$\mathbb{Q}$ - rationals, K - # field, $[K:\mathbb{Q}] = d < \infty$

Primitive not thm: $K = \mathbb{Q}(\gamma)$, $\gamma \in \mathbb{C}$.

K finite, γ algebraic. root of polynomial in $\mathbb{Z}[x]$.

γ will have a minimal poly, $f(x)$, irreducible, degree $= d$).

$f(x)$ has r real roots, $2s$ complex rots, $r+2s = d$.

Thm: There are exactly d embeddings of $K \to \mathbb{C}$ fix $\mathbb{Q}$ pointwise.

$K = \mathbb{Q}(\gamma) \to \mathbb{Q}(\gamma_i)$.

$$\begin{cases} \gamma \longmapsto \gamma_i, \ / \ x \bmod f \mapsto \gamma_i \\ q \longmapsto q \in \mathbb{Q} \end{cases}$$

Exercise: This produces d embeddings, why at most d?

Def: K is normal over $\mathbb{Q} \Leftrightarrow \forall i, \gamma_i \in K \Leftrightarrow$ closed under taking conjugates,

$\Leftrightarrow$ every embedding has image K.

if $K = \mathbb{Q}(\gamma)$ not normal, $\exists \gamma_i \in \mathbb{C}$, $\gamma_i \notin K$.

normal closure: adding all roots.

Examples: • $\mathbb{Q}(\sqrt{d})$ always normal

• $\mathbb{Q}(\sqrt[3]{2})$ not normal. other roots are $\omega\sqrt[3]{2}$, $\omega^2\sqrt[3]{2}$.

but $\omega\sqrt[3]{2}$, $\omega^2\sqrt[3]{2} \notin \mathbb{Q}(\sqrt[3]{2})$

• $\mathbb{Q}(\zeta_n)$ is normal $\forall n$.

Def: $\mathrm{Gal}(K/\mathbb{Q}) = \{$automorphism $K \to K$, fix $\mathbb{Q}$ pointwise$\}$.

K normal $\Leftrightarrow |\mathrm{Gal}(K/\mathbb{Q})| = d$

Main Thm of Galois Thm:

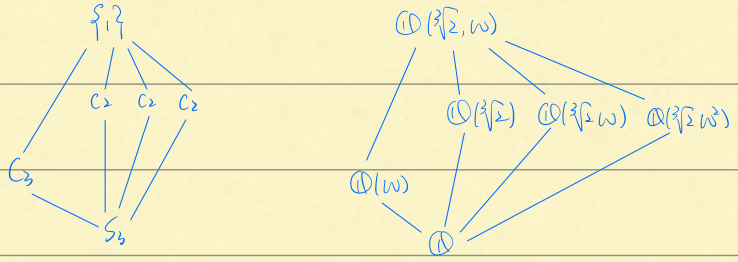
Subgroups of $Gal(K/\mathbb{Q})$ $\Leftrightarrow$ Subfield of K.

If $H \leq Gal(K/\mathbb{Q})$, define $K^H = \{\alpha \in K \mid \forall \sigma \in H, \sigma(\alpha) = \alpha\}$.

$\mathbb{Q}(\sqrt[3]{2})$ not normal, $Gal(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$ trivial.

$\mathbb{Q}(\sqrt[3]{2}, w) = \overline{\mathbb{Q}(\sqrt[3]{2})}$, $Gal(\mathbb{Q}(\sqrt[3]{2}, w)/\mathbb{Q}) = \left\{ \begin{matrix} \sqrt[3]{2} \to \sqrt[3]{2} \\ w \to w \end{matrix}, \begin{matrix} \sqrt[3]{2} \to w\sqrt[3]{2} \\ w \to w \end{matrix}, \begin{matrix} \sqrt[3]{2} \to w^2\sqrt[3]{2} \\ w \to w \end{matrix} \right\} = S_3$.

Exercise:



- $\mathbb{Q}(\sqrt[4]{2})$ not normal, $Gal(\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}) = \left\{ \begin{matrix} \sqrt[4]{2} \to \sqrt[4]{2} \\ \sqrt[4]{2} \to -\sqrt[4]{2} \end{matrix} \right\} = C_2$.
- $\mathbb{Q}(\zeta_n)$ normal, $Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q}) = \{\zeta_n \to \zeta_n^k, (n,k)=1\} \simeq (\mathbb{Z}/n\mathbb{Z})^\times$

Galois Group acting on prime ideals:

- $K = \mathbb{Q}(\gamma)$, $[K:\mathbb{Q}] = d$, $\mathcal{O}_K$ = ring of integers
  - rank d module over $\mathbb{Z}$.
  - unique factorization of ideals.

If p is a prime ideal, then $(p) = p\mathcal{O}_K = \prod p_i^{e_i}$

$Nm(p_i) = p^{f_i}$, $\sum_{i=1}^{g} e_i f_i = d$.

- If $\exists e_i > 1$, p ramifies in $\mathcal{O}_K$.
- If $e_i = 1$, $g = 1$, p stays inert.
- If $\forall e_i = f_i = 1$, p splits completely.

Assume $K/\mathbb{Q}$ normal

Let $\mathfrak{p}_i$ prime laying over p.

if $\sigma \in Gal(K/\mathbb{Q})$, what is $\sigma(\mathfrak{p}_i)$?

We know that $\sigma(p)=p$. $\Rightarrow \sigma(\pi \mathfrak{p}_i^{e_i}) = \pi \mathfrak{p}_i^{e_i}$

$\Rightarrow \sigma(\mathfrak{p}_i)$ also a prime over p.

If $\mathfrak{p}_i \neq \mathfrak{p}_j$, $\exists \sigma \in G$, $\sigma(\mathfrak{p}_i) = \mathfrak{p}_j$.

So if $K/\mathbb{Q}$ normal, we can simplify the factorization $p\mathcal{O}_K = \prod_{i=1}^{g} \mathfrak{p}_i^{e}$

Examples: $\mathbb{Q}(\zeta_n)$

① $\mathcal{O}_{\mathbb{Q}(\zeta_n)} = \mathbb{Z}(\zeta_n)$

② p ramifies in $\mathbb{Z}(\zeta_n) \Leftrightarrow p \mid n$

③ If $p \nmid n$, f_p is the order of p in $(\mathbb{Z}/n\mathbb{Z})^\times$

④ In particular, p splits completely iff $p \equiv 1 \pmod n$.

remains inert iff p generates $(\mathbb{Z}/n\mathbb{Z})^\times$.

Set up: (K normal)

$$\begin{array}{ccccc} K & \supset & \mathcal{O}_K & \supset & \mathfrak{p} \\ | & & | & & | \\ \mathbb{Q} & \supset & \mathbb{Z} & \supset & (p) \end{array}$$

Assume K normal,

Def: The decomposition group of $\mathfrak{p}$ over p $D(\mathfrak{P}/p) = \{\sigma \in Gal(\mathfrak{P}/p) \mid \sigma(\mathfrak{p}) = \mathfrak{p}\}$.

$p\mathcal{O}_K = \prod_{i=1}^{g} \mathfrak{p}_i^{e}$, $Nm(\mathfrak{p}_i) = p^{d/g} = p^f$

Recall: $\forall \sigma \in G$, $\sigma(\mathfrak{p}_i) = \mathfrak{p}_j$

Could also use the def: $D(\mathfrak{P}/p) = \{\sigma \in G \mid \sigma(x) \equiv 0 \bmod \mathfrak{p} \Leftrightarrow x \equiv 0 \bmod \mathfrak{p}\}$.

Exercise: $D(\mathfrak{P}/p)$ is actually a group.

Def: Inertia group $I(\mathfrak{P}/p) = \{\sigma \in G \mid \sigma(x) \equiv x \bmod \mathfrak{P} \ \forall x \in \mathcal{O}_K\}$.

Consider $\mathcal{O}_K/\mathfrak{P}$ = finite field extension of $\mathbb{F}_p$ of degree f where $Nm(\mathfrak{P}) = p^f$

Every $\sigma \in G$ restricts to an automorphism of $\mathcal{O}_K \to \mathcal{O}_K$.

If $\sigma \in D(\mathfrak{P}/p)$, induce a map $\mathcal{O}_K/\mathfrak{P} \to \mathcal{O}_K/\mathfrak{P}$ ($\mathcal{O}_K \xrightarrow{\sigma} \mathcal{O}_K \xrightarrow{\bmod \mathfrak{P}} \mathcal{O}_K/\mathfrak{P}$, if $\sigma \in D$,

the kernel of ↗ has to be $\mathfrak{P}$, so $\mathcal{O}_K/\mathfrak{P} \xrightarrow{\bar{\sigma}} \mathcal{O}_K/\mathfrak{P}$).

Note: $\bar{\sigma}$ fixes $\mathbb{F}_p = \mathbb{Z}/(p)$ since σ fixes $\mathbb{Z}$

Recall: all extensions of $\mathbb{F}_p$ are normal, unique one of degree n, $\forall n \in \mathbb{N}$.

$\mathbb{F}_{p^n}$ is the splitting field of $\frac{X^{p^n}-1}{X-1}$ over $\mathbb{F}_p$.

$Gal(\mathbb{F}_{p^n}/\mathbb{F}_p) = C_n$, cyclic of order n.

generator is Frob $x \mapsto x^p$, $\mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$.

We have the map $D(\mathfrak{P}/p) \xrightarrow{\varphi} Gal(\mathcal{O}_K/\mathfrak{P}/\mathbb{F}_p)$ ($\sigma \longmapsto \bar{\sigma}$)

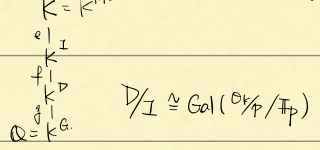
kernel consists of all $\sigma \in D(\mathfrak{P}/p)$ that maps to the identity isomorphism.

$|Gal(\mathcal{O}_K/\mathfrak{P}/\mathbb{F}_p)| = f$

$D/I \cong \operatorname{im}\varphi$, fact: $D/I = f \Rightarrow \varphi$ is surjective, $\operatorname{im}(\varphi) = Gal(\mathcal{O}_K/\mathfrak{P}/\mathbb{F}_p)$

Proof using transitivity, stabilizer, $efg = d$

other proof:



$D/I \cong Gal(\mathcal{O}_K/\mathfrak{P}/\mathbb{F}_p)$

If $I = \{1\}$ aka $e = 1$, then Frob (generator of RHS) is an element in D.

Note: D/I must be cyclic.

Example: $\mathbb{Q}(\zeta_{23}) \supseteq \mathbb{Z}(\zeta_{23})$. How does (2) factor?

minimal poly is $\frac{X^{23}-1}{X-1}$, compute D and I.

Set up: ($K/\mathbb{Q}$ normal)

$$\begin{array}{ccccc} K & \supset & \mathcal{O}_K & \supset & \mathfrak{p} \\ | & & | & & | \\ \mathbb{Q} & \supset & \mathbb{Z} & \supset & (p) \end{array}$$

Last time: $|I| = 1$ i.e. p unramified. Then $D(\mathfrak{p}/p) \xrightarrow{\sim} Gal(\mathcal{O}_K/\mathfrak{p}/\mathbb{F}_p)$ ↷ generator of

$\varphi \in$ Frob

φ ($\varphi(\mathfrak{p}/p)$) satisfies: $\varphi(x) \equiv x^{|\mathbb{Z}/(p)|} \pmod{\mathfrak{p}}$, $\forall x \in \mathcal{O}_K$.

Exercise: for a prime $\mathfrak{p}'$ above p, $\varphi(\mathfrak{p}'/p) = \sigma \circ \varphi(\mathfrak{p}/p) \circ \sigma^{-1}$, where $\sigma(\mathfrak{p}) = \mathfrak{p}'$

Summary Thm: If $K/\mathbb{Q}$ normal and $p \in \mathbb{Z}$ is unramified in K. For each $\mathfrak{p}$ in K above p,

there is a unique $\varphi \in Gal(K/\mathbb{Q})$ s.t. $\varphi(x) \equiv x^{|\mathbb{Z}/p|} \pmod{\mathfrak{p}}$

② If $K/\mathbb{Q}$ abelian, φ only depends on p and $\varphi(x) \equiv x^p \pmod{p\mathcal{O}_K}$.

③ $\varphi(\mathfrak{p}/p)$ has order $f(\mathfrak{p}/p)$ in $D(\mathfrak{p}/p)$

$\sigma_k \longmapsto k \iff \sigma(\zeta_n) = \zeta_n^k$.

Example: $K = \mathbb{Q}(\zeta_n)$ n odd, $Gal(K/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$

For any $p \nmid n$, p is unramified

$\varphi(\mathfrak{p}/p) \overset{②}{=}$ φ_p satisfies $\varphi_p(x) \equiv x^p \pmod{p\mathbb{Z}[\zeta_n]}$, $\forall x \in \mathcal{O}_K$.

Q: How is φ_p related to σ_p? (Same)

On a general element of $\mathcal{O}_K = \mathbb{Z}[\zeta_n]$

$$\sigma_p(a_0 + a_1\zeta_n + a_2\zeta_n^2 + \cdots + a_{\varphi(n)-1}\zeta_n^{\varphi(n)-1}) = a_0 + a_1\zeta_n^p + a_2\zeta_n^{2p} + \cdots + a_{\varphi(n)-1}\zeta_n^{(\varphi(n)-1)p}$$

For this automorphism to be Frob at p (φ_p), wts:

$$a_0 + a_1\zeta_n^p + a_2\zeta_n^{2p} + \cdots + a_{\varphi(n)-1}\zeta_n^{(\varphi(n)-1)p} \equiv \left(a_0 + a_1\zeta_n + a_2\zeta_n^2 + \cdots + a_{\varphi(n)-1}\zeta_n^{\varphi(n)-1}\right)^p \pmod{p\mathcal{O}_K}.$$

Exercise: Show that if f any poly over $\mathbb{F}_p$, then $f(x^p) = (f(x))^p$

Change lenses:

Let $K/\mathbb{Q}$ abelian (i.e. $Gal(K/\mathbb{Q})$ abelian)

By exercise, $\varphi(\mathfrak{P}/p)$ and $\varphi(\mathfrak{P}'/p)$ are conjugate in $Gal(K/\mathbb{Q})$, call them φ_p

Rebrand: $\{$rational primes unramified in $K\} \longrightarrow Gal(K/\mathbb{Q})$

$$p \longmapsto \varphi(p) \quad \text{(well-defined in } (\mathbb{Z}/n\mathbb{Z})^\times\text{)}$$

Example: $\{p \nmid n\} \longrightarrow Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q})$

$$p \longmapsto (\zeta_n \longmapsto \zeta_n^p)$$

Another map: $\{$prime in $K\} \longrightarrow Cl(K)$

$$\mathfrak{p} \longmapsto [\mathfrak{p}]$$

Class field theory says every K has an extension K_H, known as the Hilbert class field, s.t. $Gal(K_H/K) \cong Cl(K)$

- totally unramified or unramified everywhere at each prime $\mathfrak{p}$ of $\mathcal{O}_K$.
- principal prime ideals of K split completely.

Generalize the rebrand:

$$\{\text{primes of } K\} \longrightarrow Gal(K_H/K)$$

$$\mathfrak{p} \longmapsto \text{Frob}(\mathfrak{p})$$

$$\updownarrow$$

$$\mathfrak{p} \longmapsto [\mathfrak{p}]$$

$$\{\text{primes of } K\} \longrightarrow Cl(K)$$

To every # Field K, $\mathfrak{P} \mid p$, we can construct a local field $K_\mathfrak{p}$ over a new base field $\mathbb{Q}_p$, and if K normal over $\mathbb{Q}$, then $K_\mathfrak{p}$ is normal over $\mathbb{Q}_p$ with $D(\mathfrak{P}/p) = Gal(K_\mathfrak{p}/\mathbb{Q}_p)$

$\mathbb{Z}_p = \varprojlim_{n\to\infty} \mathbb{Z}/p^n\mathbb{Z} = \{ a=(a_1, a_2, \cdots, a_i, \cdots) \mid a_i \in \mathbb{Z},\ a_i \equiv a_{i+1} \mod p^i \}$

$\mathbb{Z} \hookrightarrow \mathbb{Z}_p \qquad x \mapsto (x, x, x, \cdots)$

p-ecimal description: Let $a = (a_1, a_2, \cdots) \in \mathbb{Z}_p$

Recursion: $\exists b_0 \in \{0, 1, \cdots, p-1\}$ s.t. $a_1 \equiv b_0 \ (p)$ $(\Rightarrow \forall i,\ a_i \equiv b_0 \ (p))$

$\Rightarrow a_2 \equiv b_0 + b_1 p \ (p^2)$, $a_3 = b_0 + b_1 p + b_2 p^2 \ (p^3)$

$\cdots\cdots$ $a_i = b_0 + b_1 p + \cdots + b_{i-1} p^{i-1} \ (p^i)$

Create from the recursion $(\cdots, b_i, \cdots, b_2, b_1, b_0) \to$ value $= \sum_0^\infty b_i p^i$.

