $n_p > 0$.

the completion of K at $\mathfrak{p}$.

Let $p^{e_p} \| n_p$, put $n = \prod p^{e_p}$ (finite product for p ramifying in K).

We will prove that $K \subseteq \mathbb{Q}(\zeta_n)$ by proving $K(\zeta_n) = \mathbb{Q}(\zeta_n)$.

$I_p :=$ inertia grp for p in $K(\zeta_n)$.

$U :=$ max'l unramified ext'n of $(K(\zeta_n))_{\mathfrak{p}}$ over $\mathbb{Q}_p$.

$\Rightarrow$ $(K(\zeta_n))_{\mathfrak{p}} = U(\zeta_{p^{e_p}})$. $I_p \cong \mathrm{Gal}(L_{\mathfrak{p}}/U) \cong (\mathbb{Z}/p^{e_p}\mathbb{Z})^\times$

$I :=$ the grp generated by all of the I_p.

$\Rightarrow$ $|I| \leq \prod_p |I_p| \leq \prod_p |(\mathbb{Z}/p^{e_p}\mathbb{Z})^\times| = \prod_p \phi(p^{e_p}) = \phi(n) = [\mathbb{Q}(\zeta_n) : \mathbb{Q}]$.

On the other hand, $K(\zeta_n)^I/\mathbb{Q}$ unramified everywhere

$\Rightarrow$ $K(\zeta_n)^I = \mathbb{Q}$ by Mikowski $\Rightarrow$ $I = \mathrm{Gal}(K(\zeta_n)/\mathbb{Q})$

But then $[K(\zeta_n) : \mathbb{Q}] = |I| \leq [\mathbb{Q}(\zeta_n) : \mathbb{Q}]$ $\Rightarrow$ $\mathbb{Q}(\zeta_n) \subseteq K(\zeta_n)$ $\Rightarrow$ $K(\zeta_n) = \mathbb{Q}(\zeta_n)$. $\square$