Exercise: one $\frac{1}{2}, \cdots \frac{1}{6}, \frac{1}{8}$ elements of $\mathbb{Z}_7$, what about $\frac{1}{7}$?

$\mathbb{Q}_p = \mathrm{Frac}(\mathbb{Z}_p)$

$\mathbb{Z}_p$ is a Dedekind domain, but it only has one non-zero prime/maximal ideal: $p\mathbb{Z}_p = (p)$

This is principal, and so $\mathbb{Z}_p$ is a PID.

$\mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$

p-ecimal description of $\mathbb{Q}_p$: $b \in \mathbb{Q}_p$ can be written as $\sum_{i=-k}^\infty b_i p^i$ for some $k > 0$

A local field is a finite extension of $\mathbb{Q}_p$

↳ Let $f(x) \in \mathbb{Q}_p[x]$ irre,

$\mathbb{Q}_p[x]/(f(x))$ or $\mathbb{Q}_p(\alpha)$, $f(\alpha) = 0$.

$K = \mathbb{Q}_p(\alpha) \longrightarrow$ rings of integers $\mathcal{O}_K$

$\mathbb{Q}_p \qquad \supseteq \qquad \mathbb{Z}_p$

$\mathcal{O}_K$ – only only non-zero prime ideal $\mathfrak{p}$ and $\mathfrak{p} \cap \mathbb{Z}_p = p\mathbb{Z}_p = (p)$.

$\mathcal{O}_K/\mathfrak{p}$ is a finite extension of $\mathbb{F}_p$

Local set up: $K \supset \mathcal{O}_K \supset \mathfrak{p}$

$\mathbb{Q}_p \supset \mathbb{Z}_p \supset p\mathbb{Z}_p$

Assume K normal, $\sigma \in Gal(K/\mathbb{Q}_p)$ sends $\sigma(\mathfrak{p}) = \mathfrak{p}$

$\sigma: K \to K$ restrict to $\sigma: \mathcal{O}_K \to \mathcal{O}_K$, compose $\mathcal{O}_K \xrightarrow{\sigma} \mathcal{O}_K \xrightarrow{\pi} \mathcal{O}_K/\mathfrak{p}$.

$\mathbb{Z}_p$ is the completion of $\mathbb{Z}$ wrt the p-adic absolute value.

First, the p-adic valuation:

if $x \in \mathbb{Z} \setminus \{0\}$, $\mathrm{val}_p(x) =$ max power of p dividing x

$\mathrm{val}_p(0) = \infty$

Extend to $\mathbb{Q}$: $\mathrm{val}_p(\frac{x}{y}) = \mathrm{val}_p(x) - \mathrm{val}_p(y)$

$\mathrm{val}_p: \mathbb{Q} \to \mathbb{Z} \cup \{\infty\}$.

Def: For $x \in \mathbb{Q}$, define the p-adic absolute value

$|x|_p = p^{-\mathrm{val}_p(x)}$ if $x \neq 0$.

$|0|_p = 0$

Idea: $|x-y|_p$ is small if a large power of p divides their difference.

$\Leftrightarrow x \equiv y \pmod{p^k}$ for large k.

A sequence $\{x_n\}$ in a metric space X is a Cauchy sequence wrt $|\cdot|$ if $\forall \varepsilon > 0$,

$\exists N$, $\forall m, n > 0$, $|x_n - x_m| < \varepsilon$.

$\{x_n\}, \{y_n\}$ are equivalent $\{x_n\} \sim \{y_n\} \Leftrightarrow \lim_{n\to\infty} |x_n - y_n|_p = 0$.

$(\mathbb{Q}, |\cdot|_p)$ = non-archimedian metric space, i.e. it satisfies

① $|x|_p = 0 \Leftrightarrow x = 0$

② $|xy|_p = |x|_p |y|_p$

③ $|x-y|_p \leq \max\{|x|_p, |y|_p\}$ ← much stronger than triangle ineq.

Notation: $|\cdot|_\infty : \mathbb{Q} \to \mathbb{Q}$ is archimedian absolute value

For $x \in \mathbb{Q}$, $|x|_\infty = \begin{cases} x & x \geq 0 \\ -x & x < 0 \end{cases}$

- $\mathbb{R}$ is the completion of $\mathbb{Q}$ wrt $|\cdot|_\infty$
- $\mathbb{Q}_p$ is the completion of $\mathbb{Q}$ wrt $|\cdot|_p$
- $\mathbb{Z}_p$ is the completion of $\mathbb{Z}$ wrt $|\cdot|_p$

Completion: set of equivalence classes of Cauchy sequences of $\mathbb{Q}$ / $\mathbb{Z}$ wrt $|\cdot|_?$

Generalization: For a # field K, we can take the completion of K wrt $|\cdot|_\mathfrak{p}$, $\mathfrak{p} \leq K$ prime ideal.

Galois Theory of Local Fields:

Local set up:
$$\begin{array}{ccccc} K & \supset & \mathcal{O}_K & \supset & \mathfrak{p} \\ | & & | & & | \\ \mathbb{Q}_p & \supset & \mathbb{Z}_p & \supset & p\mathbb{Z}_p \end{array}$$

$K = \mathbb{Q}_p(\alpha)$, i.e. $f(\alpha) = 0$, K normal

Then $\sigma \in Gal(K/\mathbb{Q}_p)$ must send $\sigma(\mathfrak{p}) = \mathfrak{p}$ (Exercise?)

$\sigma : K \to K$ restricted to $\sigma : \mathcal{O}_K \to K$. If we show that $\sigma(\mathcal{O}_K) \leq \mathcal{O}_K$.

Compose: $\mathcal{O}_K \xrightarrow{\sigma} \mathcal{O}_K \xrightarrow{\pi} \mathcal{O}_K/\mathfrak{p}$.

Exercise: What is the kernel of this composition is the prime ideal $\mathfrak{p}$.

$\mathcal{O}_K/\mathfrak{p} \xrightarrow{\bar{\sigma}} \mathcal{O}_K/\mathfrak{p}$

Define a map $\underbrace{Gal(K/\mathbb{Q}_p)}_{|\ |=[K:\mathbb{Q}_p]} \xrightarrow{\star} Gal(\mathcal{O}_K/\mathbb{F}_p)$

$\sigma \longmapsto \bar{\sigma}$

K # field $\Rightarrow$ surjective

$Gal(K/\mathbb{Q}_p)$ is its own decomposition group.

Q: What is the kernel of $\star$?

$I(K/\mathbb{Q}_p) = I(\mathfrak{P}/p) = \{\sigma \in Gal(K/\mathbb{Q}_p) \mid \sigma(\alpha) \equiv \alpha \ (\mathfrak{P}),\ \forall \alpha \in \mathcal{O}_K\}$.

$K/\mathbb{Q}_p$ is unramified if $e = |I(K/\mathbb{Q}_p)| = 1$

In this case, $Gal(K/\mathbb{Q}_p) \cong Gal(\mathcal{O}_K/\mathbb{F}_p)$

(generated by Frob $x \mapsto x^p$)

$Frob_{\mathfrak{P}} \longleftarrow Frob$

$Frob_{\mathfrak{P}}(\alpha) \equiv \alpha^p \pmod{\mathfrak{P}}$, $\forall \alpha \in \mathcal{O}_K$.

Fact: $\forall\ \mathbb{F}_{p^n}/\mathbb{F}_p$, $\exists!$ unramified extension K of $\mathbb{Q}_p$ of degree n with residue field $\mathbb{F}_{p^n}$

In general, describing the field extension of $\mathbb{Q}_p$, especially the Galois theory is much easier (still complicated) than that of (global) number fields.

(Lmfdb.org)

Let $K/\mathbb{Q}$ # field, $K = \mathbb{Q}(\alpha)$, $f(\alpha) = 0$

Let $K_{\mathfrak{P}}/\mathbb{Q}_p$ a local extension, $K_{\mathfrak{P}} = \mathbb{Q}_p(\alpha)$ ($f(x)$ could be reducible over $\mathbb{Q}_p$)

If $f(x)$ reducible $\Rightarrow K_{\mathfrak{P}}$ is not a field, but a product of local field extensions over $\mathbb{Q}_p$, one for each prime in the prime factorization of p.

Returning to the algebraic definition of $\mathbb{Z}_p = \varprojlim_{n>0} \mathbb{Z}/p^n\mathbb{Z}$,

Assume K Galois, let $p\mathcal{O}_K = (\mathfrak{P}_1 \mathfrak{P}_2 \cdots \mathfrak{P}_g)^e$ where $Nm(\mathfrak{P}_i) = p^f$

$\forall$ fixed $p = p_i$ above $p\mathcal{O}_K$,

$$\mathcal{O}_{K,p} = \varprojlim \mathcal{O}_K/p^n$$

Define $K_p = \mathrm{Frac}(\mathcal{O}_{K,p}) \Rightarrow K_p$ is normal over $\mathbb{Q}_p$

Note: K_p above is as if $\mathrm{Frac}(\varprojlim \mathcal{O}_K/p^n)$

There is a map $\mathrm{Gal}(K_p/\mathbb{Q}_p) \to \mathrm{Gal}(K/\mathbb{Q})$

$$\sigma \longmapsto \sigma|_K.$$

- restrict: $\sigma : K_p \to K_p$

$$\sigma|_K : K \to K_p$$

① It will fix $\mathbb{Q}_p \cap K = \mathbb{Q}$

② Image of $\sigma|_K$ is contained in K.

Fact: $D(\mathfrak{P}/p) \cong \mathrm{Gal}(K_p/\mathbb{Q}_p)$

Global case:	Local case:
K	K_p
$e \mid$	$e \mid$
K^I	K_p^I
$f \mid$	$f \mid$
K^D	$\mathbb{Q}_p = K_p^G$
$g \mid$	
$\mathbb{Q} = K^G$	

Ex: For what p, $\sqrt{2} \in \mathbb{Q}_p$

$\sqrt{2} \in \mathbb{Q}_p \Leftrightarrow x^2 - 2$ factors over $\mathbb{Z}_p$

$\Rightarrow$ ..... $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$

Kummer Factorization Theorem:

x^2-2 factors in $\mathbb{F}_p \iff p=p_1p_2$, splits completely in $\mathbb{Q}(\sqrt{2})$

So $\sqrt{2}\in\mathbb{Q}_p \iff \sqrt{2}\in\mathbb{F}_p$.

Eg: $p=7$, $(\pm 3)^2=2$.

If $K=\mathbb{Q}(\sqrt{2})$, $7\mathcal{O}_K=\mathfrak{p}_1\mathfrak{p}_2$

Then $D(\mathfrak{P}/7)\cong Gal(K_{\mathfrak{P}}/\mathbb{Q}_7)=\{e\}$

$\Rightarrow K_{\mathfrak{P}}=\mathbb{Q}_7 \Rightarrow \mathbb{Q}_7(\sqrt{2})=\mathbb{Q}_7$

Kronecker-Weber Thm:

Every finite abelian extension of $\mathbb{Q}$ lies in a cyclotomic field $\mathbb{Q}(\zeta_m)$

Thm: Every finite abelian extension of $\mathbb{Q}_p$ lies in a cyclotomic field $\mathbb{Q}_p(\zeta_m)$

Pf: (From global from local)

Let $K/\mathbb{Q}$ be finite, abelian.

$\forall$ ramified p of $\mathbb{Q}$, pick a prime $\mathfrak{p}$ in K above p, let $K_{\mathfrak{p}}$ be the completion of K "at $\mathfrak{p}$"

We have $Gal(K_{\mathfrak{p}}/\mathbb{Q}_p)\cong D(\mathfrak{p}/p)\le Gal(K/\mathbb{Q})$

$\Rightarrow K_{\mathfrak{p}}$ is finite abelian. By local, $K_{\mathfrak{p}}\le\mathbb{Q}_p(\zeta_{mp})$, $m_p\ge 1$.

Define $m=\prod_{p \text{ ramified}} p^{Vol_p(m_p)}$ (finite since p finitely many p)

Let $L=K(\zeta_m)$

strategy = show $L=\mathbb{Q}(\zeta_m) \Rightarrow \mathbb{Q}(\zeta_m)$ contains K.

↓ compositum, the smallest field contains both

$L=K\cdot\mathbb{Q}(\zeta_m)$, both $K, \mathbb{Q}(\zeta_m)$ galois.

So $Gal(L/\mathbb{Q})$ is isomorphic to a subgp $G\le Gal(K/\mathbb{Q})\times Gal(\mathbb{Q}(\zeta_m)/\mathbb{Q})$

Let $\mathfrak{q}$ be a prime of L above a ramified p of K.

Let $L_{\mathfrak{q}}$ of L at $\mathfrak{q}$ be the completion at $\mathfrak{q}$. $L_{\mathfrak{q}}$ is finite abelian $/\mathbb{Q}_p$

We can write $L_{\mathfrak{q}}=K_{\mathfrak{p}}\cdot\mathbb{Q}_p(\zeta_m)$

Let F_q = maximal unramified extension of $\mathbb{Q}_p$ in L_q

$\Rightarrow L_q/F_q$ is totally ramified ($f=1$)

$\Rightarrow Gal(\bar{\mathbb{Q}}/F_q) = I(\mathfrak{p}) = I(p) \leq Gal(\bar{\mathbb{Q}}/\mathbb{Q})$

L_q | totally ramified.

F_q | unramified

$\mathbb{Q}_p$

Fact: $\mathbb{Q}_p(\zeta_m)/\mathbb{Q}_p$ is ramified $\Leftrightarrow p \mid m$ $(e>1)$

is totally ramified $\Leftrightarrow m = p^k$ $(f=1)$

is unramified $\Leftrightarrow p \nmid m$

① $K_p \leq \mathbb{Q}_p(\zeta_{mp})$

② $\mathbb{Q}_p(\zeta_{\frac{mp}{p^{v_p(mp)}}})$ is unramified.

③ $L_q = F_q(\zeta_{p^{v_p(mp)}})$

$\Rightarrow K_p \leq F_q(\zeta_{p^{v_p(mp)}})$

$p^{v_p(mp)}$ = highest power of p dividing mp

Moreover, $F_q \cap \mathbb{Q}_p(\zeta_{p^{v_p(mp)}}) = \mathbb{Q}_p$

Since $I(p) \cong Gal(\bar{\mathbb{Q}}/F_q) = Gal(F_q(\zeta_{p^{v_p(mp)}})/F_q)$

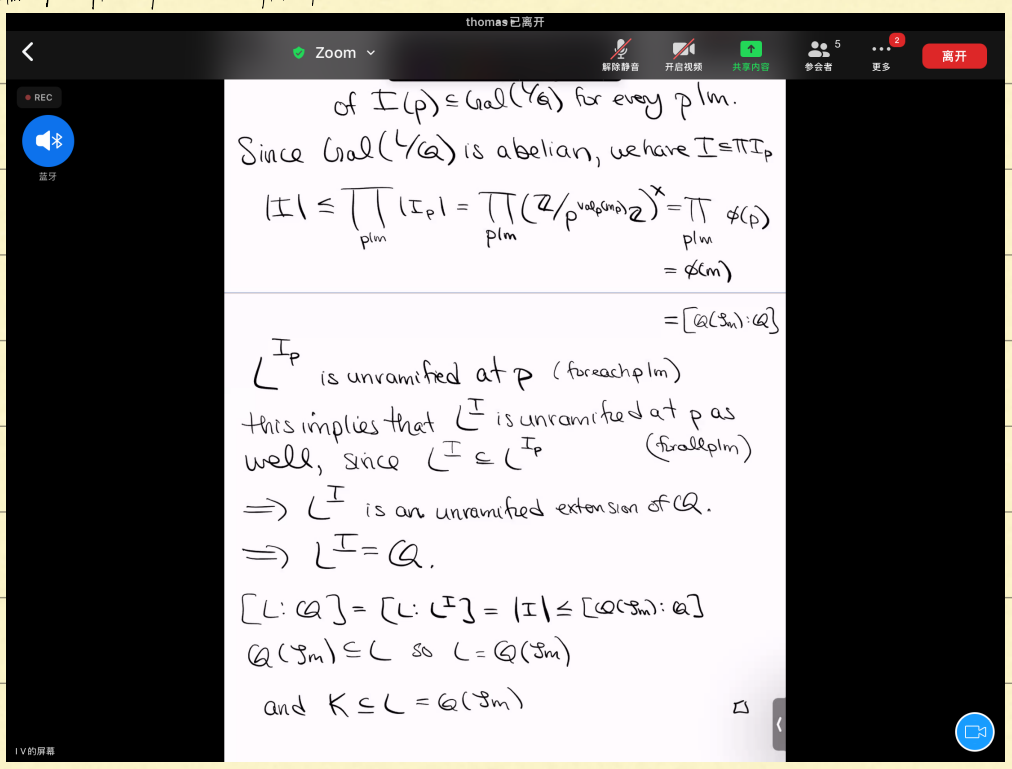
$\cong Gal(\mathbb{Q}_q(\zeta_{p^{v_p(mp)}})/\mathbb{Q}_q)$

$\cong (\mathbb{Z}/p^{v_p(mp)}\mathbb{Z})^\times$

Let I be the group generated by all of $I(p) \leq Gal(\bar{\mathbb{Q}}/\mathbb{Q})$ for every $p \mid m$

Since $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$ abelian, we have $I \leq \prod I_p$.

$|I| \leq \prod_{p \mid m} |I_p| = \prod_{p \mid m} (\mathbb{Z}/p^{v_p(mp)}\mathbb{Z})^\times = \prod_{p \mid m} \varphi(p) = \varphi(m) = I \cdot \mathbb{Q}(\zeta$



Following section 7.4 of Andrew Sutherland.

$$\begin{array}{ccccc} L & > & B\,\mathcal{O}_K & > & \mathfrak{P} \\ | & & | & & | \\ K & > & A\,\mathbb{Z} & > & \mathfrak{p}_{(p)} \end{array} \quad \text{in}$$

Assume $K/\mathbb{Q}$ Galois, if $\mathfrak{P}/p$ unramified.

recall: $\sigma(\mathfrak{P}/p)$ is a Frobenius element. It is the unique element σ s.t. $\forall x \in \mathcal{O}_K$,

we have $\sigma(x) \equiv x^{\#\mathbb{F}_p} \bmod \mathfrak{P}$

Exercise: If p splits completely, then what can we say about $\sigma(\mathfrak{P}/p)$

The decomposition group $D(\mathfrak{P}/p)$ has size of $(|I| = e, |D/I| = f)$, so D is trivial.

and $\sigma(\mathfrak{P}/p)$ generates $D(\mathfrak{P}/p)$ when $I(\mathfrak{P}/p)$ trivial and so $\sigma(\mathfrak{P}/p) = 1$.

Important: Galois L/K is complete determined by the set of primes in K that split complete in L.

Character notation for $\sigma(\mathfrak{P}/p)$:

If $K/\mathbb{Q}$ extension, $\chi_{K/\mathbb{Q}}$ character on primes p of $\mathbb{Q}$ (K abelian)

$$\chi_{K/\mathbb{Q}}(p) = \begin{cases} 1 & \text{if } p \text{ splits completely} \\ ?? \; \sigma(\mathfrak{P}/p) & \text{otherwise} \end{cases}$$

(otherwise → $\mathfrak{P}$ of K)

Another notation: $\left(\frac{K/\mathbb{Q}}{p}\right)$ ← Artin Symbol

Review of fractional ideals:

If $I \subseteq \mathcal{O}_K$ non-zero ideal, define the $\mathcal{O}_K$-module

$$I^{-1} = \{x \in K \mid xI \subseteq \mathcal{O}_K\} \subseteq K$$

Example:

denominators

Example: Let $I = a\mathbb{Z}$ in $\mathbb{Z}$

$$I^{-1} = \{x \in \mathbb{Q} \mid x(a\mathbb{Z}) \subseteq \mathbb{Z}\}$$

$$= \{\text{all rational numbers } \frac{p}{q} \in \mathbb{Q} \text{ s.t. } q \mid a\}$$

$$= \{\text{all rational numbers } \frac{p}{a} \text{ where } p \in \mathbb{Z}\}$$

$$= \frac{1}{a}\mathbb{Z} = a^{-1}\mathbb{Z} = (a^{-1})$$

Rmk: $\mathcal{O}_K \subseteq I^{-1}$

If $I = (a) = a\mathcal{O}_K$ is principal, $I^{-1} = (a^{-1}) = a^{-1}\mathcal{O}_K$

A fractional ideal I of $\mathcal{O}_K$ is an $\mathcal{O}_K$-module s.t. $I \subseteq K$ and $\exists$ a nonzero (denominator) $r \in \mathcal{O}_K$ s.t. rI is an ideal.

A fractional ideal I of $\mathcal{O}_K$ is an $\mathcal{O}_K$-module s.t. $I \subseteq K$ and $\exists$ a nonzero (denominator) $r \in \mathcal{O}_K$ s.t. rI is an ideal. $(rI \subseteq \mathcal{O}_K)$

$\mathcal{I}(\mathcal{O}_K)$ = group of all nonzero fractional ideals of $\mathcal{O}_K$

- $\mathcal{O}_K = (1)$ is the identity element.
- operation is fractional ideal multiplication

$I, J \in \mathcal{I}(\mathcal{O}_K)$

for I, $\exists r_I$ s.t. $r_I I$ is an ideal
for J, $\exists r_J$ s.t. $r_J J$ is an ideal

$\Rightarrow$ using ideal multiplication,

$(r_I I)(r_J J) = r_I r_J IJ$ is also an ideal.

$\Rightarrow IJ$ is a fractional ideal w/ $r_{IJ} = r_I r_J$.

$IJ \in \mathcal{I}(\mathcal{O}_K)$

- $I \in \mathcal{I}(\mathcal{O}_K)$, $\underbrace{r_I I}_{\text{is an ideal}} \subseteq \mathcal{O}_K$

Exercise: Prove $\mathcal{I}(\mathcal{O}_K)$ is a group using the definition of inverse of an ideal given above.

下午12:59 10月3日周二 90%
Back
File Details
MAT1210H F LEC0101 20239:Topics in Number Theory

an ideal given above.

Let S be a set of primes of $\mathcal{O}_K$, define

$\mathcal{I}(\mathcal{O}_K)^S$ to be the subgroup of $\mathcal{I}(\mathcal{O}_K)$ generated by the primes of $\mathcal{O}_K$ that do not lie in S. "away from S"

Assume that L is a finite abelian extension of K, and let S be the set of primes of K that ramify in L ($e > 1$)

then Artin map is:

$$\mathcal{I}(\mathcal{O}_K)^S \longrightarrow \mathrm{Gal}(L/K)$$

$$I = \underbrace{\prod_{i=1}^{m} \mathfrak{p}_i^{k_i}}_{\text{factorization}} \longmapsto \prod_{i=1}^{m} \sigma(\mathfrak{p}_i)^{k_i}$$

Set up:

$$\begin{array}{ccccc} L & \geq & \mathcal{O}_L & \geq & \mathfrak{P}_{ij} \\ | & & | & & | \\ K & \geq & \mathcal{O}_K & \geq & \mathfrak{p}_i \\ | & & | & & | \\ \mathbb{Q} & \geq & \mathbb{Z} & \geq & p \end{array} \qquad \begin{array}{c} \mathcal{O}_L/\mathfrak{P}_{ij} \\ | \\ \mathcal{O}_K/\mathfrak{p}_i \\ | \\ \mathbb{F}_p \end{array}$$

L/K finite abelian; $f_{(\mathfrak{P}_{ij}/\mathfrak{p}_i)}$

$f_{L/K}(\mathfrak{P}_{ij}) = [\mathcal{O}_L/\mathfrak{P}_{ij} : \mathcal{O}_K/\mathfrak{p}_i]$ cyclic extension over $\mathbb{F}_p$

Let $\mathfrak{q} = \mathfrak{P}_{ij}$, $\mathfrak{p} = \mathfrak{p}_i$. Assume $e(\mathfrak{q}/\mathfrak{p}) = 1$, unramified.

$\sigma(\mathfrak{q}/\mathfrak{p})$ is the preimage of the generator Frob in $\mathrm{Gal}(\mathcal{O}_L/\mathfrak{q} / \mathcal{O}_K/\mathfrak{p})$ ($x \mapsto x^{\#(\mathcal{O}_K/\mathfrak{p})}$)

under the isomorphism, $D(\mathfrak{q}/\mathfrak{p}) \cong \mathrm{Gal}(\text{res field})$

Because $e=1$, the decomp size.

For a different j (fixed i), $\sigma(\mathfrak{P}_{ij}/\mathfrak{p}_i)$ and $\sigma(\mathfrak{P}_{ij'}/\mathfrak{p}_i)$ are conjugate.

Since L/K abelian, $\sigma(\mathfrak{P}_{ij}/\mathfrak{p}_i) = \sigma(\mathfrak{P}_{ij'}/\mathfrak{p}_i)$. So we can call this element in $\mathrm{Gal}(L/K)$

$\sigma(\mathfrak{q}/\mathfrak{p}) = \sigma(\mathfrak{q}'/\mathfrak{p}) = \sigma(\mathfrak{p})$

Let S be the set of ramified primes, i.e. primes in K that ramified in L.

$\mathrm{cl}(\mathcal{O}_K)^S$ = subgroup of $\mathrm{cl}(\mathcal{O}_K)$ (group of fractional ideals) generated by the primes of $\mathcal{O}_K$ that do not lie in S.

= "Ideal group of K away from S"

The Artin map is:

$$\mathrm{cl}(\mathcal{O}_K)^S \xrightarrow{\sigma} \mathrm{Gal}(L/K)$$

$$\prod_{i=1}^{m} \mathfrak{p}_i^{k_i} \longmapsto \prod_{i=1}^{m} \sigma(\mathfrak{p}_i)^{k_i}$$

(ideal mult.; composition of automorphisms.)

Global CFT: σ is surjective.

Example in which σ surjective:

$L = \mathbb{Q}(\sqrt{d})$, d sq-free.

$K = \mathbb{Q}$ L/K Galois with $G = C_2$

The discriminant of $L = \begin{cases} d & d \equiv 1 \ (4) \\ 4d & d \equiv 3 \ (4) \end{cases}$

p ramifies in L iff $p \mid \mathrm{Disc}(L)$

Present $G = \{\pm 1\}$ with multiplication.

$\sigma(p) = \pm 1$ under the Artin map.

$\sigma(p) = 1$ iff p splits (complete), $g = [L:k]$

Global CFT says that some prime of k remains inert in L.

We could add in character language.

$$\chi_d(p) = \begin{cases} 1 & p \text{ splits} \\ -1 & p \text{ inert} \\ 0 & p \text{ ramifies.} \end{cases}$$

Exercise: Show that for p odd, $D = \begin{cases} d & d \equiv 1 \ (4) \\ 4d & d \equiv 3 \ (4) \end{cases}$

$$\left(\frac{D}{p}\right) = \chi_D(p) = \begin{cases} +1 & \text{if } D \text{ is a square mod } p \\ -1 & \text{if } D \text{ not } \cdots \\ 0 & \text{if } p \mid D. \end{cases}$$

for p even,

$$\left(\frac{D}{p}\right) = \chi_D(p) = \begin{cases} 1 & D \equiv 1 \pmod 8 \\ -1 & D \equiv 5 \pmod 8 \end{cases}$$

Local fields = section 7.4

Local fields are the fields that arise by completing a number field.

def 9.1: is a field with a non-trivial absolute value $|\cdot|$ that is locally compact under the topology induced by $|\cdot|$

Def (1.2): An absolute value on a field F is a map $|\cdot| : F \to \mathbb{R}_{\geq 0}$ s.t. $\forall x, y \in F$,

- $|x| = 0 \iff x = 0$
- $|xy| = |x||y|$
- $|x+y| \leq |x| + |y|$

archimedian: $\exists x_0, y_0 \in F$, s.t. $\max\{|x_0|, |y_0|\} < |x_0 + y_0| \leq |x_0| + |y_0|$

It is archimedean if also:

- $|x+y| \leq \max\{|x|, |y|\}$.

9.7

Cor: Let L be a number field with a non-trivial $|\cdot|_v$. Then the completion L_v of L wrt $|\cdot|_v$ is a local field.

Pf:
$$\begin{array}{ccc} L & > & \mathcal{O}_L \\ | & & | \\ K=\mathbb{Q} & > & \mathcal{O}_K = \mathbb{Z} \end{array}$$

- $\mathcal{O}_L$ is a dedekind domain

2 cases: ① Archimedean case:

- The completion of L wrt $|\cdot|_v$ must contain the completion of $\mathbb{Q}$ (restrict to $\mathbb{Q}$), which is $\mathbb{R}$

So the completion of L wrt $|\cdot|_v$ must be $\mathbb{R}$ or $\mathbb{C}$

② Non-Archimedean:

- $|\cdot|_v$ is induced by a discrete valuation

(**Def:** A valuation on a field F is a group homomorphism

$F^\times \to \mathbb{R}$ s.t. $\forall x,y \in F$, $v(x+y) \geq \min(v(x), v(y))$

We extend v to $F \to \mathbb{R} \cup \{\infty\}$ by $v(0) = \infty$

Note: If $|\cdot|_v$ is defined by $|x|_v := c^{v(x)}$, it is non-archimedean.

Notation/Def: v is a **discrete valuation** if the image (or a value group) in $\mathbb{R}$ is $= \mathbb{Z}$)

1.11

Def: If F is a field with valuation v,

Let $v_F := \{x \in F \mid v(x) \geq 0\}$.

Let $v_L := \{x \in F \mid |x|_v \leq 1\}$ be the valuation ring associated to $|\cdot|_v$

Let $m_v = \{x \in F \mid |x|_v < 1\}$ be the maximal ideal

iff $|\cdot|_v$ is nontrivial)

- restriction of $|\cdot|_v$ to $\mathbb{Q}$ is a nonarchimedean absolute value, and from the classification of absolute values of $\mathbb{Q}$ (Ostrowski), it is induced by a discrete valuation $|\cdot|_{\mathbb{Q}}$
- many properties of DVRs (discrete valuation rings) are used to describe $|\cdot|_v = c^{v_\sigma(\cdot)}$, specifically what σ is

Defn: A discrete valuation ring is an integral domain R that is the valuation ring of its fraction field wrt a discrete valuation

- conclude the pink highlighted portion by describing v_σ (and σ) as discrete valuation. (or proving)

- finiteness of the residue fields associated to $L/K = \mathbb{Q} \Rightarrow$ finiteness of the residue fields of $L_v/\mathbb{Q}_p$ ← completion wrt $|\cdot|_v$ ← completion wrt $|\cdot|_{\mathbb{Q}}$

Conclude that

- L_v is a complete field w/ an absolute value induced by a discrete valuation and has a finite residue field, and so By Proposition 9.6 in Sutherland, then you are a local field. □

Theorem 9.9: Let L be a local field. If L is archimedean, then it is isomorphic to $\mathbb{R}$ or $\mathbb{C}$. Otherwise, L is isomorphic to a finite extension of $\mathbb{Q}_p$ (or a finite extension of $\mathbb{F}_q((t))$)

◂ Previous Next ▸

Dashboard Calendar To Do Notifications Inbox

◂ Previous Next ▸

Dashboard Calendar To Do Notifications Inbox

REC

Lemma 9.15: Let R be a complete dvr (discrete valuation ring) with maximal ideal $\mathfrak{p}$ and residue field $k = R/\mathfrak{p}$. ← lowercase because it is a residue field

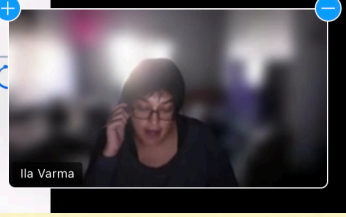
Suppose $f \in R[x]$ is a monic polynomial whose image under the projection map

$$R[x] \longrightarrow R/\mathfrak{p}[x]$$

has a simple root $\bar{a}$ in the field $k = R/\mathfrak{p}$ ← image of a under quotient by $\mathfrak{p}$ (notation assumes that the map $R \to R/\mathfrak{p}$ is surjective)

Then $\bar{a}$ can be lifted to a root of f in R.

Defn 9.14: (R a commutative ring) Let $f \in R[x]$ be a polynomial over a ring R and let $a \in R$. If $f(a) = 0$ and $f'(a) \neq 0$, then a is a simple root of f

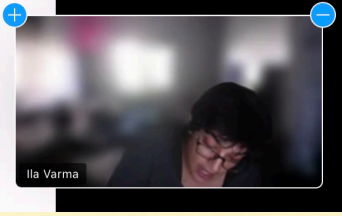


f in R.

Def'n 9.1 ... a polynomial over a ring R and let $a \in R$. If $f(a)=0$ and $f'(a) \neq 0$, then a is a simple root of f

Def'n 9.10: Let R be a commutative ring, and let $f(x)=\sum_{0 \le i < \infty} f_i x^i \in R[x]$ be a polynomial. The (formal) derivative f' of f is the polynomial

$$f'(x)=\sum i f_i x^{i-1} \in R[x].$$



Example: $R=\mathbb{Z}_5$, $f(x)=x^2-6$.

Q: $\sqrt{6} \in \mathbb{Z}_5$? how many?

A: $\bar{f}(x)=x^2-1 \in \mathbb{F}_5[x]$. $K=\mathbb{Z}_5/(5)$

$=(x+1)(x-1)$

@ $\bar{f}(x)$ has simple root $\bar{a}=1 \in \mathbb{F}_5$

By Hensel's lemma, $\exists!\ a \in \mathbb{Z}_5$, s.t. $a^2-6=0$ and $a \equiv 1 \pmod 5$

Similarly, $\exists!\ b \in \mathbb{Z}_5$, s.t. $b^2-6=0$, $b \equiv -1 \pmod 5$

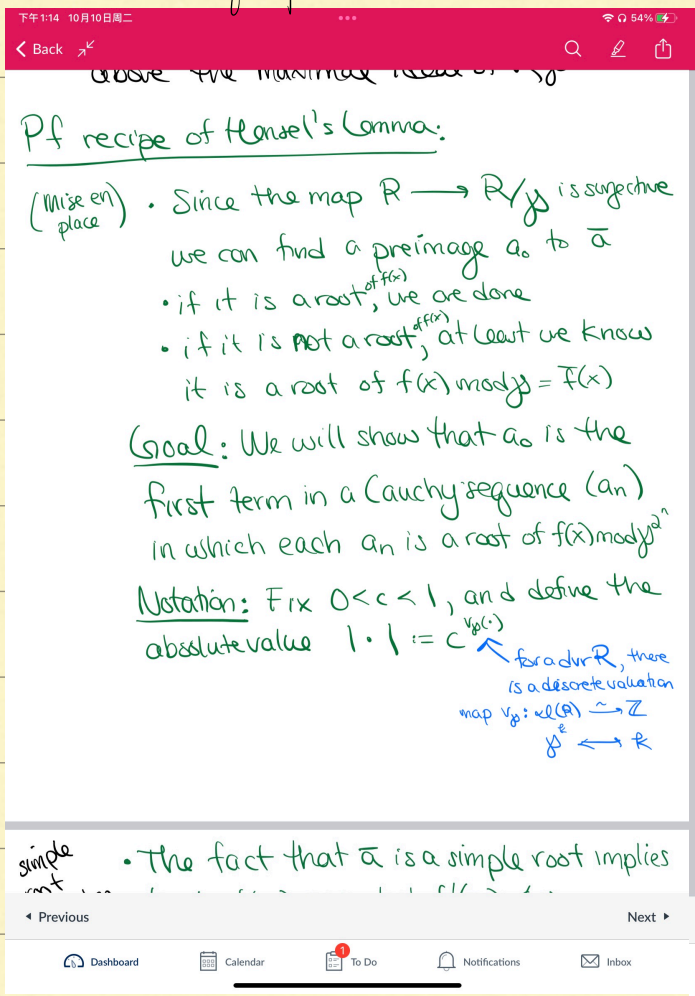
Thm: (9.22) V: complete discrete valuation ring

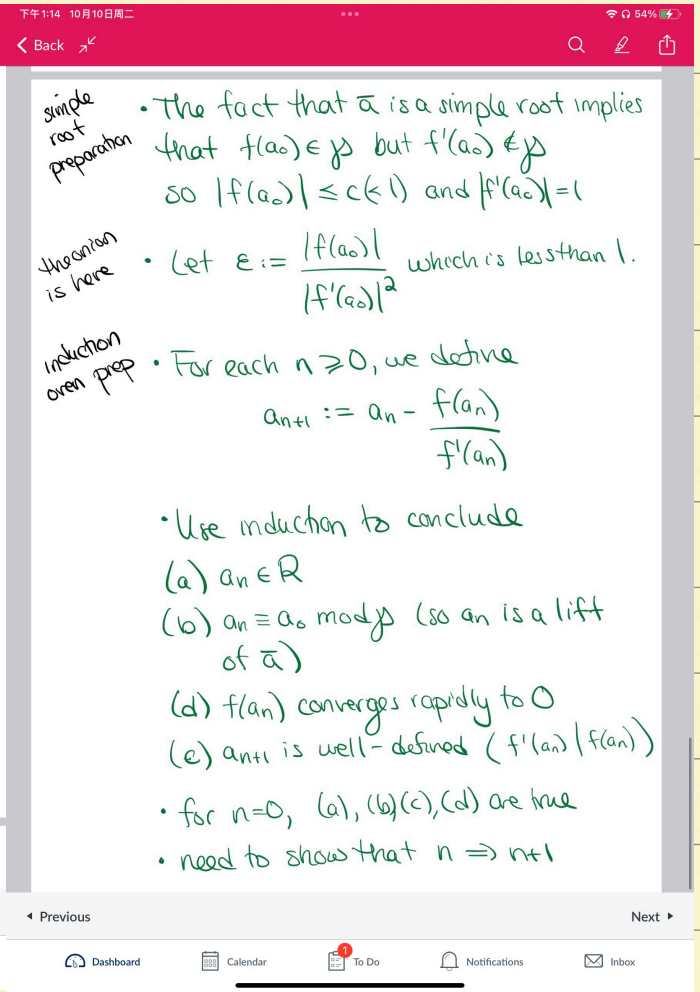
$L \supset V_L$ ← integral closure of V in L.

$\mathrm{Frac}(V)=K \supset V$

V_L is a discrete valuation ring, whose maximal ideal $\mathfrak{q}$ is necessarily

the unique prime above the maximal ideals of V.





Lemma (9.1b): f do not to be monic and $\bar{a}$ not simple.

Let R any complete dvr, $f \in R[x]$, let $a_0 \in R$ satisfies $|f(a_0)| < |f'(a_0)|^2$

(So in particular, $f'(a_0) \mid f(a_0)$), define $a_{n+1} := a_n - \dfrac{f(a_n)}{f'(a_n)}$.

The sequence is well-defined and converge to a unique root of f for which $|a - a_0| \le \varepsilon := \dfrac{|f(a_0)|}{|f'(a_0)|^2}$. Moreover, $|f(a_n)| \le \varepsilon^{2^n} |f'(a_0)|^2$ for all $n \ge 0$.

Pf: $n=0$: (a) $a_0 \in R$,

(b) $a_0 \equiv a_0 \bmod \mathfrak{p}$

$x \mid y \Leftrightarrow v(x) \le v(y) \Leftrightarrow |x| \ge |y|$

(d) $|f(a_0)| \le |f'(a_0)|^2$ by assumption.

(c) Since $f'(a_0) \mid f(a_0)$, we have $a_1 := a_0 - \dfrac{f(a_0)}{f'(a_0)}$ is well-defined.

$n \Rightarrow n+1$: (a) $|a_n| \le 1$. (b) $|a_n - a_0| \le \varepsilon < 1$ (d) $|f(a_n)| \le \varepsilon^{2^n} |f'(a_n)|^2$

(c) $|f'(a_n)| = |f'(a_0)| \Rightarrow a_{n+1} := a_n - \dfrac{f(a_n)}{f'(a_n)}$ well-defined.

Pf (a): $|a_{n+1} - a_n| = \dfrac{|f(a_n)|}{|f'(a_n)|} = \dfrac{|f(a_n)|}{|f'(a_0)|} \le \dfrac{\varepsilon^{2^n} |f'(a_0)|^2}{|f'(a_0)|} \le \varepsilon^{2^n} |f'(a_0)| \le \varepsilon^{2^n}$

$|a_{n+1}| = |a_{n+1} - a_n + a_n| \le \max\{|a_{n+1}-a_n|, |a_n|\} \le 1$

Pf (b) $|a_{n+1} - a_0| \le \max\{|a_{n+1}-a_n|, |a_n - a_0|\} \le \max\{\varepsilon^{2^n}, \varepsilon\} = \varepsilon$.

Pf (c) "Taylor expansion": $f(x) = f(a) + f'(a)(x-a) + g(x)(x-a)^2$ ← unique in $R[x]$

Apply to $f'(x)$ @ a_n:

$f'(x) = f'(a_n) + f''(a_n)(x-a_n) + g(x)(x-a_n)^2$

$x = a_{n+1}$ ↓

$f'(a_{n+1}) = f'(a_n) + f''(a_n)(a_{n+1}-a_n) + g(a_{n+1})(a_{n+1}-a_n)^2$

Since $a_{n+1} - a_n = -\dfrac{f(a_n)}{f'(a_n)}$

$f'(a_{n+1}) = f'(a_n) + \underset{R}{f''(a_n)}\left(-\dfrac{f(a_n)}{f'(a_n)}\right) + \underset{R}{g(a_{n+1})}\left(\dfrac{f(a_n)}{f'(a_n)}\right)^2$

$\Rightarrow |f''(a_n)| \le 1, \quad \Rightarrow |g(a_{n+1})| \le 1.$

Since $\left|\dfrac{f(a_n)}{f'(a_n)}\right| = \dfrac{|f(a_n)|}{|f'(a_n)|} = \dfrac{|f(a_n)|}{|f'(a_0)|} \le \varepsilon^{2^n}|f'(a_0)|$

$|f'(a_n)| = |f'(a_0)| > \left|f''(a_n)\left(-\dfrac{f(a_n)}{f'(a_n)}\right) + g(a_{n+1})\left(\dfrac{f(a_n)}{f'(a_n)}\right)^2\right|$

$|f'(a_{n+1})| = |f'(a_n)| = |f'(a_0)|$

Pf (c): $f(x) = f(a_n) + f'(a_n)(x-a_n) + h(x)(x-a_n)^2$.

$x = a_{n+1}$ ↓

$f(a_{n+1}) = \cancel{f(a_n)} + \cancel{f'(a_n)}\left(-\dfrac{\cancel{f(a_n)}}{\cancel{f'(a_n)}}\right) + h(a_{n+1})\left(\dfrac{f(a_n)}{f'(a_n)}\right)^2$

$= h(a_{n+1})\left(\dfrac{f(a_n)}{f'(a_n)}\right)^2$

$h \in R[x]$, $|a_{n+1}| \le 1 \Rightarrow a_{n+1} \in R$.

Hence $|h(a_{n+1})| \le 1$ $(h(a_{n+1}) \in R)$

$|f(a_{n+1})| \le \dfrac{|f(a_n)|^2}{|f'(a_n)|^2} \le \dfrac{|f(a_0)|^2}{|f'(a_0)|^2} \le \dfrac{(\varepsilon^{2^n}|f'(a_0)|^2)^2}{|f'(a_0)|^2} \le \varepsilon^{2^{n+1}}|f'(a_0)|^2$.

We have $|a_{n+1} - a_n| \le \varepsilon^{2^n} \xrightarrow{n\to\infty} 0$

Since $|\cdot|$ non-archimedean, this implies $\{a_n\}$ is cauchy.

Let $a = \lim a_n \in R$ (R complete)

$f(a) = \lim f(a_n) = 0 \Rightarrow a$ a root of f and $|a - a_0| = \lim_{n\to\infty}|a_n - a_0| < 1$

Prove the local K-N theorem

Recall: Thm 20.2: Every finite abelian extension of $\mathbb{Q}_p$ lies in a cyclotomic field $\mathbb{Q}_p(\zeta_m)$

Prop: Let $K/\mathbb{Q}_p$ be a cyclic extension of degree l^r for some prime l. Then K lies in a cyclotomic field $\mathbb{Q}_p(\zeta_m)$

① Prop ⇒ Thm 2012.

② Proving Prop.

Q: why does prop ⇒ local K-W?

② Proving Proposition.

Q: Why does the proposition imply the local Kronecker-Weber theorem?

Answer: If L_1 and L_2 are normal extensions of a field K, then $L = L_1L_2$, the compositum is also Galois

$$\mathrm{Gal}(L_1L_2/K) \cong \{(\sigma_1, \sigma_2) \mid \sigma_{1|L_1\cap L_2} = \sigma_{2|L_1\cap L_2}\}$$
$$\subseteq \mathrm{Gal}(L_1/K) \times \mathrm{Gal}(L_2/K)$$

↑ equality iff $L_1 \cap L_2 = K$

Exercise: Prove the above statement.

By the fundamental theorem of finite abelian groups, any finite abelian extension L/K can be decomposed into a compositum $L_1 \cdots L_n = L$ of linearly disjoint cyclic extensions L_i/K of prime

power degree. If each L_i lies in a cyclotomic extension $K(\zeta_{m_i})$, then $L \subset \underbrace{K(\zeta_{m_1}) \cdots K(\zeta_{m_n})}_{m = m_1 m_2 \cdots m_n} = K(\zeta_m)$ where

Hence, we can prove Thm 20.2 by considering cyclic extensions $K/\mathbb{Q}_p$ of prime power degree ℓ^r

1. "tame" case $\ell \neq p$ [Proposition 20.4]
2. "wild", odd case $\ell = p$, $p \neq 2$ [Thm 20.6]
3. "wild", 2 case $\ell = p = 2$ [Thm 20.10]

Proposition 20.4: Let $K/\mathbb{Q}_p$ be a cyclic extension of degree ℓ^r $(\ell \neq p)$. Then K lies in a cyclotomic field $\mathbb{Q}_p(\zeta_m)$.

Pf recipe: Let F be the maximal unramified extension of $\mathbb{Q}_p$ in K.

1. $F = \mathbb{Q}_p(\zeta_n)$ for some n (Corollary 10.17)

K/F is totally ramified, and it must be tamely ramified since the ramification index e is a power of ℓ and $\ell \neq p$. (exp)

② $K = F(\pi^{1/e})$, where π is a choice of generator of the maximal ideal in $\mathcal{O}_F$ (and $e = [K:F]$)

(11.10)

We may assume $\pi = -p \cdot u$, where $u \in \mathcal{O}_F^\times$ since $F/\mathbb{Q}_p$ is unramified. (see Thm 8.20)

$K = F(\pi^{1/e})$ lies in the compositum of ⑥ $F((-p)^{1/e})$ and ⓐ $F(u^{1/e})$

We will show that both fields lie in a cyclotomic extension of $\mathbb{Q}_p$

ⓐ $F(u^{1/e})/F$ is unramified, since $F/\mathbb{Q}_p$ is unram, $F(u^{1/e})/\mathbb{Q}_p$ is unramified

$\Rightarrow F(u^{1/e}) = \mathbb{Q}_p(\mathcal{G}_k)$ for some $k \geq 1$

(b) $K(u^{1/e}) = K \cdot F(u^{1/k}) = K \cdot \mathbb{Q}_p(\mathcal{G}_k)$ is a compositum of abelian extension so $K(u^{1/e})/\mathbb{Q}_p$ is abelian, and it contains the subextension $\mathbb{Q}_p((-p)^{1/e})/\mathbb{Q}_p$, hence it is Galois, abelian.

$\mathbb{Q}_p((-p)^{1/e})/\mathbb{Q}_p$ is totally ramified (Thm 11.5)

The field $\mathbb{Q}_p((-p)^{1/e})$ contains $\mathcal{G}_e$ (roots of the distinct roots of x^e+p)

and $\mathbb{Q}_p(\mathcal{G}_e)/\mathbb{Q}_p$ is unramified ($p \nmid e$, $e \nmid p$)

hence $\mathbb{Q}_p(\mathcal{G}_e) = \mathbb{Q}_p$. Exercise $\Rightarrow e \mid p-1$

By Lemma 20.5, $\mathbb{Q}_p((-p)^{1/e}) = \mathbb{Q}_p(\mathcal{G}_p)$

It follows that $F((-p)^{1/e}) = F \cdot \mathbb{Q}_p((-p)^{1/e})$

$$\subseteq \mathbb{Q}_p(\mathcal{G}_n) \cdot \mathbb{Q}_p(\mathcal{G}_p)$$

$$K \subseteq F(u^{1/e}) \cdot F((-p)^{1/e}) \subseteq \mathbb{Q}_p(\mathcal{G}_k)\,\mathbb{Q}_p(\mathcal{G}_{np})$$

$$\subseteq \mathbb{Q}_p(\mathcal{G}_{knp}).$$

□

Theorem 20.16: Let $K/\mathbb{Q}_p$ be a cyclic extension of odd degree p^r (p is an odd prime). Then K lies in a cyclotomic field $\mathbb{Q}_p(\zeta_m)$.

Pf: In Section 10, Corollary 10.17 and 10.18 give the two "obvious" candidates for what K could be:

① $K = \mathbb{Q}_p(\zeta_{p^r-1})$ unramified degree p^r extension

② K is the index $p-1$ subfield of $\mathbb{Q}_p(\zeta_{p^{r+1}})$ (totally ramified extension of degree p^r)

(you can double check these candidates based on a degree calculation, are they the right degrees)

Case 1: K is contained in the compositum of these two fields ①·②, then $K \subseteq \mathbb{Q}_p(\zeta_m)$ where $m = (p^r-1)(p^{r+1})$

Case 2: $K(\zeta_m)$ is a Galois extension of $\mathbb{Q}_p$

$$\mathrm{Gal}(K(\mathfrak{g}_m)/\mathbb{Q}_p) \cong \mathbb{Z}/p^r\mathbb{Z} \times \mathbb{Z}/p^r\mathbb{Z} \times \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}/p^s\mathbb{Z}$$

$\mathrm{Gal}(\mathbb{Q}_p(\mathfrak{g}_{p^r-1})/\mathbb{Q}_p)$

$\mathrm{Gal}(\mathbb{Q}_p(\mathfrak{g}_{p^{r+1}})/\mathbb{Q}_p)$ for some $s > 0$

$\mathrm{Gal}(K(\mathfrak{g}_m)/\mathbb{Q}_p(\mathfrak{g}_m))$ is nontrivial and must have order p^s w/ $1 \leq s \leq r$

It follows that $\mathrm{Gal}(K(\mathfrak{g}_m)/\mathbb{Q}_p)$ has a quotient isomorphic to $(\mathbb{Z}/p\mathbb{Z})^3$ and the subfield of $K(\mathfrak{g}_m)$ corresponding to this quotient is an abelian extension of $\mathbb{Q}_p$ w/ Galois group $(\mathbb{Z}/p\mathbb{Z})^3$ (when p is odd).

No such field exists. (Proposition 20.7).

□

Local K-W so far:

① Every ramified extension of $\mathbb{Q}_p$ is of the form $\mathbb{Q}_p(\zeta_n)$

② Every tamely totally ramified extension of degree e $(p \nmid e)$ of a local field F is of form $F(\pi^{\frac{1}{e}})$ where π generator of the maximal ideal of $\mathcal{O}_F$, known as uniformizer.

③ If F is unramified, then the uniformizer $\pi = -pu$, u unit in $\mathcal{O}_F^\times$

- $\mathbb{Q}_p(\zeta_{p^{r-1}})$ is an unramified extension of deg $= p^r$ over $\mathbb{Q}_p$
- $\mathbb{Q}_p(\zeta_{p^{r+1}})$ has an index p subfield which is totally ramified of deg p^r over $\mathbb{Q}_p$.
- Any wildly ($p \mid$ degree of extn) totally ramified Galois extension of $\mathbb{Q}_p$ is cyclic. (p odd)

($\Rightarrow$ no extension with $G = (\mathbb{Z}/p\mathbb{Z})^3$)

Thm: Let $K/\mathbb{Q}_2$ be a cyclic extension of degree 2^r. Then K lies in a cyc field $\mathbb{Q}_2(\zeta_m)$

Pf: The unramified cyc extn $\mathbb{Q}_2(\zeta_{2^{r-1}})$ has $G = (\mathbb{Z}/2^r\mathbb{Z})$

and the totally ramified cyc field $\mathbb{Q}_2(\zeta_{2^{r+2}})$ has $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^r\mathbb{Z}$.

Take $m = (2^{r-1})(2^{r+2})$

Case 1: K is contained in $\mathbb{Q}_2(\zeta_m)$

Case 2: $\mathrm{Gal}(K(\zeta_m)/\mathbb{Q}_2) = \begin{cases} \mathbb{Z}/2\mathbb{Z} \times (\mathbb{Z}/2^r\mathbb{Z})^2 \times \mathbb{Z}/2^s\mathbb{Z} & 1 \le s \le r \\ (\mathbb{Z}/2^r\mathbb{Z})^2 \times \mathbb{Z}/2^s\mathbb{Z} & 1 \le s \le r \end{cases}$

$\mathrm{Gal}(K(\zeta_m)/\mathbb{Q}_2)$ admits a quotient isomorphic to $(\mathbb{Z}/2\mathbb{Z})^3$ or $(\mathbb{Z}/4\mathbb{Z})^4$

By Lemma 20.11, no extension of $\mathbb{Q}_2$ satisfies this.

Lemma (20.11) No extension of $\mathbb{Q}_2$ has $G = (\mathbb{Z}/2\mathbb{Z})^3$ or $(\mathbb{Z}/4\mathbb{Z})^4$

Pf: (recipe): LMFDB.org

How many distinct index 2 subgroups are in $(\mathbb{Z}/2\mathbb{Z})^4$

15 → 15 distinct quadratic subfield

Since there are only 7 quadratic extensions of $\mathbb{Q}_2$ (lmfdb.org), there cannot be $(\mathbb{Z}/2\mathbb{Z})^4$ extension of $\mathbb{Q}_2$.

How many index 4 of $(\mathbb{Z}/4\mathbb{Z})^3$? ≥ 8

But only 12 extn of $\mathbb{Q}_2$ with deg 4

CFT over $\mathbb{Q}$ in language that generalizes:

Global CFT (over $\mathbb{Q}$):

① $\forall m \in \mathbb{Z}$, we have a unique ray class field of conductor, namely, $\mathbb{Q}(\zeta_m)$

② Every finite abelian extension of $\mathbb{Q}$ lies in a ray class field, $\mathbb{Q}(\zeta_m)$

③ If L is a finite abelian extension of $\mathbb{Q}$ contained in the ray class field $\mathbb{Q}(\zeta_m)$, then the Artin map $\mathcal{C}(\mathbb{Q})^{\{p \nmid m\}} \longrightarrow \mathrm{Gal}(L/\mathbb{Q})$ induces a surjective homomorphism from the ray class group $(\mathbb{Z}/m\mathbb{Z})^\times \longrightarrow \mathrm{Gal}(L/\mathbb{Q})$

letting us view $\mathrm{Gal}(L/\mathbb{Q})$ as a quotient of $(\mathbb{Z}/m\mathbb{Z})^\times$.

Def: 2 absolute $|\ |$, $|\ |'$ on k are equivalent if $\exists \alpha \in \mathbb{R}_{>0}$, for which $|x|' = |x|^\alpha$, $\forall x \in k$.

The trivial absolute $|\cdot| : k \to \mathbb{R}_{\geq 0}$ is $|x| = \begin{cases} 1 & x \neq 0 \\ 0 & x = 0 \end{cases}$

Exercise: ① trivial is non-archimedian

② every non-trivial $|\ |$ on $\mathbb{Q}$ is equivalent to $|\cdot|_p$ for some prime p

③ $\forall\, x \in \mathbb{Q}^\times$, we have $\prod_{p \le \infty} |x|_p = 1$

Def: Let K field. A **place** of K is a equivalence class of non-trivial absolute values on K

Fact: There's 1-1 correspondence between places of K and completions of K.

Notation: M_K = set of places of K. Write $v \in M_K \Leftrightarrow [v] \in M_K$, v representative of $|\cdot|_v$

K_v = completion of K wrt $|\cdot|_v$.

If K number field, for any place v of K, the completion K_v wrt v is a local field.

Classification of Completions of number fields.

$K_v = \begin{cases} \mathbb{R} \\ \mathbb{C} \end{cases}$ } infinite place.

Absolute value of K_v is induced by a discrete valuation, call it v.

We write $v|\infty$ to indicate that v is an infinite place.

Def 2.12: Let $K/\mathbb{Q}$ number field. A **modulus** $\mathfrak{m}$ of K is a function $M_K \to \mathbb{Z}_{\ge 0}$ with finite support. (finite # of places is $\neq 0$)

s.t. for $v|\infty$, we have $\begin{cases} \mathfrak{m}(v) = 0 & \text{for all complex places } (K_v \cong \mathbb{C}) \\ \mathfrak{m}(v) \le 1 & \text{for all real places.} \end{cases}$

We usually describe $\mathfrak{m}$ using formal product language: $\mathfrak{m} = \prod_{v \in M_K} v^{m(v)}$

We can decompose $\mathfrak{m}$ into its finite vs infinite part:

$\mathfrak{m} = \mathfrak{m}_f \mathfrak{m}_\infty$. $\quad \mathfrak{m}_f = \prod_{p \nmid \infty} p^{m(p)} \quad \mathfrak{m}_\infty = \prod_{v \mid \infty} v^{m(v)}$

Less formally: $\mathfrak{m}$ is/can be thought of as an $\mathcal{O}_K$-ideal.

$\mathfrak{m}_\infty$ represents a subset of real places of K ($K_v \cong \mathbb{R}$)

Def: If $\mathfrak{m}, \mathfrak{n}$ are modulli of K, we say that $\mathfrak{m} \mid \mathfrak{n}$ if $m(v) \le n(v)$, $\forall v \in M_K$.

$\mathfrak{mn}$ is defined as $\mathfrak{mn}(v) = m(v) + n(v)$ for $v \nmid \infty$ (finite places)

$\mathfrak{mn}(v) = \max\{m(v), n(v)\}$ if $v \mid \infty$ (if $m(v)=1$ or $n(v)=1$, take 1; otherwise 0)

Def: $\gcd(\mathfrak{m}, \mathfrak{n})(v) = \min\{m(v), n(v)\}$

$\operatorname{lcm}(\mathfrak{m}, \mathfrak{n})(v) = \max\{m(v), n(v)\}$

The trivial modulus: $\mathfrak{m}_f = 1$, $\#\mathfrak{m}_\infty = 0$ (no real places v w/ $m(v)$ has 0)

Cl_K = ideal group = group of fractional ideals of $\mathcal{O}_K$.

A fractional ideal $I \in Cl_K$ is (co)-prime to $\mathfrak{m}$ if $v_p(I) = 0$, $\forall p \mid \mathfrak{m}_f$

$Cl_K^{\mathfrak{m}} \le Cl_K$ is the subgroup of fractional ideals coprime to $\mathfrak{m}$.

$K^{\mathfrak{m}} \le K^\times$ is the subgroup of elements $\alpha \in K^\times$ for which $(\alpha) \in Cl_K^{\mathfrak{m}}$

$K^{\mathfrak{m},1} \le K^{\mathfrak{m}}$ is subgroup of elements $\alpha \in K^\times$ with $\alpha \equiv 1 \pmod{p^{m(p)}}$, $v_p(\alpha - 1) \ge v_p(\mathfrak{m}_f)$, $\forall p \mid \mathfrak{m}_f$

and image of α under $K \hookrightarrow K_v \cong \mathbb{R}$ is positive if $v \mid \mathfrak{m}_\infty$ (v is real and $m(v) \neq 0$)

$R_K^{\mathfrak{m}} \le Cl_K^{\mathfrak{m}}$ (ray) is subgroup of principle fractional ideals $(\alpha) \in Cl_K^{\mathfrak{m}}$ s.t. $\alpha \in K^{\mathfrak{m},1}$

Def: Let $\mathfrak{m}$ be a modulus for a # field K. The ray class group for the modulus $\mathfrak{m}$ is the quotient

$$Cl_k^{\mathfrak{m}} := Cl_k^{\mathfrak{m}} / R_k^{\mathfrak{m}}$$

If $\mathfrak{m}$ is trivial, we get the ideal class group $Cl_k = Cl_k / P_k$ ← principle fr ideals.

Let $\mathfrak{m}$ be a modulus

If L/k finite abelian, unramified at all primes $\mathfrak{p} \nmid \mathfrak{m}_f$

and no infinite (real) place $v \in \mathfrak{m}_\infty$ turns into a complex place in L.

then we can define the Artin map:

$$\Psi_{L/k}^{\mathfrak{m}} : Cl_k^{\mathfrak{m}_f} = Cl_k^{\mathfrak{m}} \longrightarrow Gal(L/k)$$

$$\prod_{\mathfrak{p} \nmid \mathfrak{m}_f} \mathfrak{p}$$

If K is a number field, for any place v of K, the completion K_v of K wrt $|\cdot|_v$ is a local field. thm(9.9)

Classification of completions of number fields:

$$K_v \cong \begin{cases} \mathbb{R} \\ \mathbb{C} \end{cases} \left.\begin{array}{l} \\ \\ \end{array}\right\} \begin{array}{l} v \text{ is} \\ \text{infinite place} \end{array}$$

$$\left.\begin{array}{l} \\ \\ \\ \\ \\ \\ \end{array}\right\} \begin{array}{l} \text{absolute value on } K_v \text{ is induced} \\ \text{by a } \underline{\text{discrete valuation}}, \text{ call it } v \\ \qquad\qquad\qquad\qquad\qquad\qquad (v_{\mathfrak{p}}) \\ \text{associated to a} \\ \text{prime ideal } \mathfrak{p} \text{ of } \mathcal{O}_K \end{array}$$

v is finite place

$\mathfrak{p} \mid p$

$v \mid p$

We write $v \mid \infty$ to indicate that v is an infinite place (i.e. it does not arise from $\mathfrak{p}$ in $\mathcal{O}_K$)

Defn 21.2: Let K be a number field,

A **modulus** $\mathfrak{m}$ of K is a function

$$M_K \longrightarrow \mathbb{Z}_{\geq 0} \quad \text{w/ finite support}$$

finite # of places ore nonzero

the modulus $\mathfrak{m}$ is the quotient

$$Cl_K^{\mathfrak{m}} := \mathcal{I}_K^{\mathfrak{m}} / \mathcal{P}_K^{\mathfrak{m}}$$

If $\mathfrak{m}$ is trivial, we get the ideal class group $Cl_K = \mathcal{I}_K / \mathcal{P}_K$ = all principal fractional ideals

Let $\mathfrak{m}$ be a modulus

If L/K is a finite abelian extension unramified at all primes $\mathfrak{p}$ dividing $\mathfrak{m}_f$ and no infinite (real) place $v \in \mathfrak{m}_\infty$ turns into a complex place in L

then we can define the Artin map:

$$\psi_{L/K}^{\mathfrak{m}} : \mathcal{I}_K^{\mathfrak{m}_f} = \mathcal{I}_K^{\mathfrak{m}} \longrightarrow Gal(L/K)$$

$$\prod_{\mathfrak{p} \nmid \mathfrak{m}_f} \mathfrak{p}^{n_\mathfrak{p}} \longmapsto \prod_{\mathfrak{p} \nmid \mathfrak{m}_f} \sigma_\mathfrak{p}^{n_\mathfrak{p}}$$

$\sigma_\mathfrak{p}$: Frobenius preimage

If $\ker(\psi_{\mathfrak{m}}^{\mathfrak{m}}) = \mathcal{R}_K^{\mathfrak{m}}$, then L is a (actually, the) ray class field of conductor $\mathfrak{m}$.

For a modulus $\mathfrak{m}$, if $\mathfrak{m}(v) = 1$ for every real place v of K, we call $Cl_K^{\mathfrak{m}}$ a narrow ray class group.

Example: $\mathbb{Q}(\zeta_m)$ is the (narrow) ray class field of conductor/modulus $\mathfrak{m} = (m)\cdot\infty$

$\mathbb{Q}(\zeta_m + \zeta_m^{-1}) = \mathbb{Q}(\zeta_m) \cap \mathbb{R}$ is the (wide) ray class field of conductor/modulus $\mathfrak{m} = (m)$.

Exercise: $\mathfrak{m} = (5)$, $K = \mathbb{Q}$.

$$\mathbb{Q}^{\mathfrak{m}} = \left\{ \frac{a}{b} : a, b \in \mathbb{Z},\ b \neq 0,\ a \not\equiv 0 \bmod 5,\ b \not\equiv 0 \bmod 5 \right\}$$

$$\mathbb{Q}^{\mathfrak{m},1} = \left\{ \frac{a}{b} : a, b \in \mathbb{Z},\ b \neq 0,\ a, b \not\equiv 0 \bmod 5,\ a \equiv b \bmod 5 \right\}$$

$$\mathcal{L}_{\mathbb{Q}}^{m} = \{(1), (2), (\tfrac{1}{2}), (3), (\tfrac{1}{3}), (\tfrac{2}{3}), (\tfrac{3}{2}),$$
$$(4), (\tfrac{1}{4}), (\tfrac{3}{4}), (\tfrac{4}{3}),$$
$$(6), (\tfrac{1}{6}),$$
$$(7), (\tfrac{1}{7}), (\tfrac{2}{7}), (\tfrac{7}{2}), \ldots\}$$

$$\mathcal{R}_{\mathbb{Q}}^{m} = \{(1), \times \quad \times, (-\tfrac{2}{3}), (-\tfrac{3}{2}),$$
$$(-4), (-\tfrac{1}{4}), \times$$
$$(6), (\tfrac{1}{6})$$
$$\times \quad (\tfrac{2}{7}), (\tfrac{7}{2}), \ldots\}$$

$$\mathcal{C}\ell_{\mathbb{Q}}^{m} = \mathcal{L}_{\mathbb{Q}}^{m} / \mathcal{R}_{\mathbb{Q}}^{m} = ?? \quad (\mathrm{Gal}(\mathbb{Q}(\zeta_r + \zeta_r^{-1})/\mathbb{Q}$$

Let $m' = (5)\cdot\infty$

$$\mathcal{R}_{\mathbb{Q}}^{m'} = \{(1), \times \quad \times \quad \times$$
$$\times \quad \times$$
$$(6), (\tfrac{1}{6}), (\tfrac{2}{7}), (\tfrac{7}{2}), \ldots\}$$

What is $\ell_{\mathbb{Q}}^{m'} = ??$ $\left(\mathrm{Gal}(\mathbb{Q}(\zeta_r)/\mathbb{Q})\right)$

Theorem 21.8 (Fundamental Exact Sequence of ray class groups). Fix a number field K and a modulus $\mathfrak{m}$. Then there is an exact sequence

$$1 \to \mathcal{O}_K^\times \cap K^{\mathfrak{m},1} \to \mathcal{O}_K^\times \to K^{\mathfrak{m}}/K^{\mathfrak{m},1} \to \ell_K^{\mathfrak{m}} \to \ell_K \to 1$$

Also, $K^{\mathfrak{m}}/K^{\mathfrak{m},1} \cong \{\pm 1\}^{\#\mathfrak{m}_\infty} \times (\mathcal{O}_K/\mathfrak{m}_f)^\times$

Pf: $K^{\mathfrak{m},1} \xhookrightarrow{f} K^{\mathfrak{m}}$ and $K^{\mathfrak{m}} \xrightarrow{g} \ell_K^{\mathfrak{m}}$

$x \longmapsto x$ $\qquad$ $\alpha \longmapsto (\alpha)$

kernels: $\ker f$ = trivial

$\ker g = \mathcal{O}_K^\times$ $\quad ((\alpha)=1 \Leftrightarrow \alpha \in \mathcal{O}_K^\times)$

$\ker g\circ f : K^{\mathfrak{m},1} \cap \mathcal{O}_K^\times$ $\qquad g|_{K^{\mathfrak{m},1}} = g\circ f$

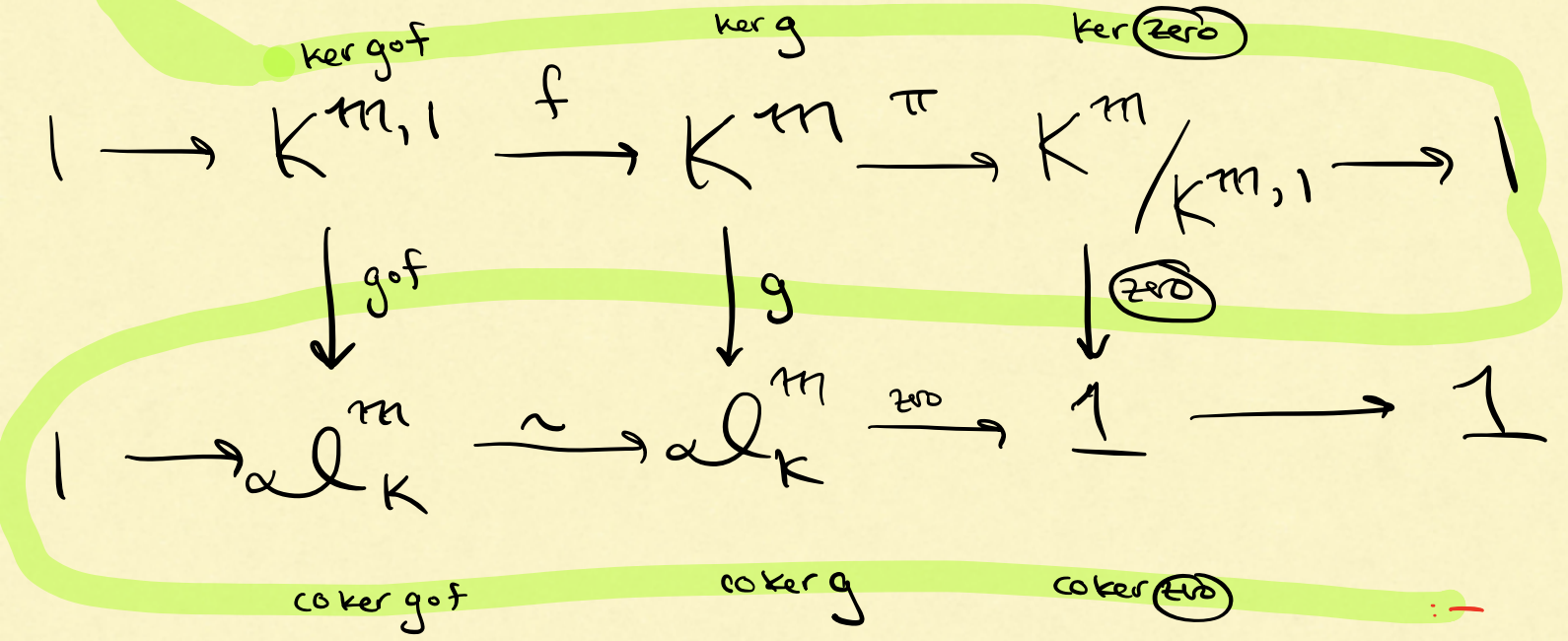
cokernels: $\mathrm{coker}\, f = K^{\mathfrak{m}}/\mathrm{im}(f) = K^{\mathfrak{m}}/K^{\mathfrak{m},1}$

$$\operatorname{coker} g = \mathcal{C}\ell_K^m / \operatorname{im}(K^m) \overset{!!}{\cong} \mathcal{C}\ell(K)$$

$$\operatorname{coker} g\circ f = \mathcal{C}\ell_K^m / \operatorname{im}(K^{m,1})$$

$$= \mathcal{C}\ell_K^m / \mathcal{R}_K^m = \mathcal{C}\ell_K^m$$

Snake Lemma:



$$\ker g\circ f \to \ker g \to \ker 0 \to \operatorname{coker} g\circ f \to \operatorname{coker} g \to \operatorname{coker} 0$$

$$1 \to \mathcal{O}_K^\times \cap K^{m,1} \to \mathcal{O}_K^\times \to K^m/K^{m,1} \to \mathcal{C}\ell_K^m \to \mathcal{C}\ell K \to 1$$

To prove $K^m/K^{m,1} \cong \{\pm 1\}^{\#m_\infty} \times (\mathcal{O}_K/m_f)^\times$:

$\alpha \in K^{\mathfrak{m}}$ can be written as $\alpha = \frac{a}{b}$ w/ $a, b \in \mathcal{O}_K$ chosen so that (a) and (b) are both coprime to $\mathfrak{m}_f$.

Define a homomorphism:

$$\varphi : K^{\mathfrak{m}} \longrightarrow \left(\prod_{v \mid \mathfrak{m}_\infty} \{\pm 1\} \right) \times \left(\mathcal{O}_K / \mathfrak{m}_f \right)^\times$$

$$\alpha \longmapsto \prod_{v \mid \mathfrak{m}_\infty} \operatorname{sgn}(\underbrace{\operatorname{im}_v(\alpha)}_{K \hookrightarrow K_v \cong \mathbb{R}}) \times (\bar{\alpha})$$

$$\bar{\alpha} = \bar{a} \cdot \bar{b}^{-1} = \bar{a} \cdot \bar{b}^{-1} \in \left(\mathcal{O}_K / \mathfrak{m}_f \right)^\times$$

where $\bar{a}, \bar{b}$ are the images of a, b in $\mathcal{O}_K / \mathfrak{m}_f$

they are units because (coprime to $\mathfrak{m}_f$) condition

It remains to show that φ is surjective and $\ker \varphi = K^{\mathfrak{m},1}$

$$\left(\mathcal{O}_K / \mathfrak{m}_f \right)^\times \cong \prod_{\mathfrak{p} \mid \mathfrak{m}_f} \left(\mathcal{O}_K / \mathfrak{p}^{m(\mathfrak{p})} \right)^\times$$

by Chinese Remainder Theorem.

By Weak Approximation (theorem 8.5)

φ is surjective

$\ker \varphi = K^{m,1}$

Weak approximation:

Let K field, $\{|\cdot|_i\}$ finite inequivalent non-trivial absolute values.

Let $\{a_i\}, \{\varepsilon_i\}$ finitely many positive numbers. Then $\exists x \in K$, $\forall i$,

$|x - a_i|_i \leq \varepsilon_i$.

(In other words, $K \to \prod_{v \in S} K_v$ is dense when S finite)

Last time: $\psi : K^m \longrightarrow \prod_{v|m_\infty} \{\pm 1\} \times \prod_{p|m_f} (\mathcal{O}_K/p^{m(p)})^\times$

$\ker \psi = K^{m,1}$

Cor 21.9: Let K a # field, m a modulus for K, then ray class group Cl_K^m is a finite (abelian) group, whose cardinality $h_K^m := \#Cl_K^m$ is given by $h_K^m = \frac{\#(K^m/K^{m,1}) \cdot h_K'}{[\mathcal{O}_K^\times : \mathcal{O}_K^\times \cap K^{m,1}]}$

$\#(K^m/K^{m,1}) = 2^{\#m_\infty} \cdot \#(\mathcal{O}_K/m_f)^\times = 2^{\#m_\infty} \cdot \frac{N_m(m_f)}{\prod_{p|m_f}(1 - N_m(p))}$

$N_m(m_f) := [\mathcal{O}_K : m_f]$,

$N_m(p) := [\mathcal{O}_K : p]$

$\Rightarrow h_K' \mid h_K^m \quad (h_K = h_K' = \#Cl(K))$

$\Rightarrow h_K^m \mid h_K' \cdot \#(K^m/K^{m,1})$

Thm 21.19: Let L/K finite abelian, m modulus, which is divisible by all primes of K that ramify in L. Then the Artin map $\psi_{L/K}^m : Cl_K^m \longrightarrow Gal(L/K)$ surjective

Pf: Let $H \subseteq Gal(L/K)$ be the image of $\psi_{L/K}^m$. Let $F = L^H$ the fixed field.

For each prime $p \in Cl_K^m$, the automorphism $\psi_{L/K}^m(p) \in H$ acts trivially on $F = L^H$.

Therefore p splits completely in F.

The group Cl_k^m contains all but finitely many primes p of K, so the "density" of the set of primes of K that split completely in F is 1.

We will show that the density being $1 \Rightarrow [F:K]=1$

Then we can conclude that $H = Gal(\Omega/k)$

Prop: If F/k finite of # fields in which all but finitely many primes split completely, then $[F:k]=1$, i.e. $F=k$.

$\zeta_k(s)$ and densities: $(K \hookrightarrow \overline{\mathbb{Q}})$

Def: Let K #field, S be a set of primes of K. the partial or "at S" Dedekind Zeta function associated to K is the complex function $\zeta_{K,S}(s) = \prod_{p \notin S} \frac{1}{1-Nm(p)^{-s}}$

It converges to a holomorphic function on $Re(s)>1$

$\{p = \mathfrak{p} | p\}$ where p rational prime $\leq n := [K:\mathbb{Q}]$

$Nm(\mathfrak{p}) = [\mathcal{O}_K : \mathfrak{p}] \geq p \quad (\mathfrak{p}|p)$

$\sum_{p \notin S} |\log(1-Nm(\mathfrak{p})^{-s})| \leq n \cdot \sum_{p \text{ rational}} |\log(1-p^{-s})|$

and the sum on the RHS converges on $Re(s)>1$ since $\zeta(s) = \prod_p (1-p^{-s})^{-1} = \sum n^{-s}$ converges on $Re(s)>1$.

If S finite, $\zeta_{K,S}(s)$ is holomorphic and it is nonzero on a nbhd of 1.

If S is all but finitely many primes of K, then it differs from $\zeta_K(s)$ by a holomorphic factor and we can study $\zeta_K(s)$, which extends to a meromorphic function with a simple pole at $s=1$

Agenda: ① Don't Look Away

② Polar Density in the context proof that the Artin map is surjective

③ Sets of primes that split completely determine a number field extension

④ Conductors

class is ending a little early (2:45)

K - a number field, Fix an algebraic closure of K, along w/ an embedding of $K \hookrightarrow \overline{K}$

Def'n: Let S be a set of primes of K

$$\zeta_{K,S}(s) = \prod_{\mathfrak{p} \notin S} \frac{1}{1 - \mathrm{Nm}(\mathfrak{p})^{-s}}$$

Def'n 21.11: If for some integer $n \geq 1$, the function $(\zeta_{K,S})^n$ extends to

a meromorphic function in a neighborhood of 1, then the <u>polar density</u> of S

$$\rho(S) := \frac{m}{n} \quad \text{where}$$

$$m = -\operatorname{ord}_{s=1}\left(\zeta_{K,S}(s)\right)^n$$

m is the order of the pole at $s=1$ (if a pole is present)

(does not depend on a choice of n)

② $$d(S) = \lim_{s\to 1^+} \frac{\sum_{\mathfrak{p}\in S} N(\mathfrak{p})^{-s}}{\sum_{\mathfrak{p}} N(\mathfrak{p})^{-s}} = \lim_{s\to 1^+} \frac{\sum_{\mathfrak{p}\in S} N(\mathfrak{p})^{-s}}{\log\frac{1}{s-1}}$$

$\zeta_K(s)$ has a simple pole at $s=1$

③ $$\delta(S) = \lim_{X\to\infty} \frac{\#\{\mathfrak{p}\in S \mid N(\mathfrak{p}) \le X\}}{\#\{\mathfrak{p} \mid N(\mathfrak{p}) \le X\}}$$

<u>Prop 21.12</u>: If $\rho(S)$ exists, then $\rho(S) = d(S)$

If $\rho(S)$ and $\delta(S)$ exist, then $\rho(S) = \delta(S)$.

$(\rho(S) \in [0, 1])$

$$\mathcal{P}_1 = \{\text{prime } \mathfrak{p} \text{ of } \mathcal{O}_K \mid N(\mathfrak{p}) = [\mathcal{O}_K : \mathfrak{p}] \text{ is prime}\}$$

(residue field of $\mathfrak{p}$ is $\mathbb{F}_p$

$\mathcal{O}_K/\mathfrak{p} = \mathbb{F}_p$

$\mathcal{P}_1$: degree 1 prime

residue field degree

Prop 21.14(d):

$\rho(\mathcal{P}_1) = 1$ and if S has a polar density, then $\rho(S \cap \mathcal{P}_1) = \rho(S)$

Pf: Let $\mathcal{P}$ = set of all primes in K

For each rational prime p, there are at most $[K:\mathbb{Q}] = n$ primes $\mathfrak{p} \mid p$

at most $\frac{n}{2}$ primes above p in $\mathcal{P} - \mathcal{P}_1$,

each of which has norm $Nm(\mathfrak{p}) \geq p^2$

$(Nm(\mathfrak{p}) = p^f)$

$\zeta_{K, \mathfrak{p}-\mathfrak{p}_1}(s)$ can be compared with

$$\zeta(2s)^n = \sum_{\mathfrak{p}} \frac{1}{p^{2s}} = \prod_{\mathfrak{p}} \frac{1}{1-p^{-2s}}$$

$$\prod_{\mathfrak{p} \text{ deg 2 or higher}} \frac{1}{1-Nm(\mathfrak{p})^{-s}} \qquad Nm(\mathfrak{p}) \geq p^2$$

$\zeta_{K, \mathfrak{p}-\mathfrak{p}_1}(s)$ converges absolutely to a holomorphic function on $Re(s) > \frac{1}{2}$ is an Euler product therefore holomorphic/ nonvanishing on a neighborhood of $s=1$

$$\rho(\mathfrak{p}-\mathfrak{p}_1) = 0 \Rightarrow \rho(\mathfrak{p}_1) = 1.$$

then for any S with a polar density,

$$\rho(S \cap (\mathfrak{p}-\mathfrak{p}_1)) = 0 \Rightarrow \rho(S) = \rho(S \cap \mathfrak{p}_1)$$

$Spl(L/K)$ = set of primes in K that split completely in L.

Theorem 21.15: Let L/K is a Galois extension of number fields of degree n. Then $\rho(Spl(L/K)) = \frac{1}{n}$.

Pf: $\mathfrak{p}$ splits completely in L iff $e=1$ and $f=1$ ($\Rightarrow g=n$)

$(Spl(L/K) \cap P_1) = S$

degree 1

S = primes $\mathfrak{p}$ of K that split completely in L.

T = set of primes $\mathfrak{q}$ of L that lie above $\mathfrak{p} \in S$.

For each $\mathfrak{q} \in T$ lying above $\mathfrak{p} \in S$

$$Nm_{L/K}(\mathfrak{q}) = \mathfrak{p}^{f(\mathfrak{q}/\mathfrak{p})} = \mathfrak{p}$$

$$Nm_{L/\mathbb{Q}}(\mathfrak{q}) = Nm_{K/\mathbb{Q}}(Nm_{L/K}(\mathfrak{q}))$$

$$[\mathcal{O}_L : \mathfrak{q}] = Nm_{K/\mathbb{Q}}(\mathfrak{p}) = p \quad \text{by degree 1 assumption}$$

$\mathfrak{q}$ has to be a degree 1 prime

(since $\mathrm{Nm}_{L/\mathbb{Q}}(\mathfrak{q})$ is prime)

if $\mathfrak{q}$ is any unramified degree 1 prime in L

and let $\mathfrak{q} \cap \mathcal{O}_K = \mathfrak{p}$

$$\mathrm{Nm}_{L/\mathbb{Q}}(\mathfrak{q}) = \mathrm{Nm}_{K/\mathbb{Q}} \mathrm{Nm}_{L/K}(\mathfrak{q})$$

$$= \mathrm{Nm}_{K/\mathbb{Q}}(\mathfrak{p}^{f(\mathfrak{q}/\mathfrak{p})})$$

must be prime if $\mathfrak{q}$ is degree 1 prime.

then $\mathfrak{p}$ is also degree 1 prime and it splits completely in $L \Rightarrow \mathfrak{p} \in S$.

only finitely many primes ramify in L

so all but finitely many of degree 1 primes in L lie in T, thus $\rho(T) = 1$.

Each $\mathfrak{p} \in S$ has exactly n primes $\mathfrak{q} \in T$ lying above it, $\zeta_{L,T}(s) = \prod_{\mathfrak{q} \in T} \frac{1}{1 - N_{K/\mathbb{Q}}(\mathfrak{q})^{-s}}$

$$= \prod_{\mathfrak{q} \in T} \frac{1}{1 - N_{K_{\mathfrak{q}}/K}(N(\mathfrak{q})^{-s})}$$

$$= \prod_{\mathfrak{p} \in S} \left(\frac{1}{1 - N_{K_{\mathfrak{q}}}(\mathfrak{p})^{-s}} \right)^n$$

$$= \zeta_{K,S}(s)^n$$

$$\rho(S) = \frac{1}{n} \rho(T) = \frac{1}{n}. \qquad \square$$

We can conclude the Artin map is surjective: Thus we have an exact sequence

$$1 \longrightarrow \ker \psi_{Y_K}^m \longrightarrow \mathcal{C}_K^m \longrightarrow \mathrm{Gal}(Y_K) \longrightarrow 1$$

existence of ray class fields, more generally the idea that every finite abelian extension Y_K is a class field, comes from the fact that $\mathcal{R}_K^m \subseteq \ker \psi_{Y_K}^m$

$\mathcal{R}_K^m = \mathrm{im}(K^{m,\mathbb{1}})$

$$K^{\mathfrak{m},1} = \{\alpha \in K^\times \mid v_\mathfrak{p}(\alpha - 1) \geq v_\mathfrak{p}(\mathfrak{m}_\mathfrak{f})\}$$

Artin reciprocity: When L is a ray class field of K ($\mathfrak{R}_K^\mathfrak{m} = \ker \psi_{L/K}^\mathfrak{m}$) the Artin map allows us to relate the subfields of L containing K to quotients of ray class group

$$Cl_K^\mathfrak{m} = \mathcal{I}_K^\mathfrak{m} / \mathfrak{R}_K^\mathfrak{m} \cong Gal(L/K).$$

Theorem 21.18: If $L, M/K$ are a finite Galois extensions of number fields, then

$$L = M \iff Spl(L) = Spl(M)$$

One proves this by showing that

$$L = M \iff Spl(L) \sim Spl(M)$$

$$(Spl(L) - Spl(M)) \cup (Spl(M) - Spl(L))$$

is finite set

density 0

There is a map

$$\left\{\begin{array}{l}\text{finite Galois} \\ \text{extensions of } K\end{array}\right\} \longrightarrow \left\{\begin{array}{l}\text{sets of primes of } K \\ \text{that have a positive} \\ \text{polar density}\end{array}\right\}$$

$$L \longmapsto Spl(L/K)$$

Another way to look at Theorem 21.18 is the above map is injective.

$$L \subseteq M \iff Spl(M/K) \subseteq Spl(L/K)$$

Theorem 21.20: Let $\mathfrak{m}$ be a modulus for a number field K, and let L and M be finite abelian extensions of K unramified at all primes not dividing $\mathfrak{m}_f$. If

$$\ker \psi^{\mathfrak{m}}_{L/K} = \ker \psi^{\mathfrak{m}}_{M/K}, \text{ then } L = M$$

In particular, ray class fields are unique wherever they exist. (s.t $\ker \psi_{\mathfrak{m}}^{\mathfrak{m}} = R_K^{\mathfrak{m}}$).

Agenda: ① Discomfort

② Conductors (22.3)

- def'n
- properties

③ Norm Groups

Conductors

Def'n: Let L/K be a finite abelian extension of local fields.

The conductor $c(L/K)$ (sometimes $f(L/K)$)

① If K is archimedean, then

$$c(L/K) = \begin{cases} 1 & \text{if } L \cong \mathbb{C} \text{ and } K \cong \mathbb{R} \\ 0 & \text{otherwise} \end{cases}$$

② If K is nonarchimedean, and

$\mathfrak{p}$ is the maximal ideal of its valuation ring $\mathcal{O}_K$, then

$$c(L/K) := \min\left\{ n : 1+\mathfrak{p}^n \subseteq N_{L/K}(L^\times) \right\}$$

($1+\mathfrak{p}^n$ is a subgroup of $\mathcal{O}_K^\times$ for $n \geq 0$

For $n=0$, $1+\mathfrak{p}^0 = \mathcal{O}_K^\times$)

Exercise: Does the above def'n require L/K to be abelian?

If L/K is a finite abelian extension of global fields, then its conductor is the modulus:

$$c(L/K) : M_K \longrightarrow \mathbb{Z}$$

$$v \longmapsto c(L_w/K_v)$$

where K_v is the completion of K at v

and L_w is the completion of L at a place $w|v$ (L/K is Galois $\Rightarrow$ does not matter which place above v we choose)

Prop 22.25: Let L/K be a finite abelian extension of local or global fields. For each prime $\mathfrak{p}$ of K, we have

$$v_{\mathfrak{p}}(c(L/K)) = \begin{cases} 0 & \text{iff } \mathfrak{p} \text{ is unramified in } L \\ 1 & \text{iff } \mathfrak{p} \text{ is tamely ramified in } L \\ \geq 2 & \text{iff } \mathfrak{p} \text{ is wildly ramified in } L \end{cases}$$

$\mathfrak{q}$ a prime of L

$\downarrow$

$\mathfrak{p}$ a prime of K

$\downarrow$

p

$\mathfrak{p}$ is tamely ramified iff the rational prime p below $\mathfrak{p}$, $p \nmid e(\mathfrak{q}/\mathfrak{p})$

$\mathfrak{p}$ is wildly ramified iff $p \mid e(\mathfrak{q}/\mathfrak{p})$

Pf sketch:

(0) L/K abelian finite extension of local fields, archimedean

(1) L/K abelian finite extension of local fields, nonarchimedean

(a) $K^\times \cong \mathbb{Z} \times \mathcal{O}_K^\times \cong \mathbb{Z} \times (1+\mathfrak{p}^0)$

(b) $\mathcal{O}_K \longrightarrow \mathcal{O}_K/\mathfrak{p}$ induces a map

$$\mathcal{O}_K^\times \longrightarrow (\mathcal{O}_K/\mathfrak{p})^\times \text{ and kernel } 1+\mathfrak{p}^1$$

(c) For $n \geq 1$, $1+\mathfrak{p}^n/1+\mathfrak{p}^{n+1} \cong \mathcal{O}_K/\mathfrak{p}$

$$1+\pi^n x \longmapsto x$$

where π is a uniformizer, i.e. a generator of $\mathfrak{p}$.

(2) If L/K is unramified,

(a) $\mathrm{Nm}_{L/K}(\mathcal{O}_L^\times) = \mathcal{O}_K^\times$

official def'n If $x \in L$,

$\mathrm{Nm}_{L/K}(x)$ = determinant of the K-linear "multiplication by x" map

$$\ell \longmapsto x \cdot \ell$$

It is also $\mathrm{Nm}_{L/K}(\alpha) = \prod_{\sigma \in \mathrm{Hom}(L,\bar{L})} \sigma(\alpha)$

(b) Q: Can $\mathrm{Nm}_{L/K}(L^\times) = K^\times$?

(no unless $L = K$).

(c) $K^\times / \mathrm{Nm}_{L/K}(L^\times) \cong \mathrm{Gal}(L/K)$

(L/K unramified $\Rightarrow$ Galois group is cyclic).

(3) If L/K is totally ramified

$$K^\times / \mathrm{Nm}_{L/K}(L^\times) \cong \mathcal{O}_K^\times / \mathrm{Nm}_{L/K}(\mathcal{O}_L^\times)$$

If $\mathfrak{o}$ is the maximal ideal of $\mathcal{O}$, and $\mathfrak{p}$ is the maximal ideal of K,

then (a) If L/K is tame: $\mathrm{Nm}_{L/K}(1+\mathfrak{o}) = 1+\mathfrak{p}$

(b) If L/K is wild: $\mathrm{Nm}_{L/K}(1+\mathfrak{o}) \neq 1+\mathfrak{p}$

Exercise: With all these facts, one should be able to prove the theorem.

Lemma 22.26: Let $L_1, L_2/K$ be finite abelian extensions of local or global field K. If $L_1 \subseteq L_2$, then

$$c(L_1/K) \mid c(L_2/K)$$

Pf idea: in nonarchimedean local case

$$\mathrm{Nm}_{L_2/K}(L_2^\times) = \mathrm{Nm}_{L_1/K} \circ \mathrm{Nm}_{L_2/L_1}(L_2^\times)$$

$\subseteq N_{M_{L/K}}(L^\times)$

Agenda

1. First Parhcipatory Democracy
2. Norm groups and congruence subgroups
3. CFT, ideal-theoretic precise version
4. Fundamental Inequalities of CFT necessary in the structure of the proof of Artin Reciprocity

---

Norm Groups: For a finite abelian extension L/K, in order to define the Artin $\psi_{L/K}^{\mathfrak{m}}$, one must choose a modulus containing all the primes of K that ramify in L. Say we have such an $\mathfrak{m}$: $\psi_{L/K}^{\mathfrak{m}} : \mathcal{I}_K^{\mathfrak{m}} \longrightarrow \mathrm{Gal}(L/K)$

We have a norm map on ideals

$$N_{L/K} : \mathcal{I}_L \longrightarrow \mathcal{I}_K$$

$$\prod_{i<\infty} \mathfrak{q}_i^{n_i} \longmapsto \prod_i \mathfrak{p}_i^{n_i \cdot f_i}$$

$\mathfrak{q}_i \cap \mathcal{O}_K = \mathfrak{p}_i$

$f_i = [\mathcal{O}_L/\mathfrak{q}_i : \mathcal{O}_K/\mathfrak{p}_i]$

In Sutherland (Lecture 6), $Nm_{L/K}$ is defined as $Nm_{L/K}(\mathfrak{q}) \overset{\text{def'n}}{=} [\mathcal{O}_L : \mathfrak{q}]_{\mathcal{O}_K} \overset{6.10}{=} \mathfrak{p}^f$ where $f = [\mathcal{O}_K/\mathfrak{q} : \mathcal{O}_L/\mathfrak{p}]$

"module index" ideal of $\mathcal{O}_K$ (6.1)

Recall that we defined the ray class field of modulus $\mathfrak{m}$ to be the field L such that $\ker \psi^{\mathfrak{m}}_{L/K} = \mathcal{P}^{\mathfrak{m}}_K = \mathrm{im}(K^{\mathfrak{m},1})$

We want to consider what the kernels are in other situations (for class fields that are not ray class fields):

Def'n 22.27: Let L/K be a finite abelian

extension of number fields, and let $\mathfrak{m}$ be a modulus for K divisible by the conductor $(\mathfrak{f})$.

The <u>norm group</u> associated to $\mathfrak{m}$ is the congruence subgroup

$$T_{L/K}^{\mathfrak{m}} := \mathcal{R}_K^{\mathfrak{m}} \cdot \mathrm{Nm}_{L/K}\left(\mathcal{I}_L^{\mathfrak{m}}\right)$$

Takagi

$\mathcal{I}_K^{\mathfrak{m}}$ $\quad$ $\mathcal{I}_K^{\mathfrak{m}}$

where $\mathcal{I}_L^{\mathfrak{m}}$ = subgroup of fractional ideals in $\mathcal{I}_L$ that are coprime to $\mathfrak{m}_{\mathfrak{f}}\mathcal{O}_L$.

<u>Prop 22.28:</u> Let L/K be a finite abelian extension of number fields, and let $\mathfrak{m}$ be a modulus for K divisible by the conductor of L/K. Then

$$\ker \psi_{L/K}^{\mathfrak{m}} \subseteq T_{L/K}^{\mathfrak{m}}$$

<u>Pf:</u> Let $\mathfrak{p}$ be a prime of K that lies in $\ker \psi_{L/K}^{\mathfrak{m}}$. Then $\mathfrak{p}$ is a prime coprime to $\mathfrak{m}_{\mathfrak{f}}$ and splits completely in L, i.e.

$e=1, f=1$. There is at least one prime $\mathfrak{q}$ of L above $\mathfrak{p}$, and $Nm_{L/K}(\mathfrak{q}) = \mathfrak{p}^f = \mathfrak{p}$

so $\mathfrak{p} \in Nm_{L/K}(\mathcal{I}_L^{\mathfrak{m}}) \subseteq T_{L/K}^{\mathfrak{m}}$. □

Theorem 22.29: Let L/K be a finite abelian extension of number fields and let $\mathfrak{m}$ be a modulus for K divisible by conductor of L/K.

Then $$\left[\mathcal{I}_K^{\mathfrak{m}} : T_{L/K}^{\mathfrak{m}}\right] \leq [L:K]$$

Pf sketch:

(1) $T_{L/K}^{\mathfrak{m}}$ is a congruence subgroup that contains all the primes of K that split completely in L: To see this, if $\mathfrak{p}$ splits completely, then $f=1$ and for any prime $\mathfrak{q}$ (of L) $|\mathfrak{p}$ we have $Nm_{L/K}(\mathfrak{q}) = \mathfrak{p}^f = \mathfrak{p}$ and therefore

$$\mathfrak{p} \in T_{L/K}^{\mathfrak{m}} = \mathcal{R}_{L/K}^{\mathfrak{m}} Nm_{L/K}(\mathcal{I}_L^{\mathfrak{m}})$$

(2) Since $\rho(\mathrm{Spl}(L/K)) = \frac{1}{[L:K]}$ and this equal to the Dirichlet density

Also, $\mathrm{Spl}(L/K) \subseteq \{\mathfrak{p} \in T^{\mathfrak{m}}_{L/K}\}$

What we need to conclude the inequality is $\{\mathfrak{p} \in T^{\mathfrak{m}}_{L/K}\}$ has Dirichlet density $\frac{1}{[\mathcal{C}\ell^{\mathfrak{m}}_K : T^{\mathfrak{m}}_{L/K}]}$

$$\Rightarrow \frac{1}{[L:K]} = d(\mathrm{Spl}(L/K)) \leq d(\{\mathfrak{p} \in T^{\mathfrak{m}}_{L/K}\}) = \frac{1}{[\mathcal{C}\ell^{\mathfrak{m}}_K : T^{\mathfrak{m}}_{L/K}]}$$

Ideal-Theoretic Version of CFT: Now with precision!!

Let $\mathfrak{m}$ be a modulus for a number field K

- Existence: The ray class field $K(\mathfrak{m})$ exists
- Completeness: If L/K is a finite abelian extension then $L \subseteq K(\mathfrak{m})$ iff $\mathfrak{e}(L/K) \mid \mathfrak{m}$

In particular every finite abelian extension L/K lies in a ray class field.

- Artin Reciprocity: For each subextension L/K of $K(\mathfrak{m})$, we have $\ker \psi^{\mathfrak{m}}_{L/K} = T^{\mathfrak{m}}_{L/K}$ and $c(L/K) \mid \mathfrak{m}$ and a canonical isomorphism

($c(L/K)$: conductor)

$$\mathcal{C}l^{\mathfrak{m}}_K / T^{\mathfrak{m}}_{L/K} \cong \mathrm{Gal}(L/K)$$

Artin reciprocity can be described in terms of a commutative diagram: Fix K and modulus $\mathfrak{m}$

$$L \longmapsto T^{\mathfrak{m}}_{L/K}$$

$$\begin{array}{ccc}
\left\{\begin{array}{l}\text{finite abelian extensions } L/K \\ \text{w/ } c(L/K) \mid \mathfrak{m}\end{array}\right\} & \longrightarrow & \left\{\begin{array}{c}\text{congruence subgroups} \\ C \subseteq \mathcal{C}l^{\mathfrak{m}}_K\end{array}\right\} \\
\Big\downarrow L & & \Big\downarrow C \\
\left\{\text{quotients of } \mathrm{Gal}(K(\mathfrak{m})/K)\right\} & \xleftarrow[\psi^{\mathfrak{m}}_{L/K}]{\sim} & \left\{\text{quotients of } \mathcal{C}l^{\mathfrak{m}}_K\right\}
\end{array}$$

(the vertical arrows: $L \mapsto \mathrm{Gal}(L/K)$ and $C \mapsto \mathcal{C}l^{\mathfrak{m}}_K/C$)

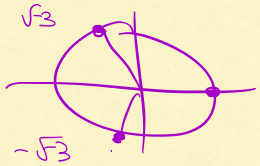
Def'n 22.1: Let K be a number field, and let $\mathfrak{m}$ be a modulus for K. A <u>congruence subgroup for the modulus $\mathfrak{m}$</u> is a subgroup C of $\mathcal{I}_K^{\mathfrak{m}}$ that contains $\mathcal{P}_K^{\mathfrak{m}} = \mathrm{im}(K^{\mathfrak{m},1})$.

We will use $\bar{C}$ to denote the image of C in $\mathcal{I}_K^{\mathfrak{m}}/\mathcal{P}_K^{\mathfrak{m}} = Cl_K^{\mathfrak{m}}$.

Example: $K = \mathbb{Q}$ $\quad L = \mathbb{Q}[x]/(x^3 - 3x - 1)$ cubic (cyclic)

$\Rightarrow$ L ramifies only at 3.

can define $\psi_{L/K}^{\mathfrak{m}}$ for any modulus $\mathfrak{m}$ divisible by (3).



The ray class field for $\mathfrak{m} = (3)$ is $\mathbb{Q}(\zeta_3 + \zeta_3^{-1}) = \mathbb{Q}$

The ray class field for $\mathfrak{m} = (3)\infty$ is $\mathbb{Q}(\zeta_3) = \mathbb{Q}(\sqrt{-3})$

neither of these fields contain L, and so $\ker(\psi_{L/K}^{\mathfrak{m}})$ does not contain $\mathcal{P}_K^{\mathfrak{m}}$ for either

$\mathfrak{m} = (3)$ or $\mathfrak{m} = (3)\infty$, and so $\ker$ is not a congruence subgroup for either modulus.

On the other hand, L is equal to the ray class field of modulus $\mathfrak{m} = (9)$

Exercise: $\mathbb{Q}(\zeta_9 + \zeta_9^{-1}) = \mathbb{Q}[x]/(x^3 - 3x - 1)$

so $\ker \psi_{L/K}^{(9)}$ contains (is equal to) $R_K^{(9)} := \mathrm{im}(\mathbb{Q}^{9,1})$ and is thus a congruence subgroup for the modulus $\mathfrak{m} = (9)$.

Def'n: Let K be a number field. The Hilbert (ray) class field of K is the maximal unramified abelian extension of K, i.e. the compositum of all finite unramified abelian extensions of K. (inside a fixed algebraic closure of K).

unramified away from $\mathfrak{m}$ for which the primes in $\mathbb{P}_K^{\mathfrak{m}}$ split completely.

It is not clear :
- Hilbert class field is finite.
- not clear if it is a ray class field.

Fact: Hilbert class field is indeed ray class field of modulus (1).

Agenda: ① Huron-Wendat Nation

② $[\mathcal{I}_K^m : T_{L/K}^m] \geq [L:K]$

for $m=1$, L/K cyclic unramified.

③ motivate Group/Tate cohomology and Herbrand quotients.

L/K finite abelian extension. Let m be a modulus for K s.t. $\mathfrak{c}(L/K) \mid m$.

$$\psi_{L/K}^m : \mathcal{I}_K^m \longrightarrow \mathrm{Gal}(L/K)$$

Last time, we showed that $T_{L/K}^m$ contains the $\ker \psi_{L/K}^m$

$$\Rightarrow [\mathcal{I}_K^m : T_{L/K}^m] \leq [L:K] = \#\mathrm{Gal}(L/K)$$

Want to show $T_{L/K}^m = \ker \psi_{L/K}^m$

Let $\mathfrak{m}=1$, only consider L/K cyclic w/ conductor $\mid \mathfrak{m} \Rightarrow L/K$ is unramified at every prime.

$\mathcal{P}_K$ = principal fractional ideals of K

$= \mathrm{im}(K^\times)$ under the map $K^\times \longrightarrow \mathcal{I}_K$, $\alpha \longmapsto (\alpha)$

$\mathcal{P}_K^1 = \mathcal{P}_K$

$\|$

$\mathrm{im}(K^{1,1}) =$ $\longrightarrow$ nonzero elements of K that are $1 \bmod 1$.

Theorem 24.12: Let L/K be a totally unramified cyclic extension of number fields.

Then ~~$[\mathcal{I}_K : \mathcal{P}_{K,\mathfrak{m}}]$~~

$$[\mathcal{I}_K' : \mathcal{P}_K \mathrm{Nm}(\mathcal{I}_L')] \geq [L:K]$$

("$\downarrow$" "N")

Pf: We have

$$[\mathcal{I}_K : \mathcal{P}_K \mathrm{Nm}(\mathcal{I}_L)] = \frac{[\mathcal{I}_K : \mathcal{P}_K]}{[\mathcal{P}_K \mathrm{Nm}(\mathcal{I}_L) : \mathcal{P}_K]} = \frac{\#Cl(K)}{[\mathcal{P}_K \mathrm{Nm}(\mathcal{I}_L) : \mathcal{P}_K]}$$

same

$$[Nm(\mathcal{O}_L)\mathfrak{P}_K : \mathfrak{P}_K] = [Nm(\mathcal{O}_L) : Nm(\mathcal{O}_L) \cap \mathfrak{P}_K]$$

If $Nm^{-1} : Nm(\mathcal{O}_L) \longrightarrow \mathcal{O}_L$ denotes the

n | K

(surjective) group homomorphism

$$\prod_{i<\infty} \mathfrak{p}_i^{n_i} \longmapsto \prod_{i<\infty} \mathfrak{q}_i^{n_i/f_i}$$ ← residue field degree

where $\mathfrak{q}_i$ is a fixed choice of prime ideal above $\mathfrak{p}_i$.

then, $\ker(Nm^{-1})$ is trivial and therefore contained in $\mathfrak{P}_K$.

0 ker ⟶ 0 ker

$$\ker Nm^{-1} \hookrightarrow \mathfrak{P}_K \xrightarrow{Nm^{-1}} Nm^{-1}(\mathfrak{P}_K) \longrightarrow 0$$

$$\ker Nm^{-1} \hookrightarrow Nm(\mathcal{O}_L) \cap \mathfrak{P}_K \xrightarrow{Nm^{-1}} Nm^{-1}(Nm(\mathcal{O}_L) \cap \mathfrak{P}_K) \to 0$$

coker $\boxed{0}$ coker $=$ coker 0

$$[\mathrm{Nm}(\mathcal{O}_L) : \mathrm{Nm}(\mathcal{O}_L) \cap \mathfrak{P}_K] = [\mathcal{O}_L : \mathrm{Nm}^{-1}(\mathfrak{P}_K)]$$

Exercise: ↗ application of Snake

Lemma, but how do we define

$\mathrm{Nm}^{-1}(\mathfrak{P}_K)$ because Nm^{-1} is defined on $\mathrm{Nm}(\mathcal{O}_L)$

why does it contain $\mathfrak{P}_K$?

One suggestion: Consider for every $(\alpha) \in \mathfrak{P}_K$

consider $(\alpha)\mathcal{O}_L$ $(\alpha \in K^\times \subset L^\times)$

$$[\mathcal{O}_L : \mathrm{Nm}^{-1}(\mathfrak{P}_K)] = [\mathcal{O}_L/\mathfrak{P}_L : \mathrm{Nm}^{-1}(\mathfrak{P}_K)/\mathfrak{P}_L]$$

$$= [[\mathcal{O}_L : \mathrm{Nm}^{-1}(\mathfrak{P}_K)/\mathfrak{P}_L]]$$

$\mathrm{Gal}(L/K)$-modules homomorphism

Define $N_{\mathrm{Gal}(L/K)} : \mathcal{O}_L \longrightarrow \mathcal{O}_L$

$$[\alpha] \longmapsto \left[\left(\sum_{g \in \mathrm{Gal}(L/K)} g\right) \cdot \alpha\right]$$

Here, if $\mathfrak{q} = \mathfrak{q}_1$ and $\mathfrak{q}_2, \ldots, \mathfrak{q}_g$ are the other primes of L above $\mathfrak{q} \cap \mathcal{O}_K = \mathfrak{p}$.

Assume $g \in \mathrm{Gal}(L/K)$ is a generator,

$g(\mathfrak{q}_1) = \mathfrak{q}_2$ orders the prime ideals above $\mathfrak{p}$ s.t. $g(\mathfrak{q}_i) = \mathfrak{q}_{i+1}$ and $g(\mathfrak{q}_g) = \mathfrak{q} = \mathfrak{q}_1$

$$[\mathfrak{q}] \longmapsto \left(\sum [\mathfrak{q}_i] \right) \quad \#\text{Decomposition group}$$

$\leftarrow Cl_L$ as $\mathbb{Z}[\mathrm{Gal}(L/K)]$-module

$$\left[(Cl_L : Nm^{-1}(\mathfrak{p}_K)/\mathfrak{p}_L \right] = \left[Cl_L : Cl_L / N_{\mathrm{Gal}(L/K)}(Cl_L) \right]$$

$$= \# N_{\mathrm{Gal}(L/K)}(Cl_L).$$

$$= \frac{\# Cl_L^{\mathrm{Gal}(L/K)}}{\left[Cl_L^{\mathrm{Gal}(L/K)} : N_{\mathrm{Gal}(L/K)}(Cl_L) \right]}$$

$Cl_L^{\mathrm{Gal}(L/K)} = \mathrm{Gal}(L/K)$-invariant subgroup

of $\mathbb{Q}(\zeta)$.

class group formula:

use cohomology to compute numerator and denominator

$$[\mathcal{O}_K^\times : \mathrm{Nm}(\mathcal{O}_L^\times)\mu_K] \geq [L:K].$$

Assume that G a finite group

Def 23.29: The norm element of $\mathbb{Z}[G]$ is $N_G = \sum_{g \in G} g$

(If G cyclic, $N_G = \sum \sigma^i$)

Define the G-module endomorphism:

$$N_G : A \to A$$

$$a \mapsto N_G a.$$

I_G = augmentation ideal in $\mathbb{Z}[G]$, generated by elements of the form $g - e_g$ (e identity).

(If $G = \langle \sigma \rangle$, $I_G = (\sigma - e_G)$)

Lemma 23.30: A G-module, $I_G(A) \le \ker N_G$. $\operatorname{Im} N_G \le A^G$

N_G induces a morphism $\hat{N}_G : \hat{A}_G \to A^G$, with $\hat{A}_G = A/I_G A$

Pf: If $g \in G$, $g \circ N_G = N_G$ (g permute the order) $\Rightarrow \operatorname{Im} N_G \le A^G$

$N_G \cdot (g - e_g) = 0 \quad \forall g \in G$. So N_G annihilates I_G and $I_G A \le \ker N_G$.

Def 23.31: A a G-module, $|G| < \infty$, For $n \ge 0$, the **Tate Cohomology**

$$\hat{H}^n(G, A) := \begin{cases} \operatorname{coker} \hat{N}_G & \text{for } n = 0 \\ H^n(G, A) & \text{for } n > 0. \end{cases}$$

$$\hat{H}^{-n}(G, A) := \begin{cases} \ker \hat{N}_G & \text{for } n = 1 \\ H_n(G, A) & \text{for } n > 1 \end{cases}$$

$H_n(G, A)$ is defined as $\ker d_{n*} / \operatorname{im} d_{n+1*}$

where $\cdots \longrightarrow \mathbb{Z}[G^{n+1}] \otimes_{\mathbb{Z}[G]} A \xrightarrow{d_{n*}} \mathbb{Z}[G^n] \otimes_{\mathbb{Z}[G]} A \to \cdots \to \mathbb{Z}[G] \otimes_{\mathbb{Z}[G]} A \to \mathbb{Z} \otimes_{\mathbb{Z}[G]} A \to 0$

where d_{n*} is defined by $(g_0, \cdots, g_n) \otimes a \mapsto d_n(g_0, \cdots, g_n) \otimes a$.

$$d_n(g_0, \cdots, g_n) = \sum_{i=0}^{n} (-1)^i (g_0, \cdots, g_{i-1}, g_{i+1}, \cdots, g_n)$$

Def 4.34:

$\mathbb{Z}[G^n]$ in a $\mathbb{Z}[G]$-module and a ring A is a $\mathbb{Z}[G]$-module

$\mathbb{Z}[G^n] \otimes_{\mathbb{Z}[G]} A$ is a $\mathbb{Z}[G^n]$-module, $z(z' \otimes a) = zz' \otimes a$.

Note: the action of $\mathbb{Z}[G]$ on $\mathbb{Z}[G^n]$ has to be a right action

$(g_1, \cdots, g_n) \cdot g = (g_1 g, \cdots, g_n g)$

$A/I_G A \cong \mathbb{Z} \otimes_{\mathbb{Z}[G]} A$

Thm 23.34: Let $|G| < \infty$, $B = \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G], A)$ for some abelian group A

Then $\hat{H}(G, B) = 0$, $\forall n \in \mathbb{Z}$

Cor 23.38: If A a free $\mathbb{Z}[G]$ module, then $\hat{H}(G, A) = 0$, $\forall n \in \mathbb{Z}$

Thm 23.37: Let $G = \langle g \rangle$, A a G-module

$\forall n \in \mathbb{N}$ $\hat{H}^{2n}(G, A) \cong \hat{H}^0(G, A) = \mathrm{coker}\, \hat{N}_G = \ker \langle g - eg \rangle / \mathrm{Im}\, N_G$.

$\hat{H}^{2n-1}(G, A) \cong \hat{H}_0(G, A) = \ker \hat{N}_G = \ker N_G / \mathrm{Im} \langle g - eg \rangle$

Cor 23.40: $G = \langle \sigma \rangle$ finite, then for an exact sequence of G-modules $0 \to A \to B \to C \to 0$

we have an exact hexagon: