Algebraic Number Theory. (lecture 1) 19/1/2024

Topics: ⊛ Global CFT (ideal theoretic + idele theoretic)
⊛ Zeta functions + L-series
⊛ Density Theorems.

Rough Goals: 1) Given NF K, what are its abelian exts?

If $K = \mathbb{Q}$: ⇒ Kronecker-Weber:

Any finite + Abelian ext. of $\mathbb{Q}$ is in some $\mathbb{Q}(\zeta_n)$, $n \in \mathbb{N}$.

⇒ Finite abelian $\mathbb{Q}$-exts are generated by special values of exponential function $z \mapsto e^{2\pi i z}$.

Open problem: Can we explicitly construct all abelian exts, for arbitrary NF K?

Partial Answer: for imaginary QF's, can construct using special values of analytic functions (elliptic + Modular fn's).

In Class Fields, we classify: exts using notion of class fields.

For K NF: will show: any finite Abelian ext. of K is contained in a Class Field; & its Galois group is $\cong$:

- (ideal) Generalised ideal class group
- (idele) Subgroup of the idele class group.

2) Given finite + Abelian ext: how do the prime ideals in smaller field behave in the extension?

* Quadratic Case: $\Rightarrow$ Quadratic Reciprocity.

Most generally: Decomposition Law. Consequence of Artin reciprocity Theorem.

Basic ANT.] K NF, $\Rightarrow \mathcal{O}_K \equiv$ ring of ints.

$\mathcal{O}_K$ Dedekind $\Rightarrow$ any $I \subseteq \mathcal{O}_K$ ideal has unique fact. into product of prime ideals of $\mathcal{O}_K$.

If L/K ext. of NF's: $\&$ $\mathfrak{p} \subseteq \mathcal{O}_K$ prime: then $\mathfrak{p}\mathcal{O}_L \subseteq \mathcal{O}_L$ is an ideal, so $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_h^{e_h}$, (distinct $\mathfrak{P}_i$) $\&$ ($e_i \geq 1$ $\forall i$.)

In this case: write $\mathfrak{P}_i \mid \mathfrak{p}$.

$\&$ $e_i \equiv$ Ramification indices for $\mathfrak{P}_i$. $e_i \equiv e_{\mathfrak{P}_i/\mathfrak{p}}$.

Say: $\mathfrak{p}$ unramified in $L \iff (e_i = 1 \ \forall i)$, and ramified else.

Say: $\mathfrak{p}$ totally ramified in $L \iff \mathfrak{p}\mathcal{O}_L = \mathfrak{P}^e$ with $e = e_{\mathfrak{P}/\mathfrak{p}} = [L:K]$

Say: $\mathfrak{p}$ inert in $L \iff \mathfrak{p}\mathcal{O}_L$ prime

Say: $\mathfrak{p}$ splits completely in $L \iff k = [L:K]$.

Note: $\mathcal{O}_K/\mathfrak{p}$ is finite field, of characteristic p, where $\mathfrak{p} \cap \mathcal{O}_K = p\mathbb{Z}$. This is called the Residue Field.

If $\mathfrak{P}/\mathfrak{p}$ ($\mathfrak{P} \subseteq \mathcal{O}_L$, $\mathfrak{p} \subseteq \mathcal{O}_K$): can view $\mathcal{O}_K/\mathfrak{p} \subseteq \mathcal{O}_L/\mathfrak{P}$ as a subfield. Then, $f_{\mathfrak{P}/\mathfrak{p}} \equiv [\mathcal{O}_L/\mathfrak{P} : \mathcal{O}_K/\mathfrak{p}]$.

$\Rightarrow$ If $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_k^{e_k}$, then: $\sum_i e_{\mathfrak{P}_i/\mathfrak{p}} f_{\mathfrak{P}_i/\mathfrak{p}} = [L:K]$.

$\&$ If L/K Galois: then since Galois group permutes $\mathfrak{P}_i$, $\square 2$

get: $e_1 = \cdots = e_k = e$.

& also have $f_1 = \cdots = f_k = f$. So, $ef \cdot k = [L:K]$.

Recall: (Kummer – Dedekind): Can find factorisation of $p\mathcal{O}_L$.

& $p \subseteq \mathcal{O}_K$ ramifies in $L/K \Leftrightarrow p \mid d_{L/K}$ discriminant (ideal).

DEF 1) Decomp group $D_p = \{\sigma \in Gal(L/K) : \sigma(p) = p\}$

& Inertia subgroup $I_p \equiv \{\sigma \in Gal(L/K) : \sigma(\alpha) \equiv \alpha \bmod p\}$.
$\forall \alpha \in \mathcal{O}_L$:

$\Rightarrow I_p \subseteq D_p$.

$\forall \sigma \in D_p$: induces $\bar{\sigma} : \mathcal{O}_L/p \longrightarrow \mathcal{O}_L/P$, such that:

$\bar{\sigma}|_{\mathcal{O}_K/p} = id|_{\mathcal{O}_K/p}$, $p = P \cap \mathcal{O}_K$.

$\Rightarrow$ Get map $D_p \longrightarrow Gal(\mathcal{O}_L/P / \mathcal{O}_K/p)$.

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

Prop 2) 1) $Gal(\mathcal{O}_{L/P} / \mathcal{O}_{K/p})$ cyclic & $= \langle x \mapsto x^{Fr_q} \rangle$.
$(q = |\mathcal{O}_K/p|)$

2) $D_p \longrightarrow Gal(\mathcal{O}_L/P / \mathcal{O}_K/p)$ surjective hom
$\sigma \longmapsto \bar{\sigma}$ + kernel $= I_p$.

3) $|I_p| = e_{P/p}$ & $|D_p| = e_{P/p} f_{P/p}$.

Recall: if $P|p$: Norm $N_{L/K}(P) = p^{f_{P/p}}$.

If p prime in k: write $N(p) \equiv N_{K/\mathbb{Q}}(p)$ and also $N(p) = |\mathcal{O}_K/p|$.

Artin Symbol]

[lemma 3] L/K Galois & $p \subseteq \mathcal{O}_K$ prime. Unramified in L. If $P|p$ ($P \subseteq \mathcal{O}_L$) then $\exists!\, \sigma \in Gal(L/K)$ s.t. $\forall \alpha \in \mathcal{O}_L$: $\sigma(\alpha) \equiv \alpha^{N(p)} \mod P$.

Proof] Let $\sigma \in D_P$ & $\overline{\sigma} \in Gal(\mathcal{O}_L/P, \mathcal{O}_K/p)$ image under map from Prop 2.

By assumption: p unramified, so: $|I_P| = 1$

$\Rightarrow$ $D_P \xrightarrow{\cong} Gal(\mathcal{O}_L/P, \mathcal{O}_K/p)$ (Prop 2)

& This group is generated by Frobenius element $x \mapsto x^q$, $q = |\mathcal{O}_K/p|$. So, choose $\sigma \in D_P$ unique element that maps to Frobenius under this $\cong$.

$\Rightarrow \sigma(\alpha) \equiv \alpha^q \mod P$ $\forall \alpha \in \mathcal{O}_L$, $q = |\mathcal{O}_K/p| = N(p)$. ✓

Uniqueness: follows since any $\sigma \in Gal(L/K)$ satisfying both conditions is an element of D_P. ✓

ANT: lecture 2 | 22/01/2024

let: L/K Galois, $\mathfrak{p} \subseteq \mathcal{O}_K$, $\mathfrak{P} \subseteq \mathcal{O}_L$ lying above it.

From last time: $\exists! \sigma \in Gal(L/K)$ s.t. $\sigma(\alpha) \equiv \alpha^{N(\mathfrak{p})} \bmod \mathfrak{P}$ $\forall \alpha \in \mathcal{O}_K$.

The unique σ is called: Artin symbol $\left(\frac{L/K}{\mathfrak{P}}\right)$.

DEF V] For p odd prime (in $\mathbb{Z}$) & $a \in \mathbb{Z}$: Legendre symbol

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

For $n = u \cdot p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ $(u = \pm 1)$ $(n \in \mathbb{Z})$. & $a \in \mathbb{Z}$. The Kronecker Symbol $\left(\frac{a}{n}\right) = \left(\frac{a}{u}\right) \cdot \prod_i \left(\frac{a}{p_i}\right)^{\alpha_i}$, where:

$$\left(\frac{a}{2}\right) = \begin{cases} 0 & \text{if } 2 \mid a \\ +1 & \text{if } a \equiv \pm 1 \bmod 8 \\ -1 & \text{if } a \equiv \pm 3 \bmod 8 \end{cases} \quad \& \quad \left(\frac{a}{1}\right) = 1$$

$$\left(\frac{a}{-1}\right) = \begin{cases} -1 & \text{if } a < 0 \\ 1 & \text{if } a \geq 0. \end{cases}$$

Quadratic case: $K = \mathbb{Q}$, $L = \mathbb{Q}(\sqrt{N})$. $N \neq 0, 1$ squarefree.

⇒ From Part II NF: $d_{L/K} = \begin{cases} N & \text{if } N \equiv 1 \bmod 4 \\ 4N & \text{if } N \not\equiv 1 \bmod 4. \end{cases}$

& $\mathcal{O}_L = \begin{cases} \mathbb{Z}\left[\frac{1+\sqrt{N}}{2}\right] & \text{if } N \equiv 1 \bmod 4 \\ \mathbb{Z}[\sqrt{N}] & \text{if } N \not\equiv 1 \bmod 4. \end{cases}$

⇒ $Gal(L/K)$ has 2 elements: $\begin{cases} 1 : \sqrt{N} \to \sqrt{N} \\ \sigma : \sqrt{N} \to -\sqrt{N}. \end{cases}$

⇒ Identify $Gal(L/K)$ with $\{\pm 1\}$.

Then, Artin symbol:

If $\mathfrak{p} \subseteq L$ unramified & $\mathfrak{P} \subseteq \mathcal{O}_L$ lying above $\mathfrak{p}$, then: write, for $\sigma \in Gal(L/K)$, $\sigma(x) \equiv x^p \bmod \mathfrak{P}$ $\forall x \in \mathcal{O}_L$.

Then exercise: $\left(\frac{L/K}{\mathfrak{p}}\right) = \left(\frac{d_{L/\mathbb{Q}}}{\mathfrak{p}}\right) = \pm 1 \quad (\mathfrak{p} \nmid d_{L/\mathbb{Q}})$.

Prop 6] Suppose $\mathfrak{p}$ unramified in L. Then, $\mathfrak{p}$ splits in K iff $\left(\frac{d_{L/K}}{\mathfrak{p}}\right) = 1$. ($\Rightarrow$ Artin symbol tells you about decomp.)

Lemma 7] L/K Galois, $\mathfrak{p} \subseteq \mathcal{O}_K$ unram. & $\mathfrak{P} \subseteq \mathcal{O}_L$ $\mathfrak{P} | \mathfrak{p}$.

1) $\forall \sigma \in \mathrm{Gal}(L/K)$: $\sigma \left(\frac{L/K}{\mathfrak{P}}\right) \sigma^{-1} = \left(\frac{L/K}{\sigma(\mathfrak{P})}\right)$.

2) $\left(\frac{L/K}{\mathfrak{P}}\right)$ has order $f = f_{\mathfrak{P}/\mathfrak{p}}$.

3) $\mathfrak{p}$ splits completely in $L \iff \left(\frac{L/K}{\mathfrak{P}}\right) = 1$. $\forall \mathfrak{P} | \mathfrak{p}$.

DEF 8] L/K Abelian ext $\iff$ Galois (ext of NF's) with Abelian Galois group $\mathrm{Gal}(L/K)$.

Let: L/K Abelian, $\mathfrak{p} \subseteq \mathcal{O}_K$ unram & $\mathfrak{P}, \mathfrak{P}' \subseteq \mathcal{O}_L$ lying above $\mathfrak{p}$.

Then: $\exists \sigma \in \mathrm{Gal}(L/K)$, $\sigma(\mathfrak{P}) = \mathfrak{P}'$ (LF, last term)

$\Rightarrow \left(\frac{L/K}{\mathfrak{P}'}\right) = \left(\frac{L/K}{\sigma(\mathfrak{P})}\right) = \sigma \left(\frac{L/K}{\mathfrak{P}}\right) \sigma^{-1} = \left(\frac{L/K}{\mathfrak{P}}\right)$. (abelian)

So, if L/K Abelian, can write $\left(\frac{L/K}{\mathfrak{p}}\right)$ for $\left(\frac{L/K}{\mathfrak{P}}\right)$ $\forall \mathfrak{P} | \mathfrak{p}$.

$\Rightarrow$ Defines map: $\left\{ \begin{matrix} \text{Unram primes} \\ \mathfrak{p} \subseteq \mathcal{O}_K \text{ in } L \end{matrix} \right\} \longrightarrow \mathrm{Gal}(L/K)$

$$\mathfrak{p} \longmapsto \left(\frac{L/K}{\mathfrak{p}}\right).$$

Question: how to extend this map?

Interlude (Fractional Ideals). Let: K NF.

Recall: $a \subseteq K$ is Fractional ideal $\iff$ is $\mathcal{O}_K$-submodule of K, and: $\exists\, 0 \neq x \in \mathcal{O}_K$, s.t. $xa \subseteq \mathcal{O}_K$.

Equivalently, of form αI, for $\alpha \in K$ & $I \subseteq \mathcal{O}_K$ ideal.

A frac ideal is <u>principal</u> $\Leftrightarrow$ Generated by some nonzero $\alpha \in K$.

Since $\mathcal{O}_K$ <u>Dedekind</u>: any fractional ideal is invertible, so obtain a group with identity $(1) = \mathcal{O}_K$.

<u>Notation</u> $I_K \equiv$ Group of ~~principal~~ fractional ideals of K

$P_K \equiv$ Subgroup of Principal ~~ideal~~ fractional ideals.

$I_K / P_K \equiv Cl_K \equiv$ Ideal Class Group.

<u>Know</u> (Part II NF): Cl_K <u>finite</u> abelian group, order h_K, called <u>class number</u> of K.

<u>Recall</u>: $\forall\, \underline{a} \in I_K$: $\exists$ unique fact. $\underline{a} = \prod_{i=1}^{n} \mathfrak{p}_i^{\alpha_i}$, $\alpha_i \in \mathbb{Z}$ and $\mathfrak{p}_i \subseteq \mathcal{O}_K$ distinct <u>prime</u> ideals.

<u>DEF 9</u> L/K Unramified ext ($\Leftrightarrow$ any prime unramified).

Define <u>Artin map</u> as the group hom:

$$\left(\frac{L/K}{\cdot}\right) : I_K \longrightarrow Gal(L/K), \quad \left(\frac{L/K}{\underline{a}}\right) = \prod_{i=1}^{n} \left(\frac{L/K}{\mathfrak{p}_i}\right)^{\alpha_i}.$$

<u>Question</u>: define it even more generally?

<u>Interlude</u> (<u>Finite + Infinite primes</u>).

For K NF: ~~$\mathfrak{p} \subseteq \mathcal{O}_K$~~ σ <u>infinite</u> prime $\Leftrightarrow$ Determined by the embeddings $K \xhookrightarrow{\sigma} \mathbb{C}$. Correspond to Archimedean absolute values (from part III LF).

An infinite prime is <u>real</u> $\Leftrightarrow$ is embedding $\sigma : K \to \mathbb{R}$

complex $\Leftrightarrow$ <u>pair</u> of embeds $\sigma, \bar{\sigma} : K \hookrightarrow \mathbb{C}$.

Examples 1) $\mathbb{Q}$ has one infinite real prime $\sigma(\frac{a}{b}) = \frac{a}{b}$

2) $\mathbb{Q}(\sqrt{2})$ has 2 real infinite primes $a+b\sqrt{2} \longmapsto a \pm b\sqrt{2}$.

3) $\mathbb{Q}(\sqrt{-2})$ has ~~2 imag.~~ one complex infinite primes $a+b\sqrt{-2} \mapsto a \pm b\sqrt{-2}$.

Remark L/K extension. An infinite prime σ of K ramifies in $L \iff$ σ real & has extension to L which is complex.

Example The (real) inf prime at $\mathbb{Q}$ unram. in $\mathbb{Q}(\sqrt{2})$, but ramified in $\mathbb{Q}(\sqrt{-2})$.

DEF 10 K NF, A modulus in K is formal product:

$\mathfrak{m} = \prod_{\mathfrak{p}} \mathfrak{p}^{n_{\mathfrak{p}}}$ over $\mathfrak{p} \subseteq \mathcal{O}_K$ prime (finite or infinite) s.t.

1) $n_{\mathfrak{p}} \geq 0$ $\forall \mathfrak{p}$ & finitely many $n_{\mathfrak{p}}$ nonzero

2) $n_{\mathfrak{p}} = 0$ for $\mathfrak{p}$ infinite & complex primes

3) $n_{\mathfrak{p}} \leq 1$ for $\mathfrak{p}$ infinite & real primes.

(If $n_{\mathfrak{p}} = 0$ $\forall \mathfrak{p}$, then set $\mathfrak{m} = 1$.)

Note: If K purely imaginary ($\iff$ no real primes), the modulus of K is just an ideal of $\mathcal{O}_K$.

Can write $\mathfrak{m}$ as $\mathfrak{m}_0 \cdot \mathfrak{m}_\infty$ for $\mathfrak{m}_0 \subseteq \mathcal{O}_K$ ideal, and $\mathfrak{m}_\infty$ product of distinct real/imag inf primes of $\mathcal{O}_K$.

Algebraic NT: lecture 3 — 24/01/2024.

From last time: Artin map & Moduli.

Defined: Artin map for unramified Abelian exts:

$\left(\frac{L/K}{\cdot}\right): I_K \longrightarrow Gal(L/K)$, by $\underline{a} \longmapsto \left(\frac{L/K}{\underline{a}}\right) = \prod_{i=1}^{n} \left(\frac{L/K}{\mathfrak{p}_i}\right)^{e_i}$.

Extend using moduli: $\underline{m} = \prod_{\mathfrak{p}} \mathfrak{p}^{n_{\mathfrak{p}}} = \underline{m}_0 \cdot \underline{m}_\infty$.

DEF 11] $\underline{m}$ modulus. Let: $I_K(\underline{m})$ = Group of fractional ideals coprime to $\underline{m}$: i.e. $\{\underline{a} \in I_K$ s.t. $v_{\mathfrak{p}}(\underline{a}) = 0 \ \forall \mathfrak{p} \mid \underline{m}\}$

[Note: infinite primes play no role in this def. $I_K(\underline{m}) = I_K(\underline{m}_0)$]

Example] $\underline{m} = (1) \Rightarrow I_K(\underline{m}) = I_K$.

If $K = \mathbb{Q}$ & $\underline{m} = (m)$, $(m \in \mathbb{Z}_{>0})$ then:

$I_{\mathbb{Q}}(\underline{m}) = \left\{\left(\frac{a}{b}\right)\mathbb{Z} : (a,m) = (b,m) = 1\right\}$.

Let L/K Abelian (not necessarily unram).

DEF 12] $\underline{m}$ modulus of K that is divisible by ALL primes that ramify in L. Then, the Artin map for L/K and $\underline{m}$ is a hom. $\Phi_{\underline{m}} = \Phi_{\underline{m},L/K,\underline{m}} : I_K(\underline{m}) \longrightarrow Gal(L/K)$ given by $\underline{a} \longmapsto \prod_i \left(\frac{L/K}{\mathfrak{p}_i}\right)^{e_i}$. $\left(\underline{a} = \prod \mathfrak{p}_i^{e_i}\right)$

Examples] $m \in \mathbb{Z}_{>0}$, ζ_m = m'th primitive root of 1.

$K = \mathbb{Q}$, $L = \mathbb{Q}(\zeta_m) \Rightarrow Gal(L/K) \cong (\mathbb{Z}/m\mathbb{Z})^\times$

$(\sigma : \zeta_m \mapsto \zeta_m^a) \mapsto a$.

& If a prime p ramifies in L, then: $p \mid m$.

let: $\underline{m} = (m)\infty \Rightarrow$ Divisible by all ramified prime ideals.

$\Rightarrow \Phi_{\underline{m}} : I_{\mathbb{Q}}(\underline{m}) \longrightarrow Gal(L/K) \cong (\mathbb{Z}/m\mathbb{Z})^{\times}$.

For $(\frac{a}{b})\mathbb{Z} \in I_{\mathbb{Q}}(\underline{m})$, with $\frac{a}{b} > 0$ (wlog), have:

$\Phi_{\underline{m}}((\frac{a}{b})\mathbb{Z}) = [a][b]^{-1} \in (\mathbb{Z}/m\mathbb{Z})^{\times}$.

Exercise: Verify this, show $\Phi_{\underline{m}}$ surjective. & find kernel.

DEF 13] $P_K(\underline{m}) \leq I_K(\underline{m})$ subgroup generated by:

$\{(\alpha) : \alpha \in \mathcal{O}_K,\ \alpha \equiv 1 \bmod \underline{m}_0$ & $\sigma(\alpha) > 0\ \forall \sigma \mid \underline{m}_\infty\}$.

(σ real infinite prime)

Note: $(\alpha \equiv 1 \bmod m_0) \Leftrightarrow (v_{\mathfrak{p}}(\alpha - 1) \geq v_{\mathfrak{p}}(\underline{m}_0))$

where $v_{\mathfrak{p}}(\alpha) = v_{\mathfrak{p}}(\alpha \mathcal{O}_K)\ \forall \alpha \in \mathcal{O}_K$)

$P_K(\underline{m})$ called: Ray group for $\underline{m}$.

Example] Again, $K = \mathbb{Q}$, $L = \mathbb{Q}(\zeta_m)$. $\underline{m} = (m)$.

$\Rightarrow P_{\mathbb{Q}}(\underline{m}) = \{(\frac{a}{b})\mathbb{Z} \in I_{\mathbb{Q}}(\underline{m}) : a \equiv b \bmod m\}$.

Note: $I_{\mathbb{Q}}(\underline{m}) = I_{\mathbb{Q}}(\underline{m}_0)$, but not true for P_K!

Suppose $\underline{m} = (m)\infty$ (infinite prime of $\mathbb{Q}$).

$\Rightarrow P_{\mathbb{Q}}(\underline{m}) = \{(\frac{a}{b})\mathbb{Z} \in I_{\mathbb{Q}}(\underline{m}) : a \equiv b \bmod m$ & $a/b > 0\}$.

& $\frac{I_{\mathbb{Q}}((m))}{P_{\mathbb{Q}}((m))} \cong (\mathbb{Z}/m\mathbb{Z})^{\times} / \{\pm 1\}$

& $\frac{I_{\mathbb{Q}}((m)\infty)}{P_{\mathbb{Q}}((m)\infty)} \cong (\mathbb{Z}/m\mathbb{Z})^{\times}$.

In general, $P_K(\mathfrak{m})$ has finite idx in $I_K(\mathfrak{m})$.

DEF 14) $I_K(\mathfrak{m})/P_K(\mathfrak{m}) =$ Ray class group for $\mathfrak{m}$.

Goal: show this is finite.

Recall by Ostrowski's Theorem: any nontrivial abs val is equivalent to: $|\cdot|_\mathfrak{p}$ for $\mathfrak{p} \subseteq \mathcal{O}_K$ prime ideal, or $|\cdot|_\sigma$ for $\sigma: K \hookrightarrow \mathbb{C}$.

[where, $|x|_\sigma = |\sigma(x)|$, complex modulus.]

[& $|x|_\mathfrak{p} = \begin{cases} 0 & \text{if } x=0 \\ c^{v_\mathfrak{p}(x)} & \text{if } x \neq 0 \end{cases}$ for $c \in (0,1)$, e.g. $c = \frac{1}{p}$]

~~DEF #~~ **Theorem 15** (Approximation Theorem) (Local fields)

Let: $|\cdot|_1, \dots, |\cdot|_n$ nontrivial & pairwise inequiv abs vals on K.

& $\beta_1, \dots, \beta_n \in K^*$. For any $\varepsilon > 0$, $\exists \alpha \in K$, s.t.

$|\alpha - \beta_i|_i < \varepsilon \quad \forall 1 \leq i \leq n$.

Consequence: $\mathfrak{p}$ infinite prime (real), corresponding to $\sigma: K \hookrightarrow \mathbb{R}$. Then, if $\alpha\beta \neq 0$ & $|\alpha - \beta|_\mathfrak{p} < \varepsilon$, then $\sigma(\frac{\alpha}{\beta}) > 0$.

& If $\mathfrak{p}$ finite prime, then: $|\alpha - \beta|_\mathfrak{p} < \varepsilon \iff \left|\frac{\alpha}{\beta} - 1\right|_\mathfrak{p} < \frac{\varepsilon}{|\beta|_\mathfrak{p}} \equiv \varepsilon'$.

In particular, $\forall n$, if $\varepsilon' < c^n$, then $v_\mathfrak{p}(\frac{\alpha}{\beta} - 1) > n$

$\Rightarrow \alpha \equiv \beta \mod \mathfrak{p}^n$.

Remark) $I \subseteq \mathcal{O}_K$ any ideal. Then, any class in $Cl(K)$ has a representative coprime to I.

Def 16 Let $P_{\underline{m}} \subseteq I_K(\underline{m})$ be subgroup of principal fractional ideals coprime to $\underline{m}$.

Prop 17 Let $P_{\underline{m}}$ as above. Then, have exact sequences:

$$0 \longrightarrow P_{\underline{m}} \longrightarrow I_K(\underline{m}) \longrightarrow Cl_K(\mathcal{O}_K) \longrightarrow 0$$

& $0 \longrightarrow P_{\underline{m}}/P_K(\underline{m}) \longrightarrow I_K(\underline{m})/P_K(\underline{m}) \longrightarrow Cl(K) \longrightarrow 0$.

Proof Let $\underline{a} \in I_K(\underline{m})$ & define $I_K(\underline{m}) \xrightarrow{f} Cl(K)$

$\underline{a} \longmapsto [\underline{a}]$.

Clearly: f is group hom. Surj. (by remark) & $\ker(f) = P_{\underline{m}}$. So, gives first exact sequence.

For second: follows since f acts trivially on $P_K(\underline{m})$.

Algebraic NT: Lecture 4. 26/01/2024.

From last time: ⊛ Approximation Theorem. & Congruences.

⊛ $I_K(\underline{m}) = \{\underline{a} \in I_K : \text{coprime to } \underline{m}\}$

⊛ $P_{\underline{m}} = \{(\alpha) \in I_K : \text{coprime to } \underline{m}\}$

⊛ $P_K(\underline{m}) = \{(\alpha) \in I_K : \alpha \equiv 1 \bmod \underline{m}_0 \ \&\ \sigma(\alpha) > 0 \ \forall \sigma \mid \underline{m}_\infty\}$
(σ real inf prime.)

& Quotient $I_K(\underline{m})/P_K(\underline{m}) = $ Ray class grp.

Prop 17] $0 \to P_{\underline{m}} \to I_K(\underline{m}) \to Cl(K) \to 0$ (proved last time).

DEF 18] $\underline{m}$ modulus. $K_{\underline{m}} = \{\alpha \in K^\times : (\alpha) \in I_K(\underline{m})\}$.

& $K_{\underline{m},1} = \{\alpha \in K^\times : \alpha \equiv 1 \bmod \underline{m}_0 \ \&\ \sigma(\alpha) > 0 \ \forall \sigma \mid \underline{m}_\infty\}$.

$\Rightarrow P_K(\underline{m}) = \{(\alpha) : \in I_K(\underline{m}) : \alpha \in K_{\underline{m},1}\}$ by def.

Prop 19] Ray class group $I_K(\underline{m})/P_K(\underline{m})$ is finite, with size $h_K(\underline{m}) = \dfrac{h_K \cdot \varphi(\underline{m})}{[O_K^\times : (O_K^\times \cap K_{\underline{m},1})]}$

where: h_K = Class number of K

& $\varphi(\underline{m}) = \varphi(\underline{m}_0)\,\varphi(\underline{m}_\infty)$

where: $\varphi(\underline{m}_0) = |(O_K/\underline{m}_0)^\times| = N(\underline{m}_0) \prod_{\mathfrak{p} \mid \underline{m}_0} (1 - N(\mathfrak{p})^{-1})$

& $\varphi(\underline{m}_\infty) = 2^{\#}$ of Real infinite primes dividing $\underline{m}_\infty$.

Proof] Step 1: Show $P_{\underline{m}}/P_K(\underline{m}) \cong K_{\underline{m}}/O_K^\times K_{\underline{m},1}$.

Proof of Step 1: Consider $K_{\underline{m}} \longrightarrow P_{\underline{m}} / P_K(\underline{m})$

$\Rightarrow$ This is surjective. $\alpha \longmapsto (\alpha) P_K(\underline{m})$.

Kernel: $\{\alpha \in K_{\underline{m}} : (\alpha) \in P_K(\underline{m})\}$.

$= \{\alpha \in K_{\underline{m}} : \exists \beta \in K_{\underline{m},1}, \text{ with } \underbrace{(\alpha) = (\beta)}_{\beta = \alpha\varepsilon, \text{ some } \varepsilon \in \mathcal{O}_K^\times}\}$

$= \mathcal{O}_K^\times K_{\underline{m},1}$. ✓

Step 2: $K_{\underline{m}} / K_{\underline{m},1} \cong \{\pm 1\}^{\#\underline{m}_\infty} \times (\mathcal{O}_K / \underline{m}_0)^\times$

Proof of Step 2: $\forall \alpha \in K_{\underline{m}}$ write $\alpha = a/b$, where: $a, b \in \mathcal{O}_K$ coprime & (a), (b) coprime to $\underline{m}_0$.

Denote $\bar{a} = a + \underline{m}_0$ & $\bar{b} = b + \underline{m}_0$ images in $\mathcal{O}_K / \underline{m}_0$.

& Consider map $K_{\underline{m}} \longrightarrow \left(\prod_{\sigma \in \underline{m}_\infty} \{\pm 1\}\right) \times (\mathcal{O}_K / \underline{m}_0)^\times$

$$\alpha \longmapsto \left(\prod_{\sigma \in \underline{m}_\infty} \operatorname{sgn} \sigma(\alpha)\right) \times \bar{\alpha} \quad \leftarrow = \bar{a}\bar{b}^{-1}.$$

Then, this map surjective (Approximation Theorem)

& Has: kernel $\{\alpha \in K_{\underline{m}} : \sigma(\alpha) > 0 \ \forall \sigma | \underline{m}_\infty\} = K_{\underline{m},1}$.

& $\alpha \equiv 1 \bmod \underline{m}_0$

Step 3: $\mathcal{O}_K^\times K_{\underline{m},1} / K_{\underline{m},1} \cong \mathcal{O}_K^\times / (\mathcal{O}_K^\times \cap K_{\underline{m},1})$

(2nd isomorphism theorem).

All together: $I_K(\underline{m}) / P_K(\underline{m}) \cong (I_K(\underline{m}) / P_{\underline{m}}) / (P_{\underline{m}} / P_K(\underline{m}))$

~~and~~: $P_{\underline{m}} / P_K(\underline{m}) \cong K_{\underline{m}} / \mathcal{O}_K^\times K_{\underline{m},1}$

$\cong (K_{\underline{m}} / K_{\underline{m},1}) / (\mathcal{O}_K^\times K_{\underline{m},1} / K_{\underline{m},1})$

$\cong$ " " $/ (\mathcal{O}_K^\times / \mathcal{O}_K^\times \cap K_{\underline{m},1})$

& $I_K(\underline{m}) / P_{\underline{m}} \cong Cl(K)$ (Prop 17).

$\Rightarrow [I_K(\underline{m}) : P_K(\underline{m})] = [I_K(\underline{m}) : P_{\underline{m}}][P_{\underline{m}} : P_K(\underline{m})]$

$= |Cl(K)| \cdot \dfrac{[K_{\underline{m}} : K_{\underline{m},1}]}{[\mathcal{O}_K^\times : (\mathcal{O}_K^\times \cap K_{\underline{m},1})]}$

$= \dfrac{h_K \varphi(\underline{m})}{[\mathcal{O}_K^\times : (\mathcal{O}_K^\times \cap K_{\underline{m},1})]}$ ✓

Next]: Consider more general class groups: i.e. $I_K(\underline{m})/H$ where $P_K(\underline{m}) \subseteq H$.

DEF 20] A subgroup $H \subseteq I_K(\underline{m})$ is: Congruence subgroup for $\underline{m}$, if: $P_K(\underline{m}) \subseteq H \subseteq I_K(\underline{m})$.

Motivation: For "suitably chosen" moduli $\underline{m}$, the congruence subgroups are: Kernel of $\Phi_{Cl_K, \underline{m}}$.

DEF 21] H congruence subgroup for $\underline{m}$. The quotient $I_K(\underline{m})/H$ is: Generalised ideal Class group for $\underline{m}$.

Remark] Recall: for $K = \mathbb{Q}$, $\underline{m} = (m)\infty$, saw that: $I_K(\underline{m}) / P_K(\underline{m}) \cong (\mathbb{Z}/m\mathbb{Z})^\times$.

& $(\mathbb{Z}/m\mathbb{Z})^* \cong Gal(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \cong I_k(\underline{m})/P_k(\underline{m})$.

$\Rightarrow$ Artin map $\ker(\Phi_{\underline{m}}) = P_k(\underline{m})$.

The idea of CFT is that: Generalised ideal class groups are Galois groups of Abelian extensions.

& Link between them is given by Artin map!

We will prove Artin map is surjective, although computing its kernel is much harder.

For L/k Abelian, want to know: for which moduli $\underline{m}$ is $\ker(\Phi_{\underline{m}})$ a congruence subgroup.

Lemma 22 L/k Abelian ext, $\underline{m}$ modulus, divisible by All ramified primes of k.

If $\underline{n}$ another modulus s.t. $\underline{m} \mid \underline{n}$, then: $P_k(\underline{m}) \subseteq \ker(\Phi_{\underline{m}})$

$\Downarrow$

$P_k(\underline{n}) \subseteq \ker(\Phi_{\underline{n}})$.

Proof If $\underline{m} \mid \underline{n}$: $\Rightarrow I_k(\underline{n}) \subseteq I_k(\underline{m})$.

$\Rightarrow \Phi_{\underline{n}} : I_k(\underline{n}) \longrightarrow Gal(L/k)$ is well-defined, and

$\Phi_{\underline{n}} = \Phi_{\underline{m}}|_{I_k(\underline{n})}$. So, $\ker(\Phi_{\underline{n}}) = \ker(\Phi_{\underline{m}}) \cap I_k(\underline{n})$.

Also: if $\underline{m} \mid \underline{n}$, then $P_k(\underline{n}) \subseteq P_k(\underline{m}) \subseteq \ker(\Phi_{\underline{m}})$.

$\Rightarrow P_k(\underline{n}) \subseteq P_k(\underline{m}) \cap I_k(\underline{n}) \subseteq \ker(\Phi_{\underline{m}}) \cap I_k(\underline{n})$

In above situation, if $\ker(\Phi_{\underline{m}})$ is Congruence subgroup, then: $\ker(\Phi_{\underline{n}})$ is for $\underline{n}$. $= \ker(\Phi_{\underline{n}})$ ✓

Algebraic NT: Lecture 5 — 29/01/2024

From last time:

- Congruence subgroups $[P_K(\mathfrak{m}) \subseteq \ker(\Phi_{L/K,\mathfrak{m}})]$
- Generalised ideal class groups
- Proved: $I_K(\mathfrak{m})/P_K(\mathfrak{m})$ finite.

Statements of global Class Field Theory.

Interested in: Given L/K, (Abelian ext), for which $\mathfrak{m}$ is $\ker(\Phi_{L/K,\mathfrak{m}})$ a Congruence subgroup?

Theorem 23 (The Conductor Theorem).

Let: L/K Abelian ext. There is a modulus $\mathfrak{f} = \mathfrak{f}(L/K)$ s.t.

- A prime of K (finite/infinite) ramifies in $L \iff$ it divides $\mathfrak{f}(L/K)$
- If $\mathfrak{m}$ is divisible by all primes that ramify, then $\ker(\Phi_{L/K,\mathfrak{m}})$ is a congruence subgroup $\iff \mathfrak{f}_{L/K} \mid \mathfrak{m}$.

DEF 24 $\mathfrak{f}_{L/K}$ is uniquely determined by L/K (for $\mathfrak{m}$) & called Conductor.

Example $L = \mathbb{Q}(\sqrt{N})$, $K = \mathbb{Q}$. $\mathfrak{f}_{L/K} = \begin{cases} |d_{L/K}|, & N>0 \\ |d_{L/K}|\infty, & N<0 \end{cases}$

(∞ = unique real infinite prime of $\mathbb{Q}$).

Remark $\mathfrak{f}_{L/K}$ is NOT product of ramified primes (in general).

In exercises: $\exists\, L/\mathbb{Q}$ cubic ext, ramified only at 3.

But, if $\mathfrak{m} \in \{(3), (3)\infty\}$ then $\ker(\Phi_{L/K,\mathfrak{m}})$ NOT Congruence subgroup. So, by Conductor Thm, $\mathfrak{f}_{L/K} \nmid \mathfrak{m}$.

Next: fncts on Kernel.

Recall: If $\mathfrak{P} \subseteq \mathcal{O}_L$ prime ideal $\Rightarrow N_{L/K}(\mathfrak{P}) = \mathfrak{p}^{f_{\mathfrak{P}/\mathfrak{p}}}$

where $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_K$.

Notation $N_{L/K} : I_L \longrightarrow I_K$

$\underline{a} \longmapsto N_{L/K}(\underline{a})$.

[$\underline{a} = \prod \mathfrak{P}_i^{r_i}$ ~~$\mathcal{O}_{L/K}$~~

$\Rightarrow N_{L/K}(\underline{a}) = \prod N(\mathfrak{P}_i)^{r_i}$.

$= \prod (\mathfrak{p}_i^{f_{\mathfrak{P}_i/\mathfrak{p}_i}})^{r_i}$]

DEF 25) L/K Abelian ext, $\underline{m}$ modulus of K divisible by $\underline{f}_{L/K}$. Then, Norm group (Tayagi group):

$T_{L/K}(\underline{m}) = P_K(\underline{m}) \cdot N_{L/K}(I_L(\underline{m}))$. (Congruence subgroup)

~~Where: $I_K(\underline{m}) \subseteq I_K$ subgroup whose elements coprime to $\underline{m}\mathcal{O}_L$.~~

Theorem 26) (Artin Reciprocity)

L/K Abelian ext, $\underline{m}$ modulus of K divisible by all ramified primes. The map $\Phi_{L/K,\underline{m}} : I_K(\underline{m}) \longrightarrow Gal(L/K)$ is surjective. (Part 3, Theorem 12)

If furthermore $\underline{f}_{L/K} \mid \underline{m}$, then: $\ker(\Phi_{\underline{m}})$ is congruence subgroup, so: $\ker(\Phi_{L/K,\underline{m}}) = T_{L/K}(\underline{m})$

& $I_K(\underline{m}) / T_{L/K}(\underline{m}) \cong Gal(L/K)$. (Part 3, Prop 19)

$\Rightarrow Gal(L/K)$ is: Generalised ideal class group for $\underline{m}$.

Artin reciprocity gives: useful info about decomp of primes.

Theorem 27) (Decomposition Law)

L/K abelian ext, $[L:K] = n$. & $\mathfrak{p} \subseteq \mathcal{O}_K$ un-ram prime ideal.

& $\underline{m}$ divisible by $\underline{f}_{L/K}$, but not $\mathfrak{p}$.

Denote $H = \ker(\Phi_{\mathfrak{m}})$ Congruence subgroup of $\mathfrak{m}$.

Let: f smallest positive integer s.t. $\mathfrak{p}^f \in H$ ~~(i.e. Order of $\mathfrak{p}$~~

(i.e. Order of $\mathfrak{p}+H$ in $I_K(\mathfrak{m})/H$).

Then: $\mathfrak{p}$ decomposes in L: $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1 \cdots \mathfrak{P}_g$, $g = n/f$

& $\mathfrak{P}_i$ are: distinct prime ideals of degree f over $\mathfrak{p}$.

Proof | Let $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1 \cdots \mathfrak{P}_g$ prime decomp. ($\mathfrak{P}_i$ distinct, since assumed $\mathfrak{p}$ unramified in L.)

Abelian ext $\Rightarrow$ Each $\mathfrak{P}_i$ has same residue field degree $f_{\mathfrak{P}_i/K}$.

& Know: $f_{\mathfrak{P}_i/\mathfrak{p}} = \text{Order of } \left(\frac{L/K}{\mathfrak{p}}\right)$

$\Rightarrow$ By isomorphism $I_K(\mathfrak{m})/H \cong Gal(L/K)$, $f_{\mathfrak{P}_i/\mathfrak{p}}$ must also be order of $\mathfrak{p}+H$ in $I_K(\mathfrak{m})/H$.

Result follows, since: $[L:K] = n = ef \cdot g = fg$ ✓ $f = f_{\mathfrak{P}_i/\mathfrak{p}}$.

Theorem 28 | (Existence Theorem).

Let: $\mathfrak{m}$ modulus of K & H congruence subgroup for $\mathfrak{m}$.

Then: $\exists!$ Abelian ext L/K with following properties:

- ✱ All primes of K (finite or infinite) divide $\mathfrak{m}$
- ✱ $H = T_{L/K}(\mathfrak{m})$
- ✱ $I_K(\mathfrak{m})/H \cong Gal(L/K)$ (under Artin map $\Phi_{L/K,\,\mathfrak{m}}$).

$\Rightarrow$ For K Number field: this means we can find Abelian exts, of specified ramification.

DEF 29 Let: $\underline{m}$ Any modulus (of K) & $H = P_K(\underline{m})$.

The Ray Class Field is: unique Abelian ext $K(\underline{m})/K$ with $\ker(\Phi_{K(\underline{m})/K,\ \underline{m}}) \cong P_K(\underline{m})$. (Guaranteed by Existence Theorem)

Hence: $\mathrm{Gal}(K(\underline{m})/K) \cong I_K(\underline{m})/P_K(\underline{m})$.

Example $K = \mathbb{Q}$. $\underline{m} = (m)\infty$, $m \in \mathbb{Z}$ odd or $\equiv 0 \bmod 4$.

Then: $\mathbb{Q}(\underline{m}) = \mathbb{Q}(\zeta_m)$.

If instead $\underline{m} = (m)$, then $\mathbb{Q}(\underline{m}) = \mathbb{Q}(\zeta_m + \zeta_m^{-1})$.

Next: Show that $\forall\, L/K$ Abelian ext, it is contained in some Ray class field.

Algebraic NT: lecture 6. 31/01/2024.

From last time) Conductor Theorem, Artin Reciprocity, Existence thm.

Today: Classification Theorem.

Classify: All Abelian exts, using Congruence subgroups.

& Show: Each Abelian ext in a Ray class field:

given $K, \underline{m}$: have unique $K(\underline{m})/K$ s.t. $P_K(\underline{m}) = \ker(\Phi_{K(\underline{m})/K, \underline{m}})$.

Prop 29 $M/L/K$ Abelian exts (tower of). Suppose $\underline{m}$ contains all prime ideals $\mathfrak{p} \subseteq \mathcal{O}_K$ ramifying in M.

& Write: $res: Gal(M/K) \to Gal(L/K)$ restriction map.

$\sigma \longmapsto \sigma_L$

Then: have commuting diagram:

$$\begin{array}{ccc} I_K(\underline{m}) & \xrightarrow{\Phi_{M/K,\underline{m}}} & Gal(M/K) \\ & \searrow^{\Phi_{L/K,\underline{m}}} & \downarrow res \\ & & Gal(L/K) \end{array}$$

(Proof: example sheet 1)

Lemma 30 L/K, M/K Abelian exts. Then: $L \subseteq M$ iff: $\exists \underline{m}$ modulus divisible by All primes of K ramified in either L or M, with $P_K(\underline{m}) \subseteq \ker(\Phi_{M/K,\underline{m}}) \subseteq \ker(\Phi_{L/K,\underline{m}})$.

Proof) $\Rightarrow$: If $L \subseteq M$, then: by Artin reciprocity, $\exists \underline{m}_1, \underline{m}_2$ for L/K, M/K resp. with: $P_K(\underline{m}_1) \subseteq \ker(\Phi_{L/K,\underline{m}_1})$ & $P_K(\underline{m}_2) \subseteq \ker(\Phi_{M/K,\underline{m}_2})$

By Lemma 22: $\exists \underline{m}$ modulus with:

$P_K(\underline{m}) \subseteq \ker(\Phi_{L/K,\underline{m}})$ & $P_K(\underline{m}) \subseteq \ker(\Phi_{M/K,\underline{m}})$.

& By Prop 29: $res \circ \Phi_{M/K,\underline{m}} = \Phi_{L/K,\underline{m}}$. ∎

So, follows: $P_K(m) \subseteq \ker(\Phi_{M/K,m}) \subseteq \ker(\Phi_{L/K,m})$ ✓

$\Leftarrow$: Suppose $\exists m$, $P_K(m) \subseteq \ker(\Phi_{M/K,m}) \subseteq \ker(\Phi_{L/K,m})$.

Consider: map $\Phi_{M/K,m} : I_K(m) \longrightarrow Gal(M/K)$.

The subgroup $\ker(\Phi_{M/K,m})$ is: mapped to some $H \leq Gal(M/K)$,

& by Galois correspondence: $\exists \hat{L}$, $K \subseteq \hat{L} \subseteq M$, and

~~$H \cong Gal(\hat{L}/K)$~~. $H \cong Gal(\hat{L}/K)$.

Then: Apply first part of proof, to: $\hat{L} \subseteq M$. Then, obtain

$\ker(\Phi_{L/K,m}) = \ker(\Phi_{\hat{L}/K,m})$. So, by uniqueness of existence thm.

get: $L = \hat{L}$ ✓

Corollary 31 K NF. Then: any Abelian L/K is in a Ray class field (for some m).

Proof Let m modulus of K with $\mathfrak{f}_{L/K} \mid m$. Then, $H = \ker(\Phi_{L/K,m})$ is congruence subgroup for m (by def of $\mathfrak{f}_{L/K}$ conductor).

$\Rightarrow P_K(m) \supseteq \ker(\Phi_{K(m)/K,m}) \subseteq H = \ker(\Phi_{L/K,m})$

$\Rightarrow$ By Lemma 30: $L \subseteq K(m)$ ✓

Before stating Classification Theorem: need to define an equivalence rel. on set of Congruence subgroups.

Why: ⊛ If $\ker(\Phi_m)$ Congruence subgroup for m: then

$\ker(\Phi_n)$ Congruence subgroup for n $(\forall\, m \mid n)$

□

④ If $\underline{m}, \underline{n}$ same support $\Rightarrow I_k(\underline{m}) = I_k(\underline{n})$. But, $P_k(\underline{m}), P_k(\underline{n})$ may be different.

DEF 32 Two congruence subgroups H_1, H_2 equivalent ($H_1 \sim H_2$) if $\exists \underline{m}$ modulus, with: $\boxed{I_k(\underline{m}) \cap H_1 = I_k(\underline{m}) \cap H_2.}$

& If $\underline{m}, \underline{m}'$ are 2 modulus with $P_k(\underline{n}) \subseteq \ker(\Phi_{L/k, \underline{n}})$ for $\underline{n} \in \{\underline{m}, \underline{m}'\}$, then: $\boxed{\ker(\Phi_{L/k, \underline{m}}) \sim \ker(\Phi_{L/k, \underline{m}'})}$

[since: $\ker(\Phi_{L/k, \underline{m}}) \cap I_k(\underline{m}\underline{m}') = \ker(\Phi_{L/k, \underline{m}\underline{m}'})$.]

$\Rightarrow$ The collection of such ~~#~~ congruence subgroups H (i.e. those with $\exists \underline{m}$, $H = \ker(\Phi_{L/k, \underline{m}})$) lie in a single equivalence class, denoted $H(L/k)$ for this class.

Theorem 33 (Classification Theorem).
Let: k Number Field. There is inclusion-reversing bijection:

$$\{\text{Abelian exts}\} \longleftrightarrow \{\text{Congruence subgroups}/\sim\}$$
$$L/k \longmapsto H(L/k).$$

Applications of Main Theorems:

Theorem 34 (Kronecker-Weber). If $L/\mathbb{Q}$ Abelian ext, then $\exists n \geq 1$, $L \subseteq \mathbb{Q}(\zeta_n)$.

Proof By Artin reciprocity: $\exists$ modulus $\underline{m}$, with: ~~$P_{\mathbb{Q}}(\underline{m})$~~
$P_{\mathbb{Q}}(\underline{m}) \subseteq \ker(\Phi_{L/\mathbb{Q}, \underline{m}}) \subseteq I_{\mathbb{Q}}(\underline{m})$ (e.g. $\underline{m} = \underline{f}_{L/k}$)

Any modulus of $\mathbb{Q}$ is of form: (m) or $(m)\infty$. $(m \in \mathbb{N})$

By Lemma 22: may assume $(m)\infty$. ~~$\mathbb{Q}(\zeta_m)$~~ $\mathbb{Q}(\underline{m}) = \mathbb{Q}(\zeta_m)$

$\Rightarrow P_{\mathbb{Q}}(\underline{m}) = \ker(\Phi_{\mathbb{Q}(\zeta_n)/\mathbb{Q},\, \underline{m}}) \subseteq \ker(\Phi_{L/K,\, \underline{m}})$

$\Rightarrow$ By Lemma 30: $L \subseteq \mathbb{Q}(\zeta_n)$. ✓

Remark] Also exist purely Algebraic proof of KW. Hilbert Class Field]

Given K NF, by Existence Theorem: can find Abelian ext & "control" the ramification.

For $\underline{m} = (1)$: Corresponding Abelian ext. $K(\underline{m})/K$ is: unramified for All primes (prime or infinite).

Have: $\Phi_{\underline{m}} : I_K \longrightarrow Gal(K(1)/K)$, kernel $P_K(1) = P_K$.

$\Rightarrow$ Obtain $I_K/P_K \cong Gal(K(1)/K)$.

By Existence theorem: obtain Unramified Abelian ext, with Galois group = Ideal Class group $Cl(K)$.

DEF 35] Hilbert Class ~~Group~~ Field: F is Ray class field, for modulus $\underline{m} = (1)$.

Example] $K = \mathbb{Q}$. $\Rightarrow h_K = 1$, so $K(1) = K = \mathbb{Q}$.

Algebraic NT: lecture 7 — 02/02/2024.

From last time: Classification Theorem, Kronecker Weber, & Hilbert Class Field. [Ray class field, $\underline{m} = (1)$].

Theorem 36 Hilbert class field F is: maximal unramified ext, of K.

Proof Let: M any unramified Abelian ext. By Conductor Theorem: $\mathfrak{f}_{M/K} = 1$ & For $\underline{m} = (1)$, $P_K(\mathfrak{f}_{M/K}) = P_K(\underline{m})$

$P_K(\mathfrak{f}_{M/K}) = P_K(\underline{m}) = \ker(\Phi_{F/K,\underline{m}}) \subseteq \ker(\Phi_{M/K,\mathfrak{f}_{M/K}})$.

(by: Conductor theorem).

$\Rightarrow$ By lemma 30: $M \subseteq F$ ✓

Class Field Theory, for Unramified Abelian exts.

Corollary 37 K NF. $\Rightarrow \exists$ 1-1 Correspondence:

Unramified ~~exts~~ Abelian exts of $K \iff$ Subgroups of $Cl(K)$

& If M/K Corresponds to $H \subseteq Cl(K)$, then: Artin map induces $Cl(K)/H \xrightarrow{\sim} Gal(M/K)$.

Proof Let F be Hilbert Class Field. $\Rightarrow Gal(F/K) \cong Cl(K)$.

By Galois correspondence: $\exists$ Inclusion-Reversing bijection

$\{F \supseteq M \supseteq K \text{ subfields}\} \longleftrightarrow \{\text{Subgroups } H \subseteq Gal(F/K)\}$.

Since each unramified ext is contained in F: First part ✓

For 2nd part: Let $H \leq Gal(F/K)$, $M = F^H = \{x \in F : \sigma(x) = x \ \forall \sigma \in H\}$

$\Rightarrow$ By Prop 29: $\Phi_{M/K,\underline{m}} : Cl(K) \longrightarrow Gal(M/K)$.

& $\Phi_{M/K,\underline{m}} = res \circ \Phi_{E/K,\underline{m}}$

$\Rightarrow \forall [a] \in H : \Phi_{M/K,\underline{m}}([a]) = 1$.

$\Rightarrow \Phi_{M/K,\underline{m}}$ induces $Cl(K)/H \cong Gal(M/K)$.

$$\begin{array}{ccc} Cl(K) & \longrightarrow & Gal(M/K) \\ & \searrow & \uparrow res. \\ & & Gal(F/K) \end{array}$$

Fact) If M_1/K, M_2/K ext of NF's. $\mathfrak{p} \subseteq \mathcal{O}_K$ un-ramified in both M_1 & M_2. Then: $\mathfrak{p}$ unram in $M_1 M_2$.

Example of Hilbert Class Field.)

Show: If $K = \mathbb{Q}(\sqrt{-5})$, then: $F = \mathbb{Q}(\sqrt{-5}, i)$.

Proof) Know: $h_K = 2 \Rightarrow |Gal(F/K)| = |Cl(K)| = 2$.

So: F is quadratic ext & Unramified.

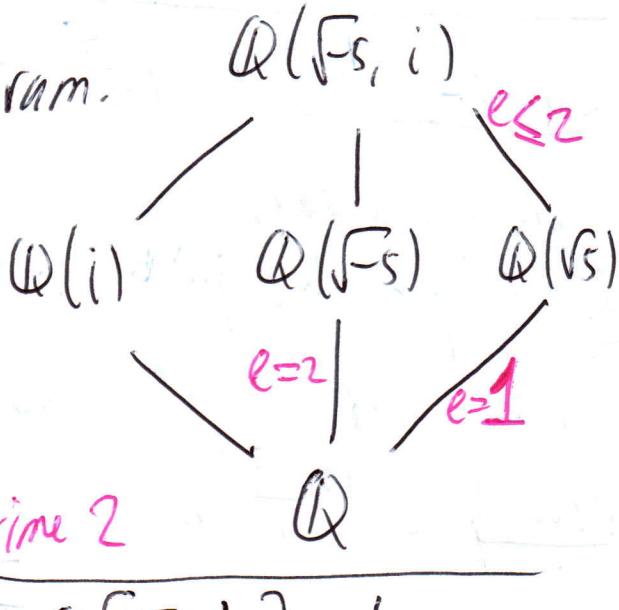
So: Need, $\mathbb{Q}(\sqrt{-5}, i)/\mathbb{Q}(\sqrt{-5})$ unram.

Fact): If $\mathfrak{P}_{M_F} \subseteq \mathcal{O}_F$, $\mathfrak{p}_M \subseteq \mathcal{O}_M$

(M any intermediate subfield),

& if $p \in K$ with $\mathfrak{P}_F | p$, $\mathfrak{P}_M | p$,

Then: $e_{\mathfrak{P}_F/p} = e_{\mathfrak{P}_F/\mathfrak{p}_M} e_{\mathfrak{p}_M/p} \leq [F:K] = 4$



Know: $Disc[\mathbb{Q}(i)/\mathbb{Q}] = 8 \Rightarrow$ Only ramified prime 2

& $Disc[\mathbb{Q}(\sqrt{5})/\mathbb{Q}] = 5 \Rightarrow$ Only ramified prime 5

$\Rightarrow$ If $p \neq 2,5$ then p unramified in $\mathbb{Q}(i)$ & $\mathbb{Q}(\sqrt{-5})$.

$\Rightarrow$ p unramified in composite $\mathbb{Q}(\sqrt{-5}, i)/\mathbb{Q}$

$\Rightarrow$ p unramified in $\mathbb{Q}(\sqrt{-5}, i)/\mathbb{Q}(\sqrt{-5})$.

Notice: $d_{K/\mathbb{Q}} = -20$ $\Rightarrow$ Only ram primes 2, 5.

Suppose 2 ramified in $\mathbb{Q}(\sqrt{-5}, i)/\mathbb{Q}(\sqrt{-5})$ $\Rightarrow e_{\mathfrak{P}_2/\mathfrak{p}_2} = 2$

(Since: $\mathfrak{p}_2$ is ideal in $\mathbb{Q}(\sqrt{-5})$, with $\mathfrak{p}_2 | 2$) ($\mathfrak{P}_2 \subseteq \mathcal{O}_F$)

($\mathfrak{P}_2 | \mathfrak{p}_2$)

Know: 2 unram in $\mathbb{Q}(\sqrt{5})/\mathbb{Q}$.

$\Rightarrow$ Write: $\mathfrak{q}_2$ for: some ideal in $\mathbb{Q}(\sqrt{5})$, with $\mathfrak{q}_2 | 2$.

$\Rightarrow e_{\mathfrak{P}_2|2} = e_{\mathfrak{P}_2/\mathfrak{q}_2} e_{\mathfrak{q}_2/2} = e_{\mathfrak{P}_2/\mathfrak{q}_2} \leq 2$.

(Since: $e_{\mathfrak{P}_2/\mathfrak{q}_2} \leq [F : \mathbb{Q}(\sqrt{5})] = 2$)

$\Rightarrow e_{\mathfrak{P}_2|2} \neq 4$, hence: 2 unramified in $\mathbb{Q}(\sqrt{-5}, i)/\mathbb{Q}(\sqrt{-5})$.

Similar argument for: $p = 5$.

Hence: $\mathbb{Q}(\sqrt{-5}, i)/\mathbb{Q}(\sqrt{-5})$ unram $\forall$ p (finite) prime.

In $\mathbb{Q}(\sqrt{-5})$: there is unique infinite prime, complex $\rightarrow$ Unram.

Hence: $\mathbb{Q}(\sqrt{-5}, i)$ is Hilbert Class Field of $\mathbb{Q}(\sqrt{-5})$ ✓

We can: allow ramification at real (infinite) primes.

DEF 38] The Narrow Hilbert Class Field is: maximal Abelian ext, un-ram at all FINITE primes.

Corollary 39] F Hilbert Class Field of K. Then: for $\mathfrak{p} \subseteq K$

prime ideal of K, $\mathfrak{p}$ splits completely in $F \Leftrightarrow \mathfrak{p}$ ~~prime~~ principal ideal.

Can: deduce from Decomp Law, or directly.

Proof] Know $\mathfrak{p}$ splits completely in $F \Leftrightarrow \left(\frac{F/K}{\mathfrak{p}}\right) = 1$,

and: $Cl(K) \cong Gal(F/K)$. So:

$\left(\frac{F/K}{\mathfrak{p}}\right) = 1 \Leftrightarrow (\mathfrak{p}) = [1]$ in $Cl(K) \Leftrightarrow \mathfrak{p}$ principal.

Theorem 38] (Principal Ideal Theorem).

In Hilbert Class Field F, any ideal $\mathfrak{a} \subseteq K$ becomes principal

Example] $K = \mathbb{Q}(\sqrt{-5})$. $\Rightarrow Cl(K) = \{[\mathcal{O}_K], [(2, 1+\sqrt{-5})]\}$.

$\Rightarrow$ For $F = \mathbb{Q}(\sqrt{-5}, i)$, $(2, 1+\sqrt{-5})\mathcal{O}_F = (1+i)\mathcal{O}_F$.

Reciprocity Theorems

Let: K NF, containing some ζ_n. Then: $\forall \alpha \in \mathcal{O}_K$: prime to $\mathfrak{p}$,

have: Fermat's Little Theorem. $\alpha^{N(\mathfrak{p})-1} \equiv 1 \bmod \mathfrak{p}$.

Exercise: $\mathfrak{p} \subseteq \mathcal{O}_K$ prime ideal, $\alpha \in \mathcal{O}_K$ ~~equiv~~ s.t. $n\alpha \notin \mathfrak{p}$.

Then: 1) $1, \zeta_n, \dots, \zeta_n^{n-1}$ all distinct mod $\mathfrak{p}$

2) $n \mid N(\mathfrak{p}) - 1$

3) $\alpha^{(N(\mathfrak{p})-1)/n} \equiv$ Unique nth root of unity mod $\mathfrak{p}$.

DEF 40] Unique root of unity here is called: nth power Legendre Symbol. Written: $\left(\frac{\alpha}{\mathfrak{p}}\right)_n$.

Algebraic NT: lecture 8 | 05/02/2024.

From last time: Hilbert Class field, Reciprocity theorem, and etc.

Let: K NF, containing primitive ζ_n. Let: $\alpha \in \mathcal{O}_K$ & $\mathfrak{p} \subseteq \mathcal{O}_K$ with: $n \nmid \alpha$ & $\mathfrak{p}$. Then: (we saw) $\exists!$ root of unity, congruent to $\alpha^{[N(\mathfrak{p})-1]/n}$ mod $\mathfrak{p}$.

DEF 41) Denote: $\left(\frac{\alpha}{\mathfrak{p}}\right)_n$ the root of unity mentioned above. ("Legendre Symbol").

Next: let $I \subseteq \mathcal{O}_K$ ideal, prime to both n & α. Then: denote $\left(\frac{\alpha}{I}\right)_n = \prod_{1 \le i \le r} \left(\frac{\alpha}{\mathfrak{p}_i}\right)^{e_i}$ (if $I = \prod \mathfrak{p}_i^{e_i}$)

So, if $\mathfrak{m}$ modulus containing all primes that contain $n\alpha$, then get a hom: $\left(\frac{\alpha}{\cdot}\right)_n : I_K(\mathfrak{m}) \to \mu_n$, $\mu_n = \{z^n = 1\}$.

Let: $L = k(\sqrt[n]{\alpha})$. Then: L/K is Galois ext, and: if $\sigma \in Gal(L/K)$, then: $\sigma(\sqrt[n]{\alpha}) = \zeta_n^k \sqrt[n]{\alpha}$ for some k.

$\Rightarrow$ Gives injective hom: $Gal(L/k) \hookrightarrow \mu_n$, $\sigma \mapsto \zeta_n^k$.

Exercises: 1) If $n\alpha \nmid \mathfrak{p}$ then $\mathfrak{p}$ unram in L.

2) $\left(\frac{L/k}{\mathfrak{p}}\right)(\sqrt[n]{\alpha}) = \left(\frac{\alpha}{\mathfrak{p}}\right)_n \sqrt[n]{\alpha}$.

Theorem 42 (Weak Reciprocity).

Let: K NF, containing ζ_n. & $\alpha \in \mathcal{O}_K$, $\alpha \neq 0$, $L = k(\sqrt[n]{\alpha})$. & $\mathfrak{m}$ modulus, divisible by all primes of k, contained in $n\alpha$.

Assume: ~~Φ~~ $\ker(\Phi_{L/K})$ is Congruence subgroup.

Then: $\exists$ Commutative Diagram: $I_K(\mathfrak{m}) \xrightarrow{\Phi_{L/K,\mathfrak{m}}} Gal(L/K)$

Let: G = Image of $Gal(L/K)$ in μ_n.

Then: $\left(\frac{\alpha}{\cdot}\right)_n$ induces: Surjective hom:

$\left(\frac{\alpha}{\cdot}\right)_n : I_K(\mathfrak{m})/P_K(\mathfrak{m}) \twoheadrightarrow G \subseteq \mu_n$.

Proof | Commutativity follows from (ii) in exercise before.

By assumptions: $P_K(\mathfrak{m}) \subseteq \ker(\Phi_{L/K,\mathfrak{m}}) \subseteq I_K(\mathfrak{m})$

$\Rightarrow \left(\frac{\alpha}{\cdot}\right)_n$ induces surj hom: $I_K(\mathfrak{m})/P_K(\mathfrak{m}) \twoheadrightarrow I_K(\mathfrak{m})/\ker\Phi_{L/K,\mathfrak{m}} \cong Gal(L/K)$.

$\Rightarrow$ Let: $I_K(\mathfrak{m})/P_K(\mathfrak{m}) \twoheadrightarrow G$. ✓

Strong Reciprocity: | Gives: Formula for comparing $\left(\frac{\alpha}{\cdot}\right)_n$ using Hilbert Symbols.

Can use Weak Recip. to show following:

Theorem 43. | (Quadratic Reciprocity)

Let: p, q distinct & odd primes. $\Rightarrow \left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$.

PART 2: Characters, Zeta Funcs, L-series.

Motivation: In Number Theory, many Arithmetic props are captured as Analytic objects.

Dirichlet Series.

DEF 1 Dirichlet Series is: of form $f(s) = \sum_{n \geq 1} a_n n^{-s}$, for: $a_n \in \mathbb{C}$ & $s \in \mathbb{C}$.

Lemma 2 (Abel's lemma / Summation)

If $(a_n), (b_n) \in \mathbb{C}$, then: $\sum_{N \leq n \leq M} a_n b_n = \sum_{N \leq n < M} (b_n - b_{n+1}) \sum_{N \leq k \leq n} a_k + \left(\sum_{N \leq n \leq M} a_k\right) b_M.$

Interlude: Uniform Convergence.

- A series $\sum a_n$ (of complex numbers) Converges to a, if: partial sums $\sum_{n \leq N} a_n \longrightarrow a$.
- A series $\sum a_n$ (of complex numbers) converge ~~Uniformly~~ Absolutely, if: $\sum_{n \leq N} |a_n|$ converges (real numbers).
- A sequence of complex funcs $(f_n)_{n \geq 1}$ Uniformly convergent to f in $S \subseteq \mathbb{C}$ if: $\forall \varepsilon > 0$, $\exists N$, $\forall n \geq N$, $|f_n(z) - f(z)| < \varepsilon$ $\forall z \in S$.
- A series $\sum f_n(z)$ converges if: $\forall z_0 \in S$, $\sum f_n(z_0)$ converges. & Converges Uniformly on S, if: $\left(\sum_{n \leq N} f_n(z)\right)_N$ converges uniformly on S.
- An infinite product $\prod_n a_n$ of nonzero complex numbers converge Absolutely $\Leftrightarrow$ $\sum \log(a_n)$ Absolutely convergent; in which case: $\prod_n a_n = \exp\left(\sum_n \log a_n\right)$.

Theorem 3 $\{a_n\}$ sequence of Complex numbers.
If $f(s)=\sum_n a_n n^{-s}$ converges at some $s=s_0$, then: it converges for any s with $Re(s)>Re(s_0)$, uniformly on every domain of form $\{s: Re(s)>Re(s_0) \& |Arg(s-s_0)|\leq\theta\}$ for any fixed $\theta<\pi/2$.

Proof Note: $f(s)=\sum_n n^{-s_0}\cdot a_n n^{-(s-s_0)} = \sum_n \tilde{a}_n n^{-s}$.

$\Rightarrow$ WLOG (by shifting) that $s_0=0$. $\Rightarrow \sum_n a_n$ converges.

For $\varepsilon>0$: Since $\sum a_n$ conv: pick N_0 big, s.t. $\left|\sum_{N\leq n\leq M} a_n\right|<\varepsilon$ for all $M,N>N_0$.

$\Rightarrow$ If $b_n=n^{-s}$ & $A_n=a_n$, apply Lemma to get:

$$\sum_{N\leq n\leq M} a_n\cdot n^{-s} = \sum_{N\leq n<M}\left(\sum_{N\leq k\leq n} a_n\right)\left(n^{-s}-(n-1)^{-s}\right)+\left(\sum_{N\leq n\leq M} a_n\right)M^{-s}.$$

& Know: $|e^{-cs}-e^{-ds}|\leq|s|\int_c^d e^{-t\,Re(s)}\,dt = \frac{|s|}{Re(s)}\left(e^{-cRe(s)}-e^{-dRe(s)}\right)$

& $\frac{|s|}{Re(s)}$ bounded by some B in given domain.

$\Rightarrow$ If $c=\log(n)$ & $d=\log(n+1)$ $\Rightarrow |n^{-s}-(n+1)^{-s}|$

$\leq B\left(n^{-Re(s)}-(n-1)^{-Re(s)}\right)$.

$$\Rightarrow \left|\sum_{N\leq n\leq M} a_n n^{-s}\right| \leq \sum_{N\leq n<M}\left|\sum_{N\leq k\leq n} a_n\right|\left|n^{-s}-(n+1)^{-s}\right| + \left|\sum_{N\leq k\leq M} a_n\right| M^{-s}.$$

$\leq \varepsilon(B+1)$ for N,M big enough ✓

Algebraic NT: lecture 9 | 07/02/2024.

From last time: (*) Reciprocity Theorem + Dirichlet Series.

Theorem 3 $\{a_n\}_{n\geq 1}$ Complex numbers. If $f(s) \equiv \sum_{n\geq 1} a_n \cdot n^{-s}$ converges at some $s=s_0$, then it converges for any $s\in\mathbb{C}$, with $Re(s) > Re(s_0)$.
& Converges Uniformly on $\{s\in\mathbb{C} : Re(s) > Re(s_0) \ \& \ |Arg(s-s_0)| \leq \theta\}$ for any $0 < \pi/2$.

Corollary 4 $f(s) = \sum_{n\geq 1} a_n \cdot n^{-s}$ Dirichlet series.

1) If $\{a_n\}$ bounded then $f(s)$ Converges absolutely $\forall Re(s)>1$.
2) If $f(s)$ Converges at $s=s_0$, converges Absolutely on the region $Re(s) > Re(s_0)+1$.

DEF 45 The smallest $\varepsilon > 0$ s.t. $f(s)$ converges $\forall Re(s) > \varepsilon$ is called the Abscissa of Convergence. (If it exists).

Theorem 86 Assume: $\exists C, \sigma_1 \geq 0$, s.t. $|A_n| \equiv |a_1| + \cdots + |a_n| \leq C n^{\sigma_1}$ for all n. Then: Abscissa $\varepsilon \leq \sigma_1$.

Riemann Zeta Function.

DEF 7 For $s\in\mathbb{C}$, with $Re(s)>1$, $\zeta(s) = \sum_{n\geq 1} n^{-s}$.

By Theorem 6: $\varepsilon_a = 1$, so: converges $\forall Re(s) > 1$.

Continue $\zeta(s)$ to the region $Re(s) > 0$.

Recall: if $f: U \to \mathbb{C}$ Complex analytic function. Then:

$\forall z_0 \in U$, $f(z) = \sum_{n \geq 0} a_n (z - z_0)^n$ is locally a power series.
This is: equivalent to: the function being Holomorphic.
A function is Meromorphic on $U \subseteq \mathbb{C}$ (open) if: $\exists A \subseteq U$ discrete set ("Poles") with $f: U \setminus A \to \mathbb{C}$ Holomorphic.
If $a \in A$ pole of f, then a is zero of $1/f$.
& $\exists n \geq 1$, with: $(z-a)^n f(z)$ Holomorphic in some $B(a, \varepsilon)$, which is nonzero here. Call: n = Order of pole of f at a.
If $n=1$, call a "Simple pole". & Argument Principle:
$\operatorname{Res}(f, a) = \lim_{z \to a} (z-a) f(z)$.

If f Mero/Holo on $U \subseteq \mathbb{C}$ & $U \subseteq V \subseteq \mathbb{C}$ also open, then: a function $F: V \to \mathbb{C}$ Mero/Holo, with $F|_U = f$, is a meromorphic/Holomorphic continuation of f.

Theorem 8 $\zeta(s)$ has Meromorphic cont. to $\operatorname{Re}(s) > 0$, with a simple pole at $s=1$ (Residue 1), and no other poles.

Proof For $s > 1$ real: $\frac{1}{s-1} \leq \int_1^\infty x^{-s}\, dx \leq \zeta(s) \leq 1 + \frac{1}{s-1}$.
$\Rightarrow 1 \leq (s-1)\zeta(s) \leq s$. So, as $s \to 1$, $(s-1)\zeta(s) \to 1$.
Hence: continuation of $\zeta(s)$ to $\operatorname{Re}(s) > 0$ has simple pole @ $s=1$ of residue 1.
For continuation: consider "Alternating" Zeta function series:

$$\zeta_2(s) \equiv \sum_{n\geq 1} (-1)^{n+1} n^{-s} = 1 - 2^{-s} + 3^{-s} - 4^{-s} + \cdots$$

Since coeffs 1 or -1: bounded $\overset{6}{\Rightarrow}$ Converges $\forall \mathrm{Re}(s) > 1$.

Note: $\frac{2}{2^s}\zeta(s) + \zeta_2(s) = \zeta(s)$. $\Rightarrow \zeta(s) = \zeta_2(s)\left(1 - \frac{1}{2^{s-1}}\right)^{-1}$

$\Rightarrow$ This gives an analytic cont. to $\mathrm{Re}(s) > 0$.

To show no other poles: note any pole not $s=1$ must satisfy

$$1 - 2^{-(s-1)} = 0 \iff \left(\exists n,\ s = \frac{2\pi i n}{\log(2)} + 1\right)$$

For $r \geq 2$, denote: $\zeta_r(s) \equiv \frac{1}{1^s} + \frac{1}{2^s} + \cdots + \frac{1}{(r-1)^s} - \frac{r-1}{r^s} + \frac{1}{(r+1)^s} + \cdots$

(so, e.g. $\zeta_3(s) = \sum_{n\geq 0}\left(\frac{1}{(3n+1)^s} + \frac{1}{(3n+2)^s} - \frac{2}{(3n+3)^s}\right)$)

Since partial sums of coeffs are bounded, (e.g. by r), know by Theorem 6 that $\zeta_r(s)$ converges $\forall \mathrm{Re}(s) > 0$.

& $\zeta(s) = \frac{\zeta_r(s)}{1 - r^{-(s-1)}}$ Similar to logic for $r=2$.

$\Rightarrow$ For $r \geq 3$, only poles occur at: $3^{s-1} = 1 \iff s = \frac{2\pi i m}{\log(3)} + 1$

So, need $\exists n, m$ with $2^n = 3^m \iff m = n = 0$ ✓

Theorem 9 $\{a_n\}_{n\geq 1}$ $(a_n \in \mathbb{C})$, $A_n \equiv a_1 + \cdots + a_n$.

Suppose $0 \leq \sigma_1 \leq 1$ & $\exists z_0 \in \mathbb{C}$, s.t. for some $C > 0$, have $|A_n - n z_0| \leq C n^{\sigma_1}$ $\forall n \in \mathbb{N}$. Then: $f(s)$ has Analytic cont. to the region $\mathrm{Re}(s) > \sigma_1$, and is analytic except for a simple pole @ $s=1$ of residue z_0.

Proof Consider $f(s) - z_0 g(s)$. Then, follows from theorem 9 + 8.

Prop. 10 $g(s) = \prod_p (1-p^{-s})^{-1}$

Proof Denote $E(s)$ for RHS. Then, $\log E(s) = \sum_p -\log(1-p^{-s})$

$$\Rightarrow \log E(s) = \sum_p \sum_{n\geq 1} \frac{1}{n p^{ns}}.$$

If $\mathrm{Re}(s) > 1+\delta$, for some $\delta > 0$, then: $|p^{ns}| = p^{n\,\mathrm{Re}(s)} \geq p^{(1+\delta)n}$

$$\Rightarrow \sum_p \sum_n \left(\frac{1}{p^{1+\delta}}\right)^n = \sum_p \frac{1}{p^{1+\delta}-1} \leq 2\sum_p \frac{1}{p^{1+\delta}} < \infty.$$

$\Rightarrow$ The series $\log(E)$ converges absolutely on $\mathrm{Re}(s) > 1+\delta$.

To show equality: for $N \in \mathbb{N}$ Fixed: choose the list $\{p_1, \dots p_n\}$ of prime numbers $\leq N$.

Then: $\prod_{p\leq N} \frac{1}{1-p^{-s}} = \sum_k{}' \frac{1}{k^s}$ where k ranges across all primes divisible only by p_i.

$\Rightarrow$ This list contains all numbers $\leq N$ (in particular)

Then, $\prod_{p\leq N} (1-p^{-s})^{-1} = \sum_{n\leq N} \frac{1}{n^s} + \sum_{n>N}{}' \frac{1}{n^s}$.

$$\Rightarrow \left| \prod_{p\leq N} (1-p^{-s})^{-1} - \sum_{n\geq 1} n^{-s} \right| \leq \left| \sum_{n\geq N}{}' n^{-s} \right| \leq \sum_{n>N} n^{1+\delta} \longrightarrow 0.$$

So indeed it converges to $g(s)$ ✓

Algebraic NT: lecture 10 | 09/02/2024.

Remark) If Dirichlet series convergent on some half-plane $\mathrm{Re}(s) > \sigma_0$, then: defines Analytic function on this half-plane. [Follows from Theorem 3].

Let: $\zeta(s) = \sum_n n^{-s} = \prod_p (1-p^{-s})^{-1}$.

DEF 11] Gamma Function $\Gamma(s) = \int_0^\infty e^{-y} y^{-s} \frac{dy}{y}$ $\forall\, \mathrm{Re}(s) > 0$.

Prop 12] 1) $\Gamma(s)$ Analytic on $\mathrm{Re}(s) > 0$ & Continues to $\mathbb{C}$

2) $\Gamma(s)$ nowhere 0 & Simple poles at $n = 0, -1, -2, \ldots$ with residue $\frac{(-1)^n}{n!}$

3) Functional Equations: $\Gamma(s+1) = s\Gamma(s)$ & $\Gamma(s)\Gamma(s+1) = \frac{s}{\sin \pi s}$ & $\Gamma(s)\Gamma\left(\frac{s+1}{2}\right) = \frac{2\sqrt{\pi}}{2^{2s}} \Gamma(2s)$

4) Special values $\Gamma(n+1) = n!$ $\forall n \geq 0$, $\Gamma(1) = 1$ & $\Gamma(\frac{1}{2}) = \sqrt{\pi}$.

Use: $\Gamma(s)$ to compute $\zeta(s)$.

Substitute: $y \mapsto \pi n^2 y$. So, $\pi^{-s}\Gamma(s) n^{-2s} = \int_0^\infty e^{-\pi n^2 y} y^s \frac{dy}{y}$

Sum $\forall n \in \mathbb{N} \Rightarrow \pi^{-s}\Gamma(s)\zeta(2s) = \int_0^\infty \sum_n e^{-\pi n^2 y} y^s \frac{dy}{y}$.

[Note: Can swap $\int, \sum$ since:

$\sum_n \int_0^\infty \left| e^{-\pi n^2 y} y^s \right| \frac{dy}{y} = \sum_n \int_0^\infty e^{-\pi n^2 y} y^{\mathrm{Re}(s)} \frac{dy}{y}$

$= \pi^{-\mathrm{Re}(s)} \Gamma(\mathrm{Re}(s)) \zeta(2\mathrm{Re}(s)) < \infty.$] ∎

DEF 13] $Z(s) \equiv \pi^{-s/2}\,\Gamma\left(\frac{s}{2}\right)\zeta(s)$ = Completed Zeta func.

DEF 14] $\theta(z) = \sum_{n\in\mathbb{Z}} e^{\pi n^2 z}$ Jacobi Theta Function.

Prop 15] $\theta(z)$ Analytic on $\mathbb{H} = \{z\in\mathbb{C} : \mathrm{Im}(z) > 0\}$.
& Satisfies: $\theta(-1/z) = \sqrt{z/i}\,\theta(z)$ for $\sqrt{z/i} = e^{\frac{1}{2}\mathrm{Log}\left(\frac{z}{i}\right)}$.

Prop 16] $Z(s) = \frac{1}{2}\int_0^\infty (\theta(iy)-1)\,y^{s/2}\,\frac{dy}{y}$

Prof Follows from def & $\theta(z) = 1 + 2\sum_{n\geq 1} e^{-\pi n^2 z}$.

DEF 17] $f: \mathbb{R}_+^\times \to \mathbb{C}$ Continuous ($\mathbb{R}_+^\times$ = group of positive reals)
$\Rightarrow$ Mellin Transform $M(f,s) = \int_0^\infty (f(y)-f(\infty))\,y^s\,\frac{dy}{y}$
(provided limit $f(\infty) = \lim_{y\to\infty} f(y)$ & Integral exists)

Theorem 18] (Mellin Principle).
Let $f, g : \mathbb{R}_+ \to \mathbb{C}$ continuous, with: $f(y) = a_0 + O(e^{-c_0 y^\alpha})$
$g(y) = b_0 + O(e^{-c_0 y^\alpha})$
(as $y\to\infty$ & $c_0, \alpha > 0$).
If $f\left(\frac{1}{y}\right) = C\cdot y^k\, g(y)$ for some real $k>0$ & $C\neq 0$, then:
1) $M(f,s)$ ~~converge~~ and $M(g,s)$ converge Absolutely & Uniformly (complex) in some compact subset of $\{\zeta\in\mathbb{C} : \mathrm{Re}(s) > k\}$.
& Admits a Holomorphic continuation to $\mathbb{C}\setminus\{0,k\}$.
2) Have simple poles @ $s=0$ and $s=k$, with residues:

$\operatorname{Res}_{s=0} M(f,s) = -a_0$, $\operatorname{Res}_{s=k} M(f,s) = c b_0$

$\operatorname{Res}_{s=0} M(g,s) = b_0$ $\operatorname{Res}_{s=k} M(g,s) = c^{-1} b_0$.

3) Have $M(f,s) = C \cdot M(f, k-s)$.

Theorem 19 $Z(s)$ admits: analytic cont. to $\mathbb{C} - \{0,1\}$.
& At these points, has simple poles @ $s = 0, 1$ with residues $-1, 1$.
& Satisfies Functional Equation $Z(s) = Z(1-s)$.

Proof By Prop 16 & Def 17: $Z(2s) = M(f,s)$, $f = \frac{1}{2\theta(iy)}$.

& $\theta(iy) = 1 + 2e^{-\pi y}\left(1 + \sum_{n \geq 2} e^{-\pi(n^2-1)y}\right)$

$\Rightarrow f(y) = \frac{1}{2} + O(e^{-\pi y})$.

By Prop 15: $f\left(\frac{1}{y}\right) = \frac{1}{2}\theta\left(\frac{-1}{iy}\right) = \frac{1}{2} y^{\frac{1}{2}} \theta(iy) = y^{\frac{1}{2}} f(y)$.

$\Rightarrow$ By Mellin principle: $M(f,s)$ has Holomorphic cont. to $\mathbb{C} - \{0, \frac{1}{2}\}$
with: simple poles at $s = 0, \frac{1}{2}$ with residues $\frac{-1}{2}, +\frac{1}{2}$.

& $M(f,s) = M(f, \frac{1}{2} - s)$.

$\Rightarrow Z(s) = M(f, \frac{s}{2})$ has Holomorphic cont to $\mathbb{C} - \{0,1\}$, with simple poles $s = 0, 1$ with residues $-1, 1$. ✓ & $Z(s) = Z(1-s)$.

Corollary 20 $\zeta(s)$ admits: analytic cont. to $\mathbb{C} \setminus \{1\}$, and: has simple pole @ $s=1$ with residue 1, and has Functional eqn:
$\zeta(1-s) = 2(2\pi)^{-s} \Gamma(s) \sin\left(\frac{\pi s}{2}\right) \zeta(s)$.

Proof $Z(s) = \pi^{-s/2}\Gamma(\frac{s}{2})\zeta(s)$ has: simple pole @ $s=0$, and so does $\Gamma(\frac{s}{2})$. So, $\zeta(s)$ has no pole @ $s=0$.

At $s=1$: $\zeta(s)$ has simple pole & $\Gamma(\frac{s}{2})$ does not.

& $\operatorname{Res}_{s=1}(\zeta(s)) = \pi^{\frac{1}{2}}\Gamma(\frac{1}{2})^{-1}\operatorname{Res}_{s=1}(Z(s)) = 1$. (Theorem 19)

Now, from FE from Theorem 19:

$$\zeta(1-s) = \pi^{\frac{1}{2}-s}\frac{\Gamma(s/2)}{\Gamma(\frac{1-s}{2})}\zeta(s) \quad \& \quad \Gamma(\tfrac{s}{2})\Gamma(\tfrac{1+s}{2}) = \frac{2\sqrt{\pi}}{2^s}\Gamma(s)$$

$$\& \quad \Gamma(\tfrac{1-s}{2})\Gamma(\tfrac{1+s}{2}) = \frac{s}{\sin(\frac{\pi s}{2})}$$

$$\Rightarrow \frac{\Gamma(s/2)}{\Gamma(\frac{1-s}{2})} = \frac{2}{2^s\sqrt{\pi}}. \quad \text{Insert} \Rightarrow \text{Get FE} \checkmark$$

Zeros of $\zeta(s)$. Know: $\zeta(s) \neq 0 \ \forall \operatorname{Re}(s) > 1$

& $\zeta(s)$ has Trivial zeros @ $s = -2, -4, -6, \ldots$ on $\operatorname{Re}(s) < 0$.

$\Rightarrow$ Any other zero lies on: Critical strip $0 \leq \operatorname{Re}(s) \leq 1$.

Riemann Hypothesis: All other zeros $\operatorname{Re}(s) = \frac{1}{2}$.

Algebraic NT: lecture 11 | 12/02/2024

From last time] Riemann ζ func, Dedekind ζ Func.

Had: $\zeta(s) = \prod_p \frac{1}{1-p^{-s}}$ (Euler Product):

Let K Number Field.

DEF 21] $\zeta_K(s) = \sum_{I \subseteq \mathcal{O}_K} N(I)^{-s}$ (I integral ideals of K, & N(I) Absolute norm)

Prop 22] $\zeta_K(s)$ converges Absolutely + Uniformly on some domain $Re(s) > 1+\delta \ \forall \delta > 0$. Also, has:

$\zeta_K(s) = \prod_{\mathfrak{p}} (1 - N(\mathfrak{p})^{-s})^{-1}$ (Euler product).

Can: Complete $\zeta_K(s)$. Denote: $Z_\infty(s) = |D_{K/\mathbb{Q}}|^{\frac{s}{2}} \pi^{-\frac{ns}{2}} \Gamma_K(\frac{s}{2})$

("Euler Product at ∞"), & Γ_K Generalised Gamma Function.

DEF 24] $Z_K(s) = Z_\infty(s)\zeta_K(s)$ Completed Zeta func.

Prop 25] $Z_K(s)$ admits: Analytic cont to $\mathbb{C} - \{0,1\}$, satisfies $Z_K(s) = Z_K(1-s)$ & Simple poles @ s=0,1 with Residues: $\frac{-2^r h_K R}{\omega}$, $\frac{2^r h_K R}{\omega}$

Where: r = # Real Infinite primes
h_K = class number
ω = # Roots of unity in K,
R = Regulator.

Corollary 25 i) $\zeta_K(s)$ has Analytic cont to $\mathbb{C} - \{1\}$

ii) @ $s=1$, Simple pole & $\operatorname{Res}_{s=1} \zeta_K(s) = \dfrac{2^{r_1}(2\pi)^{r_2} h_K R}{w |d_{K/\mathbb{Q}}|^{1/2}}$

Where r_1, r_2 = # Real inf primes, # Complex inf primes.

iii) $\exists$ Functional Equation $\zeta_K(1-s) = A(s)\zeta_K(s)$.

Remark $\operatorname{Res}_{s=1} \zeta_K(s)$ formula is: Analytic Class Number Formula.

Let: $K = \dfrac{2^{r_1}(2\pi)^{r_2} R}{w\sqrt{|d_K|}} \Rightarrow \operatorname{Res}_{s=1} \zeta_K(s) = K \cdot h_K$.

Let: $K = \mathbb{Q}(\sqrt{N})$, $N \neq 0,1$ Square-free.

$$\Rightarrow \zeta_K(s) = \prod_p \left(1 - \frac{1}{N(p)}\right)^{-1} = \prod_{p \text{ split}} \left(1 - \frac{1}{p^s}\right)^{-2} \prod_{p \text{ inert}} \left(1 - \frac{1}{p^{2s}}\right)^{-1} \prod_{p \text{ ram}} \left(1 - \frac{1}{p^s}\right)^{-1}.$$

From this: $\zeta(s) \mid \zeta_K(s)$

& $\zeta_K(s) = \prod_p \left(1 - \frac{1}{p^s}\right)^{-1} \prod_p \left(1 - \frac{\chi(p)}{p^s}\right)^{-1}$

$$\chi(p) = \begin{cases} 1 & \text{if } p \text{ split} \\ -1 & \text{if } p \text{ inert} \\ 0 & \text{if } p \text{ ram} \end{cases}$$

[Extended Dirichlet Character.]

Let: $m \in \mathbb{N}$.

DEF 26 A Dirichlet Character mod m is: homomorph. $\chi : (\mathbb{Z}/m\mathbb{Z})^\times \longrightarrow \mathbb{C}^\times$.

It is primitive $\Leftrightarrow$ does not arise from a composition

$$(\mathbb{Z}/m\mathbb{Z})^\times \longrightarrow (\mathbb{Z}/m'\mathbb{Z})^\times \xrightarrow{\chi'} \mathbb{C}^\times$$

of a proper $m' | m$ & Character χ' mod m'.

If χ is Dirichlet Character mod $\underline{f}$ & χ primitive, say $\underline{f}$ is the Conductor of χ.

Remark] Conductor = GCD of all $m' | m$ s.t. a Dirichlet Character mod m is induced from a character mod m'.

A Dirichlet Character mod m can be extended to all of $\mathbb{Z}$ by: $\chi(n) = \begin{cases} \chi(n \bmod m) & \text{if } \gcd(n,m)=1 \\ 0 & \text{else.} \end{cases}$

Example] $\chi_K(p) = \begin{cases} 1, & p \text{ split} \\ -1, & p \text{ inert} \\ 0, & p \text{ ram.} \end{cases}$ Dirichlet Character mod d_K / $\mathbb{Q}$.

DEF 27] Principal Character / Trivial Character:

χ_0 mod m has: $\chi_0(n) = \begin{cases} 1 \text{ if } (n,m)=1 \\ 0 \text{ else.} \end{cases}$

Suppose χ_1, χ_2 are Dirichlet Characters mod m. Then, can take product $(\chi_1\chi_2)(n) = \chi_1(n)\chi_2(n)$.

$\Rightarrow$ Turns {All characters of $(\mathbb{Z}/m\mathbb{Z})^\times$} into Abelian group.

Write: $\widehat{(\mathbb{Z}/m\mathbb{Z})^\times}$.

Has: identity χ_0, and inverse $n \longmapsto \chi(n)^{-1}$.

Let: A Abelian group & $\widehat{A}$ = group of homs $\chi: A \to \mathbb{C}^\times$.
This is called: Character Group of A.

Prop 28] If A finite Abelian $\Rightarrow A \cong \widehat{A}$.

Proof] Induction on $|A|$.

Assume: A Cyclic, order m. $\Rightarrow A = \langle y \rangle$

So, $y^m = 1$, so $\chi(y)$ is m'th root of unity. $\forall \chi \in \widehat{A}$.

& Note: since A cyclic, any χ is determined by $\chi(y)$.

So, pick $\zeta \in \mathbb{C}^\times$ primitive n'th root of unity. Then: $\forall r = 0, \dots, m-1$:

the function $\chi_r(y^j) = (\zeta^r)^k$. Is: A character.

So, $\chi_r = \chi_1^r$. Hence: $\widehat{A} = \langle \chi_1 \rangle$.

But: since $\chi_1^r(y) = 1$, $\zeta^r = 1 \Rightarrow \chi_1$ has order m.

$\Rightarrow \widehat{A} \cong A$ in this case.

Next: Suppose $A = A_1 \times A_2$, with A_1, A_2 Cyclic. Then,

define $\widehat{A} \to \widehat{A_1} \times \widehat{A_2}$ by $\chi \mapsto (\chi|_{A_1}, \chi|_{A_2})$.

Has: inverse $\widehat{A_1} \times \widehat{A_2} \to \widehat{A}$ by $[(a_1, a_2) \mapsto \chi_1(a_1)\chi_2(a_2)]$

Then: it follows that $\widehat{A} \cong A$ ✓

Recall: $(\mathbb{Z}/m\mathbb{Z})^\times$ has order $\phi(m)$. So does $(\mathbb{Z}/m\mathbb{Z})^*$.

Example Let $m = 4$. $\Rightarrow \phi(m) = 2$. So, 2 characters mod 4.

So, χ_0, and: $\chi_1(n) = \begin{cases} 1 & \text{if } n \equiv 1 \bmod 4 \\ -1 & \text{if } n \equiv 3 \bmod 4 \\ 0 & \text{if } n \text{ even.} \end{cases}$

Corollary 29 If A Finite Abelian: $A \cong \widehat{\widehat{A}}$ naturally, via: $a \longmapsto (\tilde{a} : \widehat{A} \to \mathbb{C}^\times)$, $\tilde{a}(\chi)(a) = \chi(a)$.

Proposition 30 (Orthogonality Relations).

Let: A finite Abelian. & $a \in A$.

1) If $\chi \in \widehat{A}$ then $\sum_{a \in A} \chi(a) = \begin{cases} 0 & \text{if } \chi \neq \chi_0 \\ |A| & \text{if } \chi = \chi_0 \end{cases}$

2) $\sum_{\chi \in \widehat{A}} \chi(a) = \begin{cases} 0 & \text{if } a \neq 1 \\ |A| & \text{if } a = 1. \end{cases}$ "Duality".

Proof: Next time!

Algebraic NT: lecture 12 | 14/02/2024

From last time: Dedekind ζ_K, Dirichlet χ & L-series.

Prop 30 (Orthogonality Relations).

Let: A finite Abelian group & $a \in A$ fixed, $\chi \in \hat{A}$ fixed.

1) $$\sum_{a \in A} \chi(a) = \begin{cases} 0 & \text{if } \chi \neq \chi_0 \\ |A| & \text{else} \end{cases}$$

2) $$\sum_{\chi \in \hat{A}} \chi(a) = \begin{cases} 0 & \text{if } a \neq 1 \\ |A| & \text{else.} \end{cases}$$

Proof 1) Fix $\chi \in \hat{A}$, $\chi \neq \chi_0$. & Take $b \in A$ s.t. $\chi(b) \neq 1$.

$$\Rightarrow \sum_{a \in A} \chi(a) = \sum_{a \in A} \chi(ab) = \chi(b) \sum_{a \in A} \chi(a) = 0 \quad \checkmark$$

2) By Corollary 29: $\sum_{\chi \in \hat{A}} \chi(a) = \sum_{\chi \in \hat{G}} \tilde{a}(\chi)$ & use 1) ✓

Prop 31 χ Dirichlet Character mod m, $\chi \neq \chi_0$. Then:

$$\left| \sum_{n \leq X} \chi(n) \right| \leq m \quad \forall X \in \mathbb{N}.$$

Dirichlet L-series.

DEF 32 χ Dirichlet Char. The Dirichlet L-series is:

$$L(\chi, s) = \sum_{n \geq 1} \frac{\chi(n)}{n^s}.$$

Prop 33 If $\mathrm{Re}(s) > 1$, it converges Absolutely, and get an Euler product. $L(\chi, s) = \prod_p (1 - \chi(p) p^{-s})^{-1}$.

If χ non-trivial: in fact, $\forall\, L(\chi,s)$ extends to analytic function on $\mathrm{Re}(s)>0$.

Proof] First part is similar to ζ case.

Second part: Follows from: Theorem 6 & Prop 31. ✓

Write: $\forall\, L(\chi,s) = \prod_{p\nmid m} \left(1-\frac{\chi(p)}{p^s}\right)^{-1}$, for $\chi \neq \chi_0$.

$\Rightarrow$ for $\chi = \chi_0$: $L(\chi_0,s) = \prod_{p \text{ prime}} \left(1-\frac{1}{p^s}\right)^{-1}$.

Next: Try factoring $\zeta_K(s)$ in terms of these L-functions.

For now: let $K = \mathbb{Q}(\zeta_m)$.

Prop 34] ($K=\mathbb{Q}(\zeta_m)$). Let $m = \prod_p p^{v_p}$ prime fact.

For each p: denote f_p = Smallest positive integer, $p^{f_p} \equiv 1 \bmod \frac{m}{p^{v_p}}$.

Then: $p\mathcal{O}_K = (\mathfrak{p}_1 \cdots \mathfrak{p}_r)^{\phi(p^{v_p})}$, distinct $\mathfrak{p}_i$, degree f_p.

In particular, if $p\nmid m$, the order of $[p] \in (\mathbb{Z}/m\mathbb{Z})^\times$ is f_p.

Prop 35] ($K=\mathbb{Q}(\zeta_m)$). $\zeta_K(s) = \prod_{\mathfrak{p}\nmid m} (1-N(\mathfrak{p})^{-s})^{-1} \prod_{\chi\in(\mathbb{Z}/m\mathbb{Z})^\times} L(\chi,s)$.

Since $\mathrm{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/m\mathbb{Z})^\times$: $\chi \in (\mathbb{Z}/m\mathbb{Z})^\times$ can also be viewed as a character for $\mathrm{Gal}(K/\mathbb{Q})$.

Proof] Denote $p\mathcal{O}_K = (\mathfrak{p}_1 \cdots \mathfrak{p}_r)^e$ & $f = f_{\mathfrak{p}_i|p}$, so $N(\mathfrak{p}_i) = p^f$.

Have: $\zeta_K(s) = \prod_{\mathfrak{p}} (1-N(\mathfrak{p})^{-s})^{-1}$.

So, $\zeta_K(s)$ contains $\prod_{P|p} (1 - N(P)^{-s})^{-1} = (1 - p^{-fs})^{-r}$.

For fixed p: $\prod_\chi L(\chi, s)$ gives factor $\prod_\chi (1 - \frac{\chi(p)}{p^s})^{-1}$

& this is 1 if $p|m$.

Assume: $p \nmid m$. Then, $e=1$, and f = Order of $[p] \in (\mathbb{Z}/m\mathbb{Z})^\times$ (by Prop 33). So, if $G_p = \langle [p] \rangle \subseteq (\mathbb{Z}/m\mathbb{Z})^\times$, then:

know: $ef r = |(\mathbb{Z}/m\mathbb{Z})^\times| = \phi(m)$, $e=1$.

$\Rightarrow r = \frac{\phi(m)}{f}$ = ~~Order of~~ Index of $G_p \subseteq (\mathbb{Z}/m\mathbb{Z})^\times$.

There is also an isomorphism between $\hat{G_p}$ and μ_f (group of roots of unity of order f), given by: $\chi \longmapsto \chi(p)$.

$\Rightarrow$ Exact Sequence $1 \longrightarrow \hat{G}/\hat{G_p} \longrightarrow \hat{G} \longrightarrow \mu_f \longrightarrow 1$

($G = (\mathbb{Z}/m\mathbb{Z})^\times$) with $r = |\hat{G}/\hat{G_p}| = |G : G_p|$. number of pre-images of $\chi(p)$.

$\Rightarrow \prod_\chi (1 - \frac{\chi(p)}{p^s})^{-1} = \prod_{\zeta \in \mu_f} (1 - \frac{\zeta}{p^s})^{-r} = (1 - p^{fs})^{-r}$

$\Rightarrow \zeta_K(s)$ contains $\prod_{P|p} (1 - N(P)^{-s})^{-1} = (1 - p^{fs})^{-r}$.

So, $\prod_\chi L(\chi, s)$ & $\zeta_K(s)$ contain these terms. Take: all product over primes $p \nmid m$, to get the result ✓

Since $\ell(\chi_0, s) = \zeta(s) \prod_{p \nmid m} (1 - p^{-s})$: get factorisation:

$$\zeta_K(s) = \prod_{\mathfrak{p} \mid m} (1 - N(\mathfrak{p})^{-s})^{-1} \left(\zeta(s) \prod_{p \mid m} \left(1 - \frac{1}{p^s}\right) \right) \prod_{\chi \neq \chi_0} L(\chi, s)$$

Since $\zeta_K(s)$ & $\zeta(s)$ have poles @ $s=1$, get following:

Prop 36 | Any nontrivial χ has $L(\chi, 1) \neq 0$.

Theorem 37 | (Dirichlet's Prime Number Theorem)

Any Arithmetic progression $a, a+m, a+2m, \ldots$ where $\gcd(a,m)=1$ contain infinitely many prime numbers.

Proof | **Note**: $L(\chi, s) \neq 0$ for any $\mathrm{Re}(s) > 1$.

& $L(\chi, s) = \prod_p (1 - \chi(p) p^{-s})^{-1}$.

$$\Rightarrow \log(L(\chi, s)) = -\sum_p \log(1 - \chi(p) p^{-s}) = \sum_p \sum_{n \geq 1} \frac{\chi(p)^n p^{-ns}}{n}.$$

(This converges Absolutely since: $\left| \frac{\chi(p)^n}{n p^{ns}} \right| \leq \left| \frac{1}{p^{ns}} \right| = p^{-n\mathrm{Re}(s)}$

$$\Rightarrow \sum_p \sum_{n \geq 1} \left| \frac{\chi(p)^n}{n p^{ns}} \right| \leq \sum_p \sum_{n \geq 1} p^{-n\mathrm{Re}(s)} \leq \sum_{n \geq 1} n^{-\mathrm{Re}(s)} < \infty \,]$$

Hence: $$\log L(\chi, s) = \sum_p \frac{\chi(p)}{p^s} + \sum_p \sum_{n \geq 2} \frac{\chi(p)^n}{n p^{ns}}.$$

& Latter sum is absolutely convergent for $\mathrm{Re}(s) > \frac{1}{2}$.

& Takes Finite sum @ $s=1$. Denote: $\theta_\chi(s)$ this double sum.

Let: $(a,m)=1$. Then: $\sum_\chi \chi(a)^{-1} \log L(\chi, s)$

$$= \sum_\chi \chi(a^{-1}) \left(\sum_p \frac{\chi(p)}{p^s} + \theta_\chi(s) \right)$$

$$= \sum_p \frac{1}{p^s} \left(\sum_\chi \chi(pa^{-1}) \right) + \sum_\chi \chi(a^{-1}) \theta_\chi(s) = \phi(m) \sum_{p \equiv a \bmod m} p^{-s} + \text{Sum}$$

So, assuming finitely many # such primes $a \pmod m$:
this tends to finite value as $s \to 1^+$.

& know: $\ell(\chi_0, s) = \zeta(s) \prod_{p \mid m} (1 - p^{-s})$.

$\Rightarrow$ $\log \ell(\chi_0, s) \to \infty$ as $s \to 1$, since $\zeta(s)$ has a pole at $s=1$. But for $\chi \neq \chi_0$, $\ell(\chi, s)$ is defined @ $s=1$ with $\ell(\chi, 1) \neq 0$.

$\Rightarrow$ $\sum_{\chi} \chi(a^{-1}) \log L(\chi, s) \to \infty$ as $s \to 1^+$ ⚡

Hence, same is true for RHS ✓

Algebraic NT: Lecture 13. 16/02/2024

From last time: Dirichlet $L(\chi, s)$, Factor $\zeta_K(s)$, $K = \mathbb{Q}(\zeta_m)$ & Dirichlet's PNT.

Let: $K/\mathbb{Q}$ Abelian $\Rightarrow \exists m,\ K \subseteq \mathbb{Q}(\zeta_m)$.

Let: $G = \mathrm{Gal}(K/\mathbb{Q})$ & consider image in $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \cong (\mathbb{Z}/m\mathbb{Z})^\times$.

$\Rightarrow$ Can: consider characters of G as: Dirichlet characters mod m $\left(\widehat{G} \subseteq (\mathbb{Z}/m\mathbb{Z})^\times\right)$.

Prop 38 For K as above: ~~$\zeta_K(s) = \prod_{p \mid m} L(\chi, s)$~~

$$\zeta_K(s) = \prod_{p \mid m} (1 - N(\mathfrak{p})^{-s})^{-1} \prod_{\chi \in \widehat{G}} L(\chi, s). \quad (\mathrm{Re}(s) > 1).$$

Corollary 39 $$h_K = \left(\prod_{p \mid m} (1 - \tfrac{1}{p})(1 - \tfrac{1}{p^{f_p}})^{-V_p} \prod_{\chi \neq \chi_0} L(\chi, 1) \right) / K.$$

Proof Follows from: Analytic Class Number formula, and:

$L(\chi_0, s) = \zeta(s) \prod_{p \mid m} (1 - \frac{1}{p^s})$ & $\zeta(s)$ has simple pole, at $s=1$, residue 1. ✓

There are Explicit formulas for $L(\chi, 1)$, and can use to compute h_K.

In Sheet 2: Exercise, making this explicit for $K = \mathbb{Q}(\sqrt{N})$ where $N \neq 0, 1$ square-free. If $m = |d_{K/\mathbb{Q}}|$ then $K \subseteq \mathbb{Q}(\zeta_m)$.

Next: Fundamental Inequality & more general Dirichlet PNT.

Notation $f(s) \sim g(s) \iff f, g$ (functions with singularity @ $s=1$) differ by function analytic @ $s=1$.

E.g. $\zeta(s) \sim \frac{1}{s-1}$, since $\log(\zeta(s)) = \sum_p \frac{1}{p^s} + \sum_p \sum_{n \geq 2} \frac{1}{np^{ns}}$

& Only $\sum_p \frac{1}{p^s}$ contributes to singularity @ $s=1$.

Similarly: since $\log \zeta_K(s) = \sum_{\mathfrak{p} \text{ prime}} \sum_{n \geq 1} \frac{1}{n \cdot N(\mathfrak{p})^s}$:

$$\Rightarrow \log \zeta_K(s) \sim \sum_{\mathfrak{p}} N(\mathfrak{p})^{-s} \sim \sum_{\deg(\mathfrak{p})=1} N(\mathfrak{p})^{-s}.$$

[Where: $\mathfrak{p}$ degree 1 $\iff$ Residue field degree /$\mathbb{Q}$ is 1 $\iff |N(\mathfrak{p})| = 1$]

Note: $\zeta_K(s) = \sum_{C \in Cl(K)} \zeta(C, s)$ (Partial Zeta function)

Where: $\zeta(C,s) \equiv \sum_{\underline{a} \in C} N(\underline{a})^{-s}$.

Prop 40] $[K:\mathbb{Q}] = n$ (any NF) & $C \in Cl(K)$.

Then $\zeta(C,s)$ Analytic for $Re(s) > 1 - \frac{1}{n}$, except for a simple pole @ $s=1$, residue K.

This is what is needed for Analytic CNF & needs estimates for # ideals in given ideal class.

More generally: let $\underline{m}$ modulus for K. Then:

$$\zeta_K(\underline{m}, s) = \sum_{(\underline{a}, \underline{m})=1} N(\underline{a})^{-s} = \prod_{\mathfrak{p} \nmid \underline{m}} (1 - N(\mathfrak{p})^{-s})^{-1}.$$

$\square$

& $\zeta_K(\underline{m}, s) = \sum_{C \in I_K(\underline{m})/P_K(\underline{m})} \zeta(C, s)$ as before. ((class in Weyl class group)

Prop 41 $\underline{m}$ modulus of K. & $C \in I_K(\underline{m})/P_K(\underline{m})$. Then:
$\zeta(C,s)$ Analytic for $\mathrm{Re}(s) > 1 - \frac{1}{n}$ except simple pole @ $s=1$ with Residue: $\rho_{\underline{m}}$ (depending only on $\underline{m}$, not on C).

Consequently: $\zeta_K(\underline{m}, s)$ for $\mathrm{Re}(s) > 1 - \frac{1}{n}$, except simple pole @ $s=1$, residue $\rho_{\underline{m}} h_{\underline{m}}(K)$.

Note: Product for $\zeta_K(\underline{m}, s)$ differs from $\zeta_K(s)$ by factors corresponding to $\mathfrak{p} | \underline{m}$, and finitely many $\mathfrak{p}$.

$\Rightarrow$ finite product does not ~~depend on~~ affect singularity.

$\Rightarrow \log(\zeta_K(\underline{m}, s)) \sim \log(\zeta_K(s))$.

DEF 42 Generalised Dirichlet Character. (Weber Char), of modulus $\underline{m}$: is Group hom. $\chi : I_K(\underline{m})/P_K(\underline{m}) \to \mathbb{C}^\times$.

The Corresponding L-series $L_{\underline{m}}(\chi, s)$ is:

$$L_{\underline{m}}(\chi, s) = \sum_{\substack{\underline{a} \subset \mathcal{O}_K \\ (\underline{a}, \underline{m}) = 1}} \chi(\underline{a}) N(\underline{a})^{-s}.$$ "Weber L-funcs"

$$= \sum_{C \in I_{\underline{m}}(K)/P_{\underline{m}}(K)} \chi(C) \zeta(C, s).$$

Prop 43 $L_{\underline{m}}(\chi, s)$ is Analytic for $\mathrm{Re}(s) > 1 - \frac{1}{n}$ if $\chi \neq \chi_0$, and has Euler Product:

$$L_{\underline{m}}(\chi, s) = \prod_{\mathfrak{p} \nmid \underline{m}} \left(1 - \frac{\chi(\mathfrak{p})}{N(\mathfrak{p})^s}\right)^{-1}.$$

Note: $L_{\underline{m}}(\chi_0, s) = \prod_{\mathfrak{p} \nmid \underline{m}} \left(1 - \frac{1}{N(\mathfrak{p})^s}\right)^{-1} = \zeta_K(\underline{m}, s)$.

$\Rightarrow$ By Prop 41: this Analytic for $\mathrm{Re}(s) > 1 - \frac{1}{n}$, ~~and has~~ except simple pole @ $s=1$.

Recall: Norm Function. If L/K Galois, then:
$T_{L/K}(\underline{m}) = P_K(\underline{m})\, N_{L/K}(I_L(\underline{m}))$.

This ~~has~~ is: Kernel of $\Phi_{\underline{m}}$ for suitable $\underline{m}$.

Call: $[I_K(\underline{m}) : T_{L/K}(\underline{m})]$ the Norm index of.

Theorem 44 (Universal Norm Index Inequality)
L/K Galois & $\underline{m}$ divisible by all primes of K that ramify in L. Then: $[I_K(\underline{m}) : T_{L/K}(\underline{m})] \leq [L:K]$.

Proof Let $\chi \neq \chi_0$ character of: $I_K(\underline{m})/P_K(\underline{m})$. Can view it as Character of $I_K(\underline{m})/P_K(\underline{m})$. Let: $m(\chi)$ = Order of zero @ $s=1$ of $L_{\underline{m}}(\chi, s)$. By Prop 43: $m(\chi) \geq 0$.

$\Rightarrow$ write: $L_{\underline{m}}(\chi, s) = (s-1)^{m(\chi)} g(\chi, s) \Rightarrow \log L_{\underline{m}}(\chi, s) \tilde{=} -m(\chi)\frac{1}{s-1}$.

Let: $\mathrm{Re}(s) > 1$, ~~and χ any char of $I_K(\underline{m})/P_K(\underline{m})$~~

$$\Rightarrow \mathrm{Log}\, L_{\underline{m}}(\chi, s) = \sum_{\mathfrak{p} \nmid \underline{m}} \sum_{n \geq 1} \frac{\chi(\mathfrak{p})}{n \cdot N(\mathfrak{p})^{-s}} = \sum_{\mathfrak{p} \nmid \underline{m}} \frac{\chi(\mathfrak{p})}{N(\mathfrak{p})} + \sum\sum_{\mathfrak{p} \nmid \underline{m}\ n \geq 2} (\ldots)$$

Since χ trivial on $T_{L/K}(\underline{m})$: $\sum_{\chi} \chi(\mathfrak{p}) = \begin{cases} h & \text{if } \mathfrak{p} \in T_{L/K}(\underline{m}) \\ 0 & \text{else.} \end{cases}$

& ~~By Orthogonality~~: let $s \to 1$, then, $\sum_{\chi} \mathrm{Log}\, L_{\underline{m}}(\chi, s) \sim h \sum_{\mathfrak{p} \in T_{L/K}(\underline{m})} N(\mathfrak{p})^{-s}$

Algebraic NT: lecture 14) 19/02/2024

Theorem 44 [Universal norm-index Ineq].

L/K Galois, $\underline{m}$ modulus, divisible by all K-primes L-ramifying. Then: $[I_K(\underline{m}) : T_{L/K}(\underline{m})] \leq [L:K]$.

Proof (continued). Had: $\forall \chi \neq \chi_0$, $m(\chi) =$ [Order of zero @ $s=1$,] and: $\Rightarrow m(\chi) \geq 0$.

& Had: $\forall \chi \neq \chi_0$, $\operatorname{Log}(L_{\underline{m}}(\chi, s)) \sim -m(\chi) \log\left(\frac{1}{s-1}\right)$

& $\forall \chi$, had: $\operatorname{Log} L_{\underline{m}}(\chi, s) \sim \sum_{\mathfrak{p} \nmid \underline{m}} \frac{\chi(\mathfrak{p})}{N(\mathfrak{p})^s}$.

So, sum over χ, & take $s \to 1$, to get:

$$\sum_{\chi} \operatorname{Log}(L_{\underline{m}}(\chi, s)) \sim \underbrace{[I_K(\underline{m}) : T_{L/K}(\underline{m})]}_{=h} \sum_{\mathfrak{p} \in T_{L/K}(\underline{m})} N(\mathfrak{p})^{-s}$$

- For $\chi = \chi_0$: $L_{\underline{m}}(\chi, s) = \zeta_K(\underline{m}, s)$

$\Rightarrow \operatorname{Log}(L_{\underline{m}}(\chi_0, s)) \sim \operatorname{Log} \zeta_K(s) \sim \log\left(\frac{1}{s-1}\right)$, $s \to 1$

- For $\chi \neq \chi_0$, had the expansion above.

Hence: $\sum_{\chi} \operatorname{Log}(L_{\underline{m}}(\chi, s)) \sim \operatorname{Log} \zeta_K(s) + \sum_{\chi \neq \chi_0} \operatorname{Log}(L_{\underline{m}}(\chi, s))$

$$\sim \log\left(\frac{1}{s-1}\right) - \sum_{\chi \neq 1} m(\chi) \log\left(\frac{1}{s-1}\right) = \left(1 - \sum_{\chi \neq 1} m(\chi)\right) \operatorname{Log}\left(\frac{1}{s-1}\right).$$

Now, if $\mathfrak{p}$ splits completely in L, then: $\forall \mathfrak{P}|\mathfrak{p}$ with $\mathfrak{P} \subseteq \mathcal{O}_L$, have $f_{\mathfrak{P}|\mathfrak{p}} = 1$, so $N_{L/K}(\mathfrak{P}) = \mathfrak{p}$.

$\Rightarrow$ If $\mathfrak{p} \nmid \mathfrak{m}$ then $\mathfrak{p} \in T_{L/K}(\mathfrak{m}) = P_K(\mathfrak{m}) N_{L/K}(I_L(\mathfrak{m}))$.

& There are: $[L:K]$ primes $\mathfrak{P}|\mathfrak{p}$ lying over $\mathfrak{P}$.

$$\Rightarrow h \sum_{\mathfrak{p} \in T_{L/K}(\mathfrak{m})} N(\mathfrak{p})^{-s} = h \cdot \Big(\sum_{\substack{\mathfrak{p} \in T_{L/K}(\mathfrak{m}) \\ \text{split completely}}} N(\mathfrak{p})^{-s} + \sum_{\substack{\mathfrak{p} \in T_{L/K}(\mathfrak{m}) \\ f_{\mathfrak{P}|\mathfrak{p}} > 1}} N(\mathfrak{p})^{-s} \Big)$$

(Since: $\mathfrak{m}$ divisible by all ramifying primes)

The 2nd series does not contribute @ singularity $s=1$, because $N(\mathfrak{p}) \geq p^2$.

& If $\mathfrak{P} \subseteq \mathcal{O}_L$ degree 1 prime & $\mathfrak{P}|\mathfrak{p}$, then: $f_{\mathfrak{P}|\mathfrak{p}} = 1$

If $\mathfrak{p}$ unramified in L, then $\mathfrak{p}$ splits completely, with $[L:K]$ primes above $\mathfrak{p}$.

So, write: $\gtrsim$ $\equiv$ "RHS is less than or equal to LHS plus some const in some nbhood $s=1$".

$$\Rightarrow h \sum_{\mathfrak{p} \in T_{L/K}(\mathfrak{m})} N(\mathfrak{p})^{-s} \gtrsim h \sum_{\substack{\mathfrak{p} \\ \text{split completely}}} N(\mathfrak{p})^{-s} \geq \frac{h}{[L:K]} \sum_{\substack{\mathfrak{P} \subseteq \mathcal{O}_L \\ (\text{degree } 1)}} N(\mathfrak{P})^{-s}$$

$$\gtrsim \frac{h}{[L:K]} \log\left(\frac{1}{s-1}\right). \quad \text{(previous Prop)}$$

$$\Rightarrow \left(1-\sum_{\chi\neq 1} m(\chi)\right)\log\left(\frac{1}{s-1}\right) \gtrsim \frac{h}{[L:K]}\log\left(\frac{1}{s-1}\right).$$

So, must have $m(\chi)=0 \ \forall \chi\neq 1$ & $h=[I_K(\mathfrak{P}):T_{L/K}(\mathfrak{P})]$

$\leq [L:K]$ ✓

In fact: $L_{\mathfrak{m}}(\chi,1)\neq 0 \ \forall \chi\neq\chi_0$ is important for proving generalisation of Prime Number Theorem.

PART III: DENSITY THEOREMS.

Recall: Dirichlet's PNT stated: if $\gcd(a,m)=1$, then:

$$\sum_{\chi\in(\mathbb{Z}/m\mathbb{Z})^\times} \chi(a)^{-1}\operatorname{Log}(L(\chi,s)) = \phi(m)\sum_{p\not\equiv a \bmod m} p^{-s} + (\text{stuff})$$

$$\Leftrightarrow \sum_{\chi}\chi(a)^{-1}\operatorname{Log}(L(\chi,s)) \sim \phi(m)\sum_{p\equiv a \bmod m} p^{-s}.$$

$$\sim \operatorname{Log}(L(\chi_0,s)) \sim \operatorname{Log}(\zeta(s)).$$

$$\Rightarrow \sum_{p\equiv a \bmod m} p^{-s} \sim \frac{1}{\phi(m)}\log\left(\frac{1}{s-1}\right)$$

As $s\to 1^+$: this diverges, and this showed Dirichlet PNT.

$$\& \Leftarrow \lim_{s\to 1^+}\left(\frac{\sum_{p\equiv a \bmod m} p^{-s}}{\log\left(\frac{1}{s-1}\right)}\right) = \frac{1}{\phi(m)}.$$

Next: S set of primes. What is: $\lim_{s\to 1^+}\left(\frac{\sum_{p\in S} p^{-s}}{\log\left(\frac{1}{s-1}\right)}\right)$?

Does it exist? If it does, say S has Dirichlet density $\delta(S)$.

Note: If S finite, then S has Dirichlet Density 0.

$\Rightarrow$ Can "Rephrase" Dirichlet PNT, by saying that the Dirichlet Density of $\{p \text{ prime}, p \equiv a \bmod m\}$ is $\frac{1}{\phi(m)} > 0$.

Prop 1] $K/\mathbb{Q}$ Galois ext. & $S_K = \{p \in \mathbb{Z} : p \text{ split completely in } K/\mathbb{Q}\}$.

Then: $\delta(S_K) = [K:\mathbb{Q}]^{-1}$.

Proof] Know: $\text{Log}\left(\zeta_K(s)\right) \sim \log\left(\frac{1}{s-1}\right) \sim \sum_{\mathfrak{p}} N(\mathfrak{p})^{-s}$

$\sim \sum_{\mathfrak{p} \text{ split completely}} p^{-s}$ (i.e. $f_{\mathfrak{p}|\mathfrak{p}} = 1 = e_{\mathfrak{p}|\mathfrak{p}}$)

$+ \sum_{\mathfrak{p}_1 \text{ with } f_{\mathfrak{p}_1|p} > 1} p^{-s \cdot f_{\mathfrak{p}_1|p}} + \sum_{\mathfrak{p}_1 \text{ with } f_{\mathfrak{p}_1|p} \geq 1,\ e_{\mathfrak{p}_1|p} > 1} p^{-s}$

$\sim \sum_{p \in S_K} [K:\mathbb{Q}] p^{-s}$. So: $\text{Log}\left(\frac{1}{s-1}\right) \sim [K:\mathbb{Q}] \sum_{p \in S_K} p^{-s} + (\cdots)$

$\Rightarrow \delta(S_K) = \lim_{s \to 1^+} \frac{\sum_{p \in S_K} p^{-s}}{\log\left(\frac{1}{s-1}\right)} = [K:\mathbb{Q}]^{-1}$.

Let: K any number Field.

DEF 2] Let S set of prime ideals of $\mathcal{O}_K$. Then, if the limit $\lim_{s \to 1^+} \left(\frac{\sum_{\mathfrak{p} \in S} N(\mathfrak{p})^{-s}}{\log\left(\frac{1}{s-1}\right)} \right)$ exists & $= \delta$, we say that

S has Dirichlet Density $\delta = \delta(S)$.

Note: Since $\log\left(\frac{1}{s-1}\right) \sim \sum_{\mathfrak{p}} N(\mathfrak{p})^{-s}$, can also write, as:

$$\delta(S) = \lim_{s \to 1^+} \frac{\sum_{\mathfrak{p} \in S} N(\mathfrak{p})^{-s}}{\sum_{\mathfrak{p} \in \mathcal{O}_K} N(\mathfrak{p})^{-s}}.$$

Lemma 3 Let P_K be set of all prime ideals of K, and: S, T subsets of P_K. Then:

1) $\delta(P_K) = 1$
2) If $S \subseteq T$, and both $\delta(S)$, $\delta(T)$ exist then $\delta(S) \leq \delta(T)$
3) If $\delta(S)$ exists then $0 \leq \delta(S) \leq 1$
4) If S, T disjoint & $\delta(S)$, $\delta(T)$ exist then $\delta(S \cup T) = \delta(S) + \delta(T)$
5) S finite $\Rightarrow \delta(S)$ exists & $= 0$
6) If T, S differ by finitely many elements, and $\delta(S)$ exists, then: $\delta(T)$ also exists and $\delta(T) = \delta(S)$.

Lemma 4 L/k Galois, $S_{L/k} \equiv \{\mathfrak{p} \in \mathcal{O}_K : \mathfrak{p}$ splits completely in $L/k\}$.

Then: $\delta(S_{L/k}) = [L:k]^{-1}$.

Proof Exercise haha [Example sheet 3, Q2]

Lemma 5 S_1 set of prime ideals, of degree 1. Then $\delta(S_1) = 1$. If also, S = set of prime ideals of K, and $\delta(S)$ exists, then $\delta(S) = \delta(S \cap S_1)$.

Proof $\operatorname{Log}(\zeta_K(s)) \sim \sum_{\mathfrak{p}} N(\mathfrak{p})^{-s} = \sum_{\mathfrak{p} \in S_1} N(\mathfrak{p})^{-s} + \sum_{\mathfrak{p} \notin S_1} N(\mathfrak{p})^{-s}$

$\sim \sum_{\mathfrak{p} \in S_1} N(\mathfrak{p})^{-s}$, since $N(\mathfrak{p}) = p^f \geq p^2 \quad \forall \mathfrak{p} \notin S_1$. ✓

$\Rightarrow$ By def, $\delta(S_1) = 1$, and also $\delta(S) = \delta(S \cap S_1)$, because $\sum_{\mathfrak{p} \in S \setminus S_1} N(\mathfrak{p})^{-s} = 0$.

Algebraic NT: Lecture 15 | 21/02/2024

From last time: Universal Norm Index ineq & Density.

Saw: $L_{\mathfrak{m}}(\chi,1)\neq 0$ $\forall \chi$ non-trivial char of $I_K(\mathfrak{m})/T_{L/K}(\mathfrak{m})$,

where: L/K Galois & $\mathfrak{m}$ div. by all ram primes.

By Existence Theorem: $\forall K$ Number Field & $\mathfrak{m}$ modulus for K, & any Congruence subgroup $P_K(\mathfrak{m}) \subseteq H \subseteq I_K(\mathfrak{m})$, have: Abelian ext L/K s.t. $H = T_{L/K}(\mathfrak{m})$.

& In particular: this holds for $H = P_K(\mathfrak{m})$.

Theorem 6 $\mathfrak{m}$ modulus for K, $\chi \neq \chi_0$ char of $I_K(\mathfrak{m})/P_K(\mathfrak{m})$.

Then, $L_{\mathfrak{m}}(\chi,1)\neq 0$.

Corollary 7 [Generalised Dirichlet PNT]

Let: $h_K(\mathfrak{m}) = |I_K(\mathfrak{m})/P_K(\mathfrak{m})|$.

& C_0 some ideal class of $I_K(\mathfrak{m})/P_K(\mathfrak{m})$.

& S set of Prime ideals in C_0. Then: $\delta(S) = \frac{1}{h_K(\mathfrak{m})}$.

Proof For $\mathrm{Re}(s)>1$, $\log L_{\mathfrak{m}}(\chi,s) \sim \sum_{\mathfrak{p}\nmid \mathfrak{m}} \frac{\chi(\mathfrak{p})}{N(\mathfrak{p})^s}$

$$\sim \sum_{C \in I_K(\mathfrak{m})/P_K(\mathfrak{m})} \chi(C) \sum_{\mathfrak{p}\in C} N(\mathfrak{p})^{-s}.$$

Then: Multiply by $\chi(C_0^{-1})$ & Sum across all χ (including the trivial character):

$\Rightarrow \log \zeta_K(s) \sim \sum_C \sum_\chi \chi(CC_0^{-1}) \sum_{\mathfrak{p} \in C} N(\mathfrak{p})^{-s}$.

& By Orthogonality relations on χ's, know: the sum over χ is 0 unless $C \cdot C_0^{-1} = 1$.

$\Rightarrow \log\left(\frac{1}{s-1}\right) \sim h_K(m) \cdot \sum_{\mathfrak{p} \in C_0} N(\mathfrak{p})^{-s}$ ✓

Hence: any ideal class contains infinitely many primes, and are distributed equally WRT δ.

Frobenius Density Theorems.

Let: $K \subseteq E \subseteq L$ Field exts, L/K Galois (E/K not necessarily)
& $G = \mathrm{Gal}(L/K)$., $H \subseteq G$, elements of G fixing E. (element-wise)

Consider: $G = H\sigma_1 + \cdots + H\sigma_k$. Cosets.

$\Rightarrow$ Any $\sigma \in G$ permutes $H\sigma_i \mapsto H\sigma_i\sigma$ (right mult).

Call a seq. $H\sigma_i, H\sigma_i\sigma, H\sigma_i\sigma^2, \ldots, H\sigma_i\sigma_i^{t-1}$ a Cycle of length t, if all distinct & $H\sigma_i = H\sigma_i\sigma^t$.

$\Rightarrow$ Cosets of H are partitioned into cycles (of σ).

Prop 9 $K \subseteq E \subseteq L$ & L/K Galois. Let: $P \subseteq \mathcal{O}_L$, $\mathfrak{p} = P \cap \mathcal{O}_K$, and assume $\mathfrak{p}$ un-ram in L.

& Let: $\sigma = \left(\frac{L/K}{P}\right)$. Suppose: σ has cycles, length $t_1, \ldots, t_s$ when acting on cosets of $H = \mathrm{Gal}(L/E)$.

Then: $\mathfrak{p}\mathcal{O}_E = P_1 \cdots P_s$, $f_{P_i/\mathfrak{p}} = t_i$.
$P_i \subset \mathcal{O}_E$,

The number of Prime ideals in E dividing $\mathfrak{p}$ is: the number of cosets $H\sigma_i$ s.t. $\sigma_i^{-1} D_{\mathfrak{P}|\mathfrak{p}} \sigma_i^{-1} \subseteq H$.

DEF 9 L/K Galois, $G = Gal(L/K)$. $\sigma \in G$ order n. The Division of σ is set of elements of G that are conjugate to σ^m, for some m s.t. $\gcd(m,n)=1$.

Lemma 10 $\sigma \in G$, $H = \langle \sigma \rangle \subseteq G$ & t = # elements in the division. Then: $t = \phi(n)[G : N_G(H)]$

Where: ϕ = Totient func & $N_G(H) = \{g \in G : gHg^{-1} = H\}$.

Proof] Use fact that: $\forall g \in G$, # elements in conj class is exactly $[G : C_G(g)]$ centraliser.

Theorem 11 [Frobenius Density Theorem]

L/K Galois, $\sigma \in G = Gal(L/K)$. Has: t elements in division.

Let: $S = \{\mathfrak{p} \subseteq K : \exists \mathfrak{P} \in \mathcal{O}_L, \mathfrak{P}|\mathfrak{p}$ & $\left(\frac{L/K}{\mathfrak{P}}\right)$ is in division (of σ)$\}$.

Then: $\delta(S) = \frac{t}{|G|}$.

Proof] Prove by Induction on order of σ. For $n=1$, $\sigma = 1$, so $S = S_{L/K} \Rightarrow$ Follows from Lemma 4.

Assume σ non-trivial & t_d = # elements of division of σ^d, for $d|n$. & S_d = Set of primes divisible by a prime of L, whose Artin symbol is in division of σ^d.

Note: $S_1 = S$. & By induction: $\delta(S_d) = \frac{t_d}{|G|}$ $\forall d \neq 1$.

Let: $H = \langle \sigma \rangle$ & $E = L^H = \{x \in L : \sigma(x) = x \ \forall \sigma \in H\}$.

By Prop 8: a prime $\mathfrak{p} \subseteq \mathcal{O}_K$ is divisible by at least one prime of E, having relative degree 1, if $\mathfrak{p}$ divisible by a prime $P \subseteq \mathcal{O}_L$ s.t. $\left(\frac{L/K}{P}\right)$ is cycle of length 1 (where: acting on cosets $H\gamma$ of H in σ).

$\iff \gamma\left(\frac{L/K}{P}\right)\gamma^{-1} \in H \iff \mathfrak{p} \in S_d$, some d.

Let: S_E = primes of E, degree 1 over K. For each $\mathfrak{p} \in S_d$, let $n(\mathfrak{p})$ = # primes of S_E, dividing $\mathfrak{p}$.

$\Rightarrow \mathfrak{p} \in S_d$ is norm of exactly $n(\mathfrak{p})$ primes in S_E.

Since $\mathfrak{f}_E$ contains all primes of degree 1 over K:

$\Rightarrow \delta(S_E) = 1$.

$$\Rightarrow -\text{Log}(s-1) \sim \sum_{\mathfrak{p}_E \in S_E} \frac{1}{N_{K/\mathbb{Q}}(N_{E/K}(\mathfrak{p}_E))^s}$$

$$\sim \sum_{d \mid n} \sum_{\mathfrak{p} \in S_d} n(\mathfrak{p}) N(\mathfrak{p})^{-s} \quad (*).$$

By Prop 8: $\forall \mathfrak{p} \in S_d$: $n(\mathfrak{p})$ = # distinct cosets $H\gamma$ of H s.t. $H\gamma\sigma^d = H\gamma \iff \gamma\sigma^d\gamma^{-1} \in H = \langle \sigma \rangle \iff \gamma \in N_G(\langle \sigma^d \rangle)$

So: $n(\mathfrak{p}) = [N_G(\langle \sigma^d \rangle) : H]$.

Then: re-arrange! Finished next time.

14

Algebraic NT: Lecture 16 | 23/02/2024

From last time: Frobenius Reciprocity.

Theorem 9 L/K Galois, $\sigma \in \mathrm{Gal}(L/K)$ order n, & $t =$ # elements in its division.

Then if $S = \{\mathfrak{p} \in P_K : \exists P \subseteq P_L,\ P \mid \mathfrak{p}$ & $\left(\frac{L/K}{P}\right)$ conj to σ^m, some $m\}$

then $\delta(S) = \frac{t}{|G|}$.

Proof (Continued). Have: $[N_G(H) : H] \sum_{\mathfrak{p} \in S_1} N(\mathfrak{p})^{-s}$

$$\sim \log(s-1) \cdot \underbrace{\left(-1 + \sum_{\substack{d \mid n \\ d \neq 1}} \frac{[N_G(\langle\sigma^d\rangle)]}{|G|} t_d\right)}_{(*)} \qquad (S_1 = S)$$

& By lemma X: $t_d = \phi\left(\frac{n}{d}\right)[G : N_G(\langle\sigma^d\rangle)]$

$$\Rightarrow (*) = -1 + \sum_{\substack{d \mid n \\ d \neq 1}} \phi\left(\frac{n}{d}\right) \frac{[G : N_G(\langle\sigma^d\rangle)] \cdot [N_G(\langle\sigma^d\rangle) : H]}{|G|}.$$

$$= -1 + \sum_{\substack{d \mid n \\ d \neq 1}} \phi\left(\frac{n}{d}\right) \frac{[G : H]}{|G|} = -1 + \sum_{\substack{d \mid n \\ d \neq 1}} \frac{1}{n} \phi\left(\frac{n}{d}\right)$$

$$= -1 - \frac{\phi(n)}{n} + \frac{1}{n} \underbrace{\sum_{d \mid n} \phi\left(\frac{n}{d}\right)}_{=1}$$

$$= \frac{\phi(n)}{n} \checkmark$$

$$\Rightarrow \sum_{\mathfrak{p}\in S} N(\mathfrak{p})^{-s} \sim \frac{-\phi(n)}{h\left[N_a(H):H\right]} \log(s-1) = \frac{-t}{|G|}\left(\log(s-1)\right)$$

by Lemma 10.

Theorem 12 [Surj of Artin Map]

Let: L/K Abelian, $\underline{m}$ modulus of K div. by all ram. primes.

Then, Artin map $\Phi_{\underline{m}} : I_K(\underline{m}) \longrightarrow Gal(L/K)$ Surj.

Proof Let $\sigma \in Gal(L/K)$. Since Abelian: division of σ consists of elements, which generate cyclic group $\langle\sigma\rangle$.

By Frobenius Density: Find infinitely many prime ideals $\mathfrak{P}$ of L, s.t. $\left(\frac{L/K}{\mathfrak{P}}\right)$ generates $\langle\sigma\rangle$.

Since only finitely many primes divide $\underline{m}$, can pick some $\mathfrak{P}$ of L, s.t. $\mathfrak{p} = \mathfrak{P}\cap\mathcal{O}_K$ is coprime to $\underline{m}$.

$\Rightarrow \mathfrak{p} \in I_K(\underline{m})$, and $\Phi_{\underline{m}}(\mathfrak{p}) = \sigma'$, where σ' is some generator of $\langle\sigma\rangle$. $\left(= \left(\frac{L/K}{\mathfrak{P}}\right)\right)$

$\Rightarrow \sigma$ is in image of $\Phi_{\underline{m}}$ ✓

Theorem 13 [Chebotarev Density Theorem]

L/K Galois, $\sigma \in Gal(L/K)$ & say σ has c conjugates in $Gal(L/K)$. & Let $S = \left\{\mathfrak{p}\in\mathcal{O}_K : \left(\frac{L/K}{\mathfrak{P}}\right) = \sigma, \text{ for some } \mathfrak{P}\mid\mathfrak{p}\right\}$

Then: $\delta(S) = \dfrac{c}{|Gal(L/K)|}$.

Note: Original proofs did not need CFT. But, those in modern textbooks do. $\square$

Notation If L/K Not Abelian, can still write $\left(\frac{L/K}{\mathfrak{p}}\right)$, to denote Conjugacy class of $\left(\frac{L/K}{\mathfrak{P}}\right)$ $\forall \mathfrak{P} | \mathfrak{p}$.

Corollary 14 L/K Abelian, $\mathfrak{m}$ modulus div. by all ram. primes. & $\sigma \in Gal(L/K)$, $S = \{\mathfrak{p} \subset \mathcal{O}_K : \mathfrak{p} \nmid \mathfrak{m}, \left(\frac{L/K}{\mathfrak{p}}\right) = \sigma\}$.

$\Rightarrow \delta(S) = \frac{1}{[L:K]}$. [Follows from Theorem 13]

Also, Chebotarev DT gives alternative proof for:

Lemma 4: $S_{L/K} = \{\text{Completely split primes}\} \Rightarrow \delta(S_{L/K}) = \frac{1}{[L:K]}$.

Proof Let $\sigma = 1$. Then, set of primes with $\left(\frac{L/K}{\mathfrak{p}}\right) = 1$ has density $\frac{1}{[L:K]}$ (by Chebotarev). But: $\left(\frac{L/K}{\mathfrak{p}}\right) = 1 \Leftrightarrow \mathfrak{p}$ split completely.

Next: Show that primes that split completely, characterise the extension L/K.

Notation Given 2 sets S, T, say $S \dot{\subset} T \Leftrightarrow S \subset T \cup \Sigma$ for some Finite set Σ. If symmetric, write $S \doteq T$.

Theorem 15 $L, M/K$ Galois exts. Then,

1) $L \subset M \Leftrightarrow S_{M/K} \dot{\subset} S_{L/K}$

2) $L = M \Leftrightarrow S_{M/K} \doteq S_{L/K}$.

Prop 16 $L, M/K$ Finite exts. Then:

1) If M/K Galois, then $L \subset M \Leftrightarrow S_{M/K} \dot{\subset} S_{L/K}$

2) If L Galois $/K$ then $L \subset M \Leftrightarrow \tilde{S}_{M/K} \doteq S_{L/K}$,

where $\tilde{S}_{M/K} = \{ \mathfrak{p} \subset \mathcal{O}_K : \mathfrak{p}$ un-ram in M & $f_{P|\mathfrak{p}} = 1$ for some $P \subseteq \mathcal{O}_M, P|\mathfrak{p} \}$.

Lemma 17 L/K Finite ext. Degree. Has: Galois closure M/K. Then: $\delta(S_{L/K}) = \delta(S_{M/K}) = \frac{1}{[M:K]}$

Proof $\mathfrak{p} \subseteq \mathcal{O}_K$ splits completely in $L \Leftrightarrow$ splits completely in all conjugates of $L \subset M$, i.e. $\sigma(L)$ & $\forall \sigma \in Gal(M/K)$.

& Galois closure M is compositum of All such $\sigma(L)$

$\Rightarrow \mathfrak{p}$ splits completely in $L \Leftrightarrow$ Splits completely in M.

Proof (of Prop 16) First, prove 2) ~~as Exercise~~.

So, assume: $\tilde{S}_{M/K} \doteq S_{L/K}$ (Exercise) when $L \subset M$.

& N Galois ext of K, containing both K, M.

So, to prove $L \subset M$, suffices to show $Gal(N/M) \subset Gal(N/L)$.

Need: $\forall \sigma \in Gal(N/M)$, need: $\sigma|_L = 1$

By Chebotarev: find $\mathfrak{p} \subset \mathcal{O}_K$, unram in N, s.t. $\left(\frac{N/K}{\mathfrak{p}}\right)$ is conj class of σ. Then: $\exists P \subset \mathcal{O}_N$, $P|\mathfrak{p}$ & $\left(\frac{N/K}{P}\right) = \sigma$.

Claim: $\mathfrak{p} \in \tilde{S}_{M/K}$.

Let: $P_M = P \cap \mathcal{O}_M$. For $\alpha \in \mathcal{O}_M$, $\alpha \equiv \sigma(\alpha) \equiv \alpha^{N(\mathfrak{p})}$ mod P_M. ($\sigma|_M = 1$, Def)

$\Rightarrow \mathcal{O}_M/P_M \cong \mathcal{O}_K/\mathfrak{p}$, hence, $f_{P_M|\mathfrak{p}} = 1$. $\Rightarrow \mathfrak{p} \in \tilde{S}_{M/K}$ ✓

By Chebotarev: Find infinitely many such $\mathfrak{p}$. $\Rightarrow$ Can assume $\mathfrak{p} \in S_{L/K}$

Proof continued | Since $\tilde{S}_{M|K} \dot{\subseteq} S_{L|K}$, and found so many $\mathfrak{p} \in \tilde{S}_{M|K}$, can assume $\mathfrak{p} \in S_{L|K}$.

$\Rightarrow \left(\frac{L|K}{\mathfrak{p}}\right) = \left(\frac{M|K}{\mathfrak{p}}\right)\Big|_L = \sigma|_L = 1$ since $\left(\frac{L|K}{\mathfrak{p}}\right) = 1$ ✓

For first part: $S_{M|K} \dot{\subseteq} S_{L|K} \Rightarrow S_{L|K} = S_{L'|K}$, where L' is Galois closure of $L|K$. So, $S_{M|K} \dot{\subseteq} S_{L|K} \Rightarrow \tilde{S}_{M|K} \dot{\subseteq} S_{L'|K}$ & By 2nd part of prop: $L' \subseteq M \Rightarrow L \subseteq M \Rightarrow S_{M|K} \dot{\subseteq} S_{L|K}$ ✓

Proof (Theorem 15)

Note 2nd part follows from 1st part & 1st part follows from Prop 17, since $\tilde{S}_{M|K} = S_{M|K}$ for Galois extensions ✓

Theorem 18 | $\mathfrak{m}$ modulus of K & L, M $|K$ Abelian exts s.t. unramified at primes that don't divide $\mathfrak{m}$.

Then, $\boxed{\ker(\Phi_{L|K,\mathfrak{m}}) = \ker(\Phi_{M|K,\mathfrak{m}}) \Rightarrow L = M.}$

In particular, Ray class field is Unique (if exists).

Proof | $S \equiv$ Set of primes of K that don't divide $\mathfrak{m}$.

Then: know, $\forall \mathfrak{p} \in S$, $\mathfrak{p}$ unram in both L, M, and $\mathfrak{p}$ splits Completely in both L (and M), iff it lies in kernel of $\Phi_{L|K,\mathfrak{m}}$.

So, if $\ker(\Phi_{L|K,\underline{m}}) = \ker(\Phi_{M|K,\underline{m}})$

$\Rightarrow S_{L|K} \doteq (S \cap \ker(\Phi_{L|K,\underline{m}})) = (S \cap \ker(\Phi_{M|K,\underline{m}})) \doteq S_{M|K}$

$\Rightarrow L = M$ by Theorem 15 ✓

Prop 19 $L|K$ Abelian & $\underline{m}$ modulus divisible by $\underline{f}_{L|K}$.
Then, $\ker(\Phi_{L|K,\underline{m}}) \subseteq T_{L|K}(\underline{m})$.

Proof Since $\underline{m}$ div. by $\underline{f}_{L|K}$, have $P_K(\underline{m}) \subset \ker(\Phi_{\underline{m}}) \subseteq I_K(\underline{m})$

$\Rightarrow$ In particular, $\forall\, \underline{a} \in I_K(\underline{m})$: $\left(\frac{L|K}{\underline{a}}\right)$ only depends on the ideal class of $\underline{a}$ mod $P_K(\underline{m})$.

& Recall: $P_K(\underline{m}) = \ker(\Phi_{K_{\underline{m}}|K,\underline{m}})$

$\Rightarrow$ By Chebotarev: $\forall \sigma \in Gal(L|K)$, $\exists$ inf many primes $\mathfrak{p}$, s.t. $\left(\frac{K_{\underline{m}}|K}{\mathfrak{p}}\right) = \sigma$. So, pick one s.t. $\mathfrak{p} \nmid \underline{m}$.

Since $\exists$ isom. $I_K(\underline{m})/P_K(\underline{m}) \cong Gal(\underline{k}_{\underline{m}}/K)$

$\Rightarrow$ Any $\underline{a} \subseteq I_K(\underline{m})$ is equivalent to a prime mod $P_K(\underline{m})$.

Now, suppose $\mathfrak{p} \subset \mathcal{O}_K$ is such that $\mathfrak{p} \in \ker(\Phi_{L|K,\underline{m}})$.

Then, $\left(\frac{L|K}{\mathfrak{p}}\right) = 1$.

$\Rightarrow \mathfrak{p}$ splits Completely in L.

& If $\mathfrak{P} \subset \mathcal{O}_L$, $\mathfrak{P} \mid \mathfrak{p}$, then $N_{L|K}(\mathfrak{P}) = \mathfrak{p} \Rightarrow \mathfrak{p} \in N_{L|K}(I_L(\underline{m})) \subset T_{L|K}(\underline{m})$ ✓

Part 4: Global CFT, using Language of Ideles.

Recap (Local Fields): Let K Nf, $\Rightarrow$ Any abs val of K is equiv to either $|\cdot|_\mathfrak{p}$ or $|\cdot|_\sigma$. [As before, $\mathfrak{p}$ = finite/infinite.]
& **Product formula:** $\prod_{\mathfrak{p}} |x|_\mathfrak{p} = 1 \quad \forall x \in K^*$.

Recall, $|\cdot|_\mathfrak{p}$ induces Topology on K.
An Abs val $|\cdot|_\mathfrak{p}$ on K **Non-Archimedean** $\Leftrightarrow |x+y| \leq \max\{|x|, |y|\}$
& **Archimedean** if not equivalent to valuation satisfying ↑.
[Which is the case for Infinite primes $\mathfrak{p}$].

If $|\cdot|_\mathfrak{p}$ Non-Archimedean: $R = \{x : |x| \leq 1\}$ & $\underline{m} = \{x : |x| < 1\}$.
$\Rightarrow R$ Local ring, $\underline{m}$ Maximal ideal & $k \equiv R/\underline{m}$ quotient field.
& $(R, |\cdot|_\mathfrak{p}) \equiv$ Valuation Ring.

For any $|\cdot|_\mathfrak{p}$: $K_\mathfrak{p} \equiv$ Completion of K WRT $|\cdot|_\mathfrak{p}$.
If $\mathfrak{p}$ Infinite: $K_\mathfrak{p} \cong \mathbb{R}$ or $\mathbb{C}$, depending on if $\mathfrak{p}$ real/complex.
If $\mathfrak{p}$ Finite: $\mathcal{O}_{K_\mathfrak{p}} = \{x \in K_\mathfrak{p} : |x|_\mathfrak{p} \leq 1\}$ Ring of Integers.
Is: Compact & Discrete Valuation. [Value group $\cong \mathbb{Z}$].
Under +: Is open subring of $K_\mathfrak{p}$, with units $\mathcal{O}_{K_\mathfrak{p}}^\times$.
& Unique maximal ideal $\underline{m}_{K_\mathfrak{p}} = \{x \in K_\mathfrak{p} : |x|_\mathfrak{p} < 1\}$.

Examples 1) $K = \mathbb{Q}$ & $\mathfrak{p} = p$ rational prime. $K_\mathfrak{p} = \mathbb{Q}_p$.

For each $\mathfrak{p}$, can embed $i_\mathfrak{p} : K \hookrightarrow K_\mathfrak{p}$.

& If $\alpha \in K$, $\alpha \neq 0 \Rightarrow i_{\mathfrak{p}}(\alpha) \neq 0$, and is unit in $K_{\mathfrak{p}}$ for all but finitely many $\mathfrak{p}$.

[Units of $K_{\mathfrak{p}}$ are: $\mathcal{O}_{K_{\mathfrak{p}}}^{*}$ if $\mathfrak{p}$ finite, and $K_{\mathfrak{p}}^{*}$ if else].

Would: Like to use Local data + Valuation Theory, to study Number fields (Global objects).
$\Rightarrow$ Want to "Embed K into all completions $K_{\mathfrak{p}}$ simultaneously".

But: doesn't work! $\prod_{\mathfrak{p}} K_{\mathfrak{p}}$ not nice, e.g. not locally compact.

Restricted Product Topology.

DEF 1] Let: (X_i) family of spaces & (U_i) family of open sets of X_i. The Restricted Product $\prod_i' (X_i, U_i)$ is the space $\{(x_i) : x_i \in U_i$ for all but finitely many $i\}$.

& Basis of open sets: $\mathcal{B} = \{\prod V_i : V_i \subset X_i$ open $\forall i$, $V_i = U_i$ for almost all $i\}$.

[Not subspace top. !]

Prop 2] $(X_i)_{i \in I}$ Locally Compact. & $(U_i)_{i \in I}$ family of open $U_i \subset X_i$, s.t. almost all U_i compact. Then: $\prod'(X_i, U_i)$ Locally compact.

Next Steps: Adeles & Ideles..

DEF 3] Adele of NF K is: family $(\alpha_{\mathfrak{p}}) = \alpha$ of elements $\alpha_{\mathfrak{p}} \in K_{\mathfrak{p}}$ ($\mathfrak{p}$ prime in K) s.t. $\alpha_{\mathfrak{p}}$ Integral in $K_{\mathfrak{p}}$, for almost all $\mathfrak{p}$.

The set of all Adeles form ring $\mathbb{A}_K$, defining + and $\times$ component-wise (for each $\mathfrak{p}$).
$= \{(\alpha_{\mathfrak{p}}) \in \prod (K_{\mathfrak{p}}, \mathcal{O}_{K_{\mathfrak{p}}})\}$.

Algebraic NT: lecture 18 | 28/02/2024

From last time Ring of Adeles.

$$\mathbb{A}_K = \left\{ (\alpha_\mathfrak{p}) \in \prod_\mathfrak{p} K_\mathfrak{p} : \alpha_\mathfrak{p} \in \mathcal{O}_{K_\mathfrak{p}} \text{ for all but fin many } \mathfrak{p} \right\}.$$

If $\alpha \in \mathbb{A}_K$ then $\alpha_\mathfrak{p}$ is Projection of α to $K_\mathfrak{p}$.

Example] $K = \mathbb{Q}$. $\Rightarrow \mathbb{A}_K = \prod_p{}' (\mathbb{Q}_p, \mathcal{O}_{\mathbb{Q}_p})$.

$= \mathbb{R} \times \left\{ (\alpha_p) \in \prod_p \mathbb{Q}_p : \alpha_p \in \mathbb{Z}_p \text{ for almost all } p \right\}$.

$= \mathbb{R} \times \left\{ (\alpha_p) \in \prod_{p \text{ fin}} \mathbb{Q}_p : |\alpha_p|_p \leq 1 \text{ for almost all } p \right\}$.

Prop 4] $\mathbb{A}_K$ Locally Compact & Hausdorff.

Proof] First, note: all $K_\mathfrak{p}$ locally compact, and all but fin. many $\mathcal{O}_{K_\mathfrak{p}}$ are Valuation Rings of Non-Arch Local Field.

$\Rightarrow$ By Prop 2: $\mathbb{A}_K$ locally compact ✓

For Hausdorff: $\prod_\mathfrak{p} K_\mathfrak{p}$ Hausdorff (since each $K_\mathfrak{p}$ is)

& Topology on $\prod'$ is finer than subspace top, so Hausdorff.

Let: S finite set of primes, Then: have a subring of $\mathbb{A}_K$, called the S-adeles $\mathbb{A}_{K,S} = \prod_{\mathfrak{p} \in S} K_\mathfrak{p} \times \prod_{\mathfrak{p} \notin S} \mathcal{O}_{K_\mathfrak{p}}$.

The Canonical embedding $K \hookrightarrow K_\mathfrak{p}$ induces canonical embed.

$K \hookrightarrow \mathbb{A}_K$, $x \mapsto (x, x, \ldots)$.

& Note $\forall x \in K$, have $x \in \mathcal{O}_{K_\mathfrak{p}}$ for all but fin many $\mathfrak{p}$.

$\Rightarrow$ The image of $K \subset \mathbb{A}_K$ is Subring of Principal Adeles.

The Group of Ideles.

The Idele Group of K is: unit group of the ring of adeles:

$$\mathbb{A}_K^* = \{ \alpha = (\alpha_p) \in \mathbb{A}_K : \alpha_p \in K_p^* \ \forall p, \ \alpha_p \in \mathcal{O}_{K_p}^* \text{ for all but fin } p \}.$$

This is not a topological group as subspace of $\mathbb{A}_K$!!

DEF 5] Group of Ideles is Topological Group:

$$\boxed{I_K = \prod_p{}' (K_p^*, \mathcal{O}_{K_p}^*)}, \text{ mult. defined component-wise.}$$

Prop 6] I_K Locally Compact & Hausdorff

Proof] Note: Topology on I_K is finer than topology of $\mathbb{A}_K^* \subset \mathbb{A}_K$, hence, Hausdorff.

For locally compact: $\forall p$ Finite prime: $\mathcal{O}_{K_p}^* = \{ x \in K_p : |x|_p = 1 \}$.

Is: Compact subspace of $\mathcal{O}_{K_p}$ (since closed $\subset$ compact)

& This applies to Almost all primes p. & K_p^* locally compact $\forall p$. $\Rightarrow$ I_K locally compact (Prop 2).

The Canonical Embedding $K \hookrightarrow \mathbb{A}_K$ restricts to a canonical embedding $K^* \hookrightarrow I_K$. $\Rightarrow$ View $K^* \subseteq I_K$.

DEF 7] $K^* \subset I_K$ Principal Ideles.

& Quotient $\boxed{C_K \equiv \mathbb{I}_K / K^*}$ Idele Class Group.

& For any S finite set of primes, let S-ideles be:

$$\mathbb{I}_{K,S} = \prod_{\mathfrak{p}\in S} K_{\mathfrak{p}}^* \times \prod_{\mathfrak{p}\notin S} \mathcal{O}_{K_{\mathfrak{p}}}^*$$

$$= \prod_{\mathfrak{p}\mid\infty} K_{\mathfrak{p}}^* \times \prod_{\substack{\mathfrak{p}\nmid\infty \\ \mathfrak{p}\mid S}} K_{\mathfrak{p}}^* \times \prod_{\mathfrak{p}\notin S} \mathcal{O}_{K_{\mathfrak{p}}}^* .$$

$$\Rightarrow \mathbb{I}_K = \bigcup_{S \text{ fin.}} \mathbb{I}_{K,S}$$

So, if $S_\infty \equiv \{\text{Inf. primes } \mathfrak{p}\}$, then:

$$\boxed{\mathbb{I}_{K,S_\infty} = \prod_{\mathfrak{p}\mid\infty} K_{\mathfrak{p}}^* \times \prod_{\mathfrak{p}\text{ fin}} \mathcal{O}_{K_{\mathfrak{p}}}^*}.$$

The Idele class group is NOT finite (contrast class group!)

Prop 8] $\mathbb{I}_K / \mathbb{I}_{K,S_\infty} \cong I_K$ & $Cl(K) \cong \mathbb{I}_K / \mathbb{I}_{K,S_\infty} K^*$.

Proof] Consider hom: $(\cdot) : \mathbb{I}_K \to I_K$, $(\alpha) = \prod_{\mathfrak{p}\nmid\infty} \mathfrak{p}^{v_{\mathfrak{p}}(\alpha_{\mathfrak{p}})}$.

[map ignores infinite primes & Surjective].

Kernel is: $\prod_{\mathfrak{p}\mid\infty} K_{\mathfrak{p}}^* \times \prod_{\mathfrak{p}\nmid\infty} \mathcal{O}_{K_{\mathfrak{p}}}^* = \mathbb{I}_{K,S_\infty}$. ✓

Moreover: notice $(\cdot)$ is Continuous map WRT Discrete topology on I_K. [Take $\underline{a} \in I_K$ & observe $(\cdot)^{-1}(\underline{a})$ open]

& Image $K^* \hookrightarrow \mathbb{I}_K \xrightarrow{(\cdot)} I_K$ has image P_K.

$\Rightarrow$ Map induces surjective hom: $C_K = \mathbb{I}_K / K^* \to Cl(K)$, with kernel $\mathbb{I}_{K,S_\infty} K^*$. ✓

Since I_K/P_K finite: can enlarge S_∞ to some set S, such that $\mathbb{I}_K = \mathbb{I}_{K,S} K^*$:

Prop 9 $\mathbb{I}_K = \mathbb{I}_{K,S} K^*$ & $C_K = \mathbb{I}_{K,S} K^*/K^*$ for S sufficiently large (finite) set of primes of K.

Proof $\mathfrak{a}_1, \dots, \mathfrak{a}_n$ ideals, representing $cl_K = I_K/P_K$.
$\Rightarrow \forall i$, $\mathfrak{a}_i$ divisible by finitely many prime ideals.

Claim: $\mathbb{I}_K = \mathbb{I}_{K,S} K^*$ $\forall S$ any finite set of primes containing all such primes, and infinite primes too.

Indeed: from before, $\mathbb{I}_K / \mathbb{I}_{K,S_\infty} \cong I_K$.

For $\alpha \in \mathbb{I}_K$: $(\alpha) = \prod_{p \nmid \infty} \mathfrak{p}^{v_\mathfrak{p}(\alpha_p)}$ belongs to some $\mathfrak{a}_i P_K$.

$\Leftrightarrow \exists (a)$ principal, s.t. $(\alpha) = \mathfrak{a}_i (a)$.

Consider: idele $\alpha' \equiv \alpha \cdot a^{-1}$. Then, under map $\mathbb{I}_K \to I_K$, α' mapped to $\mathfrak{a}_i = \prod_{p \nmid \infty} \mathfrak{p}^{v_\mathfrak{p}(\alpha'_\mathfrak{p})}$.

& Since primes dividing $\mathfrak{a}_i$ are in S: $v_\mathfrak{p}(\alpha'_\mathfrak{p}) = 0$ $\forall \mathfrak{p} \notin S$

$\Rightarrow v_\mathfrak{p}(\alpha'_\mathfrak{p}) = 0 \Rightarrow \alpha'_\mathfrak{p} \in \mathcal{O}_{K_\mathfrak{p}}^\times \Rightarrow \alpha' = \alpha a^{-1} \in \mathbb{I}_{K,S}$.

$\Rightarrow \alpha \in \mathbb{I}_{K,S} K^*$ ✓

Prop 10 K^* discrete subgroup of $\mathbb{I}_K$. [$\Rightarrow K^* \subset \mathbb{I}_K$ is closed subgroup]

Proof Suffices to show 1 isolated.

Consider: $U = \{\alpha \in \mathbb{I}_K : |\alpha_\mathfrak{p}|_\mathfrak{p} = 1 \ \forall \mathfrak{p} \nmid \infty$ & $|\alpha_\mathfrak{p} - 1| < 1 \ \forall \mathfrak{p} | \infty\}$

If $\exists x \neq 1$ in U principal adele, then: by Product Formula:

$1 = \prod_\mathfrak{p} |x-1|_\mathfrak{p} = \prod_{\mathfrak{p} \nmid \infty} |x-1|_\mathfrak{p} \prod_{\mathfrak{p} | \infty} |x-1|_\mathfrak{p} < \prod_{\mathfrak{p} \nmid \infty} |x-1|_\mathfrak{p} \leq \max_{\mathfrak{p} \nmid \infty} |x-1|_\mathfrak{p} \leq 1$.

Algebraic NT: Lecture 19 | 01/03/2024

From last time: Ideles, Idele Class Group.

Review: Topological group G Discrete, if $\forall g \in G$, $\exists U \ni g$ neighborhood, only containing g.

& A subgroup of top. group $H \leq G$ is discrete subgroup, if: H discrete, when viewed with Subspace top. for G.

$\iff \exists$ Nbhood of $e \in G$, of H, containing no other elements of H.

Let: K NF, $\mathbb{I}_K$ Ideles, $C_K = \mathbb{I}_K / K^*$ Idele class group.

DEF 11 Define: Absolute Norm of $\alpha \in \mathbb{I}_K$ to be $N(\alpha) \equiv \prod_f |\alpha_f|_f$. $N: \mathbb{I}_K \to \mathbb{R}^\times$.

& $\mathbb{I}_K^0 = \{\alpha \in \mathbb{I}_K : N(\alpha) = 1\}$ kernel of N.

By Product formula: $\forall x \in K^\times$, $N(x) = \prod_f |x|_f = 1$.

$\Rightarrow \exists$ well-def'ed Norm map $N: C_K \to \mathbb{R}^\times$.

Denote: $C_K^0 = \{[\alpha] \in C_K : N([\alpha]) = 1\}$ kernel of this N.

Prop 12 C_K^0 is Compact.

This can be used to: prove Generalisation of Dirichlet's Unit Theorem. Let: S Finite set of primes, containing ALL infinite ones. Let: $O_{K,S} = \{x \in K : \forall f \in S, f \text{ finite} : |x|_f \leq 1\}$.

Corollary 13 $\mathcal{O}_{K,S}^*$ is f.g. Abelian group, rank $|S|-1$.

Note Dirichlet follows, when S = primes dividing ∞.

For each prime $\mathfrak{p}$: consider Hom $n_{\mathfrak{p}}: K_{\mathfrak{p}}^* \longrightarrow \mathbb{I}_K$,

$$x \longmapsto n_{\mathfrak{p}}(x) = (1, \dots, x, \dots)$$

i.e. Idele, with 1 at all components, except at $\mathfrak{p}$ where $(N_{\mathfrak{p}}(x))_{\mathfrak{p}} = x$.

We also need: $\bar{n}_{\mathfrak{p}}: K_{\mathfrak{p}}^* \longrightarrow C_K$.

$$x \longmapsto [n_{\mathfrak{p}}(x)]$$

Prop 14 $C_K \cong C_K^0 \times r_K$, where $r_K \cong \mathbb{R}_+^*$

Proof Amounts: to showing that the group extension:

$$1 \longrightarrow C_K^0 \longrightarrow C_K \xrightarrow{N} \mathbb{R}_+^* \longrightarrow 1 \text{ splits}$$

$\Longleftrightarrow$ Need injection $\mathbb{R}_+ \hookrightarrow C_K$, when composed with $N: C_K \longrightarrow \mathbb{R}_+^*$, gives Identity map on $\mathbb{R}_+^*$.

Pick: Any infinite prime $\mathfrak{p}$ & consider map $\bar{n}_{\mathfrak{p}}: K_{\mathfrak{p}}^* \longrightarrow C_K$, as above. Then, $K_{\mathfrak{p}}^*$ contains $\mathbb{R}_+^*$ as subgroup.

* If $\mathfrak{p}$ real: $\bar{n}_{\mathfrak{p}}$ gives Injection we want (since: $N(n_{\mathfrak{p}}(x)) = |x|_{\mathfrak{p}} = x \in \mathbb{R}_+^* \quad \forall x \in K_{\mathfrak{p}}^*$)

* If $\mathfrak{p}$ complex: $N(n_{\mathfrak{p}}(x)) = |x|_{\mathfrak{p}} = x^2 \in \mathbb{R}_+^*$.

$\Rightarrow$ Choose the map $x \longmapsto \bar{n}_{\mathfrak{p}}(\sqrt{x})$. ✓

Corollary 15 The Idele class group is finite.

Proof $\exists$ Surjective map $\mathbb{I}_K^0 \longrightarrow I_K$ [Exercise], which is Continuous WRT discrete topology on I_K. Under the map $\mathbb{I}_K \longrightarrow I_K$: Have seen, image of K^* is P_K. So, $Cl(K) = I_K / P_K$ is: Continuous image of compact group C_K^0. Hence: Finite ✓

Next: let $\underline{m} = \prod_{\mathfrak{p}} \mathfrak{p}^{N_{\mathfrak{p}}}$. Modulus of K.

& $U_{\mathfrak{p}}^{n_{\mathfrak{p}}} = \begin{cases} O_{K_{\mathfrak{p}}}^\times : & \mathfrak{p} \nmid \infty \ \& \ n_{\mathfrak{p}} = 0 \\ 1 + \mathfrak{p}^{n_{\mathfrak{p}}} : & \mathfrak{p} \nmid \infty \ \& \ n_{\mathfrak{p}} > 0 \\ \mathbb{R}_+^\times \subset k_{\mathfrak{p}}^\times & \mathfrak{p} \text{ real}, \ n_{\mathfrak{p}} = 1 \\ \mathbb{R}^\times \cong k_{\mathfrak{p}}^\times & \mathfrak{p} \text{ real}, \ n_{\mathfrak{p}} = 0 \\ \mathbb{C}^\times & \mathfrak{p} \text{ Complex.} \end{cases}$

If $\alpha_{\mathfrak{p}} \in k_{\mathfrak{p}}^\times$: define $\alpha_{\mathfrak{p}} \equiv 1 \bmod \mathfrak{p}^{n_{\mathfrak{p}}} \Leftrightarrow \alpha_{\mathfrak{p}} \in U_{\mathfrak{p}}^{n_{\mathfrak{p}}}$.

Define: $U_{\mathfrak{p}}^0 \equiv U_{\mathfrak{p}}$ for the case $\mathfrak{p}$ finite, $n_{\mathfrak{p}} = 0$.

If $\mathfrak{p}$ real, $n_{\mathfrak{p}} = 1$, then: $\alpha_{\mathfrak{p}} > 0$.

Recall: $U_{\mathfrak{p}} = \begin{cases} O_{K_{\mathfrak{p}}}^\times, & \mathfrak{p} \text{ finite} \\ k_{\mathfrak{p}}^\times \cong \mathbb{R} & \mathfrak{p} \text{ real} \\ k_{\mathfrak{p}}^\times \cong \mathbb{C} & \mathfrak{p} \text{ complex.} \end{cases}$

$\Rightarrow$ for $\alpha \in \mathbb{I}_K$ idele, set $\alpha \equiv 1 \bmod \underline{m} \Leftrightarrow \alpha_{\mathfrak{p}} \equiv 1 \bmod \mathfrak{p}^{n_{\mathfrak{p}}}$ $\forall \mathfrak{p}$. $\square$

DEF 14 K NF. $\mathfrak{m} = \prod_{\mathfrak{p}} \mathfrak{p}^{n_{\mathfrak{p}}}$ modulus (for K).

Let: $I_K(\mathfrak{m}) = \{\alpha \in I_K : \alpha \equiv 1 \bmod \mathfrak{m}\} = \prod_{\mathfrak{p}} U_{\mathfrak{p}}^{n_{\mathfrak{p}}} \subset I_K$.

Examples: If $\mathfrak{m} = 1$ then $I_K(1) = I_{K,S_\infty} = \prod_{\mathfrak{p}\mid\infty} K_{\mathfrak{p}}^{*} \times \prod_{\mathfrak{p}\nmid\infty} U_{\mathfrak{p}}$.

DEF 17 $C_K(\mathfrak{m}) = I_K(\mathfrak{m}) K^* / K^* \subset C_K$

Called: Congruence Subgroup mod $\mathfrak{m}$ of C_K.

The factor Group $C_K / C_K(\mathfrak{m})$ is Ray Class Group mod $\mathfrak{m}$.

Example: for $\mathfrak{m} = 1$: $C_K / C_K(1) = (I_K / K^*) / (I_{K,S_\infty} K^* / K^*)$

$\cong I_K / I_{K,S_\infty} K^* \cong I_K / P_K \cong Cl(K)$.

Will see: the 2 notions of Ray Class Group are isomorphic $\forall \mathfrak{m}$.

Recall: had $I_K = \bigcup_S I_{K,S}$. Can: also define the topology on I_K directly by specifying a Fundamental System of neighbourhoods of the Identity in I_K, given by: the Subsets $\prod_{\mathfrak{p}\in S} W_{\mathfrak{p}} \times \prod_{\mathfrak{p}\notin S} U_{\mathfrak{p}} \subseteq I_K$.

[Where: $W_{\mathfrak{p}} \subseteq K_{\mathfrak{p}}^{*}$ ranges across all Fundamental system of neighborhoods of the Identity in $K_{\mathfrak{p}}^{*}$]

& S ranges across all Finite set of primes of K.

Prop 18 The Closed subgroups of Finite index of C_K are exactly those subgroups, that contain a Congruence Subgroup $C_K(\mathfrak{m})$.

Proof First, note $C_K(\underline{m})$ open in C_K, because $\mathbb{I}_K(\underline{m}) = \prod_{\mathfrak{p}} U_{\mathfrak{p}}^{n_{\mathfrak{p}}}$ is open in $\mathbb{I}_K$.

Will first show: $C_K(\underline{m})$ has finite idx in C_K, which suffices.

Because $C_K(\underline{m})$ is complement of union of its nontrivial open cosets, which are all open, and of which there are finitely many, will follow that $C_K(\underline{m})$ closed of finite index.

This implies: any group containing $C_K(\underline{m})$ is also closed & of finite index, because it's union of finitely many cosets of $C_K(\underline{m})$.

Note: $\mathbb{I}_K(\underline{m}) \subseteq \mathbb{I}_{K,S_\infty} = \prod_{\mathfrak{p}\nmid\infty} K_{\mathfrak{p}}^\times \times \prod_{\mathfrak{p}\mid\infty} U_{\mathfrak{p}}$.

~~Continued next time!~~

$$\begin{aligned}
[C_K : C_K(\underline{m})] &= [C_K : \mathbb{I}_{K,S_\infty} K^\times/K^\times][\mathbb{I}_{K,S_\infty} K^\times/K^\times : C_K(\underline{m})] \\
&= h_K \cdot [\mathbb{I}_{K,S_\infty} K^\times : \mathbb{I}_K(\underline{m}) K^\times] \\
&\leq h_K \cdot [\mathbb{I}_{K,S_\infty} : \mathbb{I}_K(\underline{m})] \\
&= h_K \cdot \prod_{\mathfrak{p}\nmid\infty} [U_{\mathfrak{p}} : U_{\mathfrak{p}}^{n_{\mathfrak{p}}}] \cdot \prod_{\mathfrak{p}\mid\infty} [K_{\mathfrak{p}}^\times : U_{\mathfrak{p}}^{n_{\mathfrak{p}}}] \\
&< \infty \checkmark
\end{aligned}$$

Algebraic NT: Lecture 20 | 04/03/2024

Today: Overview of steps of proof, of CFT.

Proof of Prop 18 (Continued).

Suppose: $N \subseteq C_K$ closed & finite idx. Then, N also open, since it's complement of finitely many (closed) cosets.

$\Rightarrow$ Pre-image of N, say J, in $\mathbb{I}_K$ is also open, hence, contains subset W of form $\prod_{\mathfrak{p} \in S} W_{\mathfrak{p}} \times \prod_{\mathfrak{p} \notin S} U_{\mathfrak{p}}$, for S finite & containing all inf primes.

[& $W_{\mathfrak{p}}$ Open nbhood of $1 \in K_{\mathfrak{p}}^\times$.]

* If $\mathfrak{p} \in S$: can choose $W_{\mathfrak{p}} = U_{\mathfrak{p}}^{n_{\mathfrak{p}}}$, since $\{U_{\mathfrak{p}}^n : n \geq 0\}$ form Basis of neighborhoods of $1 \in K_{\mathfrak{p}}^\times$.

* If $\mathfrak{p} \in S$ Infinite: if real, then open set $W_{\mathfrak{p}}$ generates $(\mathbb{R}_+, \times)$, else, if complex, it generates $(K_{\mathfrak{p}}^\times)$.

$\Rightarrow$ The subgroup of J generated by W is of form $\mathbb{I}_K(\mathfrak{m})$, for some suitable $\mathfrak{m}$.

$\Rightarrow$ N is Subgroup containing $\mathbb{I}_K(\mathfrak{m}) K^\times / K^\times$. ✓

Ideles in Field Extensions.

Local Fields Recap: Let L/K finite NF exts, and $P \subset O_L$, $\mathfrak{p} = P \cap O_K \subseteq O_K$. Then, $L_P \geq K_{\mathfrak{p}}$, since:

Since valuation associated to $\mathfrak{P}$ from L to K gives valuation of K associated to $\mathfrak{p}$.

Let: L/K Galois, $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^e \cdots \mathfrak{P}_r^e$, $\hat{\mathfrak{p}} = \mathfrak{p}\mathcal{O}_{K_\mathfrak{p}}$.

$\Rightarrow \hat{\mathfrak{p}}\mathcal{O}_{L_{\mathfrak{P}_i}} = \hat{\mathfrak{P}}_i^e$ and $f_{\hat{\mathfrak{P}}_i/\hat{\mathfrak{p}}} = f_{\mathfrak{P}_i/\mathfrak{p}}$.

& $\sum_{\mathfrak{P}|\mathfrak{p}} [L_\mathfrak{P} : K_\mathfrak{p}] = [L:K]$.

Let: $G \equiv Gal(L/K)$, $\sigma \in G$. Then, $K_\mathfrak{p} \subset L_{\mathfrak{P}_i}$ & $L_{\sigma\mathfrak{P}}$.

$\Rightarrow \exists$ $K_\mathfrak{p}$ - Isomorphism $L_\mathfrak{P} \xrightarrow{\sigma} L_{\sigma\mathfrak{P}}$.

If $\mathfrak{P} = \sigma\mathfrak{P}$ $\Rightarrow$ gives $K_\mathfrak{p}$ - Isom. $L_\mathfrak{P} \xrightarrow{\sigma} L_\mathfrak{P}$.

$\Rightarrow \sigma \in Gal(L_\mathfrak{P}/K_\mathfrak{p})$.

But: $\mathfrak{P} = \sigma\mathfrak{P} \Leftrightarrow \sigma \in D_{\mathfrak{P}|\mathfrak{p}}$.

$\Rightarrow$ Any $\sigma \in D_{\mathfrak{P}|\mathfrak{p}}$ gives rise to something in $Gal(L_\mathfrak{P}/K_\mathfrak{p})$.

& Converse is also true, since restrict elements of $Gal(L_\mathfrak{P}/K_\mathfrak{p})$ to L.

$\Rightarrow$ Identify $\boxed{D_{\mathfrak{P}|\mathfrak{p}} \Longleftrightarrow Gal(L_\mathfrak{P}/K_\mathfrak{p})}$

& Consider $Gal(L_\mathfrak{P}/K_\mathfrak{p}) \subseteq Gal(L/K)$. (as subgroup)

Let: L/K Finite ext. Then, embed $\mathbb{I}_K$ into $\mathbb{I}_L$, by:

$\alpha = (\alpha_\mathfrak{p}) \in \mathbb{I}_K \hookrightarrow \alpha' = (\alpha'_\mathfrak{P}) \in \mathbb{I}_L$

with components $\alpha'_\mathfrak{P} = \alpha_\mathfrak{p} \in K_\mathfrak{p}^\times \subseteq L_\mathfrak{P}^\times$ $\forall \mathfrak{P}|\mathfrak{p}$.

$\Rightarrow$ Can view $I_K \leq I_L$ as subgroup.

$\Rightarrow \alpha' = (\alpha_{\mathfrak{p}'}) \in I_L$ is in I_K iff all components $\alpha_{\mathfrak{p}'} \in K_{\mathfrak{p}}^\times$ & $\forall \mathfrak{p}, \mathfrak{p}' \mid \mathfrak{p}$, $\alpha_{\mathfrak{p}'} = \alpha_{\mathfrak{p}''}$.

Next: Let L/K Galois, $G = \mathrm{Gal}(L/K)$.

Make: I_L into G-module: $\forall \mathfrak{P} \subset \mathcal{O}_L$, & $\sigma \in G$, it induces isomorphism $L_{\sigma^{-1}\mathfrak{P}} \longrightarrow L_{\mathfrak{P}}$.

$\Rightarrow \forall \alpha \in I_L$, $\alpha = (\alpha_{\mathfrak{P}})$, define $\sigma\alpha \in I_L$ by:

$$\boxed{(\sigma\alpha)_{\mathfrak{P}} = \sigma(\alpha_{\sigma^{-1}\mathfrak{P}}) \in L_{\mathfrak{P}}.}$$

[Note: $\alpha_{\sigma^{-1}\mathfrak{P}} \in L_{\sigma^{-1}\mathfrak{P}}$ is $(\sigma^{-1}\mathfrak{P})$-component of α, mapped to $L_{\mathfrak{P}}$ by σ.]

Denote: $I_L^G = \{\alpha \in I_L : \sigma\alpha = \alpha \ \forall \sigma \in G\}$.

Prop 19 $I_L^G = I_K$. [L/K Galois, $G = \mathrm{Gal}(L/K)$]

Proof $\supseteq$: $\forall \sigma \in G$, have $\sigma : L_{\mathfrak{P}} \to L_{\sigma\mathfrak{P}}$ $K_{\mathfrak{p}}$-Isom. $\forall \mathfrak{P} \mid \mathfrak{p}$.

So, $\forall \alpha \in I_K$, view it as in I_L.

$(\sigma\alpha)_{\mathfrak{P}} = \sigma(\alpha_{\sigma^{-1}\mathfrak{P}}) = \sigma\alpha_{\mathfrak{P}} = \alpha_{\mathfrak{P}} \in K_{\mathfrak{p}}$.

$\Rightarrow \sigma\alpha = \alpha \ \forall \sigma \in G$, so $\alpha \in I_L^G$.

$\subseteq$: for $\alpha \in I_L^G$, $\sigma(\alpha) = \alpha \ \forall \sigma \in G$.

$\Rightarrow (\sigma\alpha)_{\mathfrak{P}} = \sigma\alpha_{\sigma^{-1}\mathfrak{P}} = \alpha_{\mathfrak{P}} \ \forall \mathfrak{P} \subset \mathcal{O}_L$.

Know: $\forall \sigma \in D_{\mathfrak{P}|\mathfrak{p}}$, $\sigma^{-1}\mathfrak{P} = \mathfrak{P} \Rightarrow \alpha_{\mathfrak{P}} = \sigma\alpha_{\mathfrak{P}}$. & $\alpha_{\mathfrak{P}} \in K_{\mathfrak{p}}$. $\square$

& $\forall \sigma \in Gal(L/K)$: $(\sigma\alpha)_{\mathfrak{p}} = \alpha_{\mathfrak{p}} = \sigma\alpha_{\sigma^{-1}\mathfrak{p}} = \alpha_{\sigma^{-1}\mathfrak{p}} \in K_{\mathfrak{p}}$.

$\Rightarrow$ 2 primes lying above $\mathfrak{p} \subset \mathcal{O}_K$ has the same components, hence, $\alpha \in \mathbb{I}_K$. ✓

If α idele, $\alpha \in \mathbb{I}_K$ becomes a Principal idele, i.e. $\alpha \in L^\times$, then α is already principal in K.

Prop 20 L/K Finite. Then, $L^\times \cap \mathbb{I}_K = K^\times$.

Proof $K^\times \subseteq L^\times \cap \mathbb{I}_K$ Immediate.

Let: Ω Galois closure of L/K. Then, $(\mathbb{I}_K \& \mathbb{I}_L) \subseteq \mathbb{I}_\Omega$.

For $\alpha \in \Omega^\times \cap \mathbb{I}_K$: by Prop 19, $\alpha \in \mathbb{I}_\Omega^{Gal(\Omega/K)} = \mathbb{I}_K$

i.e. $\sigma(\alpha) = \alpha$ $\forall \sigma \in Gal(\Omega/K)$.

Since $\alpha \in \Omega^\times$: $\alpha \in (\Omega^\times)^{Gal(\Omega/K)} = K^\times$.

$\Rightarrow \Omega^\times \cap \mathbb{I}_K = K^\times$. So: $L^\times \cap \mathbb{I}_K \subseteq \Omega^\times \cap \mathbb{I}_K = K^\times$ ✓

Hence: Can embed $C_K \longrightarrow C_L$ for ANY L/K finite:

$$[\alpha]_{C_K} \mapsto [\alpha]_{C_L}$$

where $\alpha \in \mathbb{I}_K \subseteq \mathbb{I}_L$. [well-def'ed by Prop 20. & Injective]

$\Rightarrow$ Can view $C_K \leq C_L$ as Subgroup.

& $[\alpha]_{C_L}$ is in $C_K \iff [\alpha]$ contains representative $\alpha' \in \mathbb{I}_K$, such that $[\alpha]_{C_L} = [\alpha']_{C_K}$.

Prop 21 Let $G = Gal(L/K)$. Then, C_L is G-module, also with $C_L^G = C_K$.

This property is called Galois Descent.

$\sum_{\sigma \in G} f(\sigma)\sigma$

Theorem 22 [Hilbert, Theorem 90]

Let: $G = Gal(L/K)$ & $f: G \to K^*$, such that:

$f(\tau\sigma) = \tau(f(\sigma))\, f(\tau) \quad \forall \sigma, \tau \in G.$

Then, $\exists\, y \in K^*$, such that $f(\sigma) = \sigma(y)/y. \quad \forall \sigma \in G.$

Proof (of Prop 21)

The G-module $\mathbb{I}_L$ contains L^* as subgroup, as G-module.

$\Rightarrow \forall \sigma \in G$, it induces Auto $C_L \xrightarrow{\sigma} C_L$, $[\alpha] \mapsto [\sigma\alpha]$.

$\Rightarrow$ Have Exact sequence of G-modules:

$$1 \to L^* \to \mathbb{I}_L \to C_L \to 1$$

Show that the following is still exact:

$$1 \to (L^*)^G \to \mathbb{I}_L^G \to C_L^G \to 1.$$

* Easy: $(L^*)^G \to \mathbb{I}_L^G$ is injective.
* Kernel of $\mathbb{I}_L^G \to C_L^G$ is exactly: $\mathbb{I}_L^G \cap L^*$
  $= \mathbb{I}_K \cap L^* = K^* = (L^*)^G$.
* To show $\mathbb{I}_L^G \to C_L^G$ Surjective:

  Consider $[\alpha] \in C_L^G$. $\Rightarrow \forall \sigma \in G$, $[\sigma\alpha] = [\alpha]$.

  $\Rightarrow \exists\, x_\sigma \in L^*$, s.t. $\sigma\alpha = \alpha \cdot x_\sigma$

Then, x_σ is "Crossed Homomorphism", i.e. $x_{\sigma\tau} = \sigma(x_\tau)\, x_\sigma$

Since: $\chi_{\tau\sigma} = \frac{(\tau\sigma)\alpha}{\alpha} = \frac{(\tau\sigma)\alpha}{\tau\alpha}\frac{\tau\alpha}{\alpha} = \tau\left(\frac{\sigma\alpha}{\alpha}\right)\frac{\tau(\alpha)}{\alpha}$

$= \tau(\chi_\sigma)\chi_\tau$.

By Hilbert 90: $\chi_\sigma = \sigma(y)/y$, some $y \in L^\times$.

Denote: $\alpha' = \alpha y^{-1}$. $\Rightarrow [\alpha] = [\alpha']$.

$\Rightarrow \sigma(\alpha') = \sigma(\alpha)\sigma(y^{-1}) = \alpha\chi_\sigma\sigma(y^{-1})$

$= \alpha\left(\frac{\sigma(y)}{y}\right)\sigma(y^{-1}) = \alpha y^{-1} = \alpha'$.

$\Rightarrow \alpha' \in \Pi_L^G$. ✓

Algebraic NT: Lecture 21 | 06/03/2024

Let: L/K ext of NF's. Define: $N_{L/K}: \mathbb{I}_L \to \mathbb{I}_K$ by:

$$N_{L/K}(\alpha)_{\mathfrak{p}} = \prod_{P|\mathfrak{p}} N_{L_P/K_{\mathfrak{p}}}(\alpha_P)$$

where (recall): $N_{L_P/K_{\mathfrak{p}}}: L_P \to K_{\mathfrak{p}}$ is determinant of mult (x). $\forall x \in L_P$.

Prop 23 1) If $K \subseteq L \subseteq M$ then: $N_{M/K} = N_{L/K} \circ N_{M/L}$

2) $N_{L/K}(\alpha) = \alpha^{[L:K]}$ $\forall \alpha \in \mathbb{I}_K \subset \mathbb{I}_L$

3) If $K \subseteq L \subseteq M$ & M/K Galois, then, if $G = Gal(M/K)$, $H = Gal(M/L)$

$\Rightarrow \forall \alpha \in \mathbb{I}_L$, $N_{L/K}(\alpha) = \prod_{\sigma \in G/H} \sigma(\alpha)$

4)
$$\begin{array}{ccc} \mathbb{I}_L & \xrightarrow{N_{L/K}} & \mathbb{I}_K \\ \uparrow & & \uparrow \\ L^\times & \xrightarrow{N_{L/K}} & K^\times \end{array}$$

Commutes.

$$\left[L \otimes_K K_{\mathfrak{p}} \cong \prod_{P|\mathfrak{p}} L_P \right]$$

---

4) implies that $\exists$ Map $N_{L/K}: C_L \to C_K$.

§: Statements of CFT

Theorem 24 [Artin Reciprocity II].

L/K Finite Galois. Then, $\exists$ Canonical Isomorphism:

$r_{L/K} : Gal(L/K)^{ab} \xrightarrow{\cong} \frac{C_K}{N_{L/K} C_L}$. "Reciprocity map".

& $r_{L/K}^{-1}$ induces $\boxed{(\cdot, L/K)} : C_K \longrightarrow Gal(L/K)^{ab}$

is the Norm Residue Symbol (Kernel $N_{L/K}(C_L)$).

Theorem 25] [Existence Theorem]

$\exists$ Inclusion-reversing Bijection:

$$\left\{ \begin{matrix} L/K \text{ Finite} \\ \text{Extension} \end{matrix} \right\} \longleftrightarrow \left\{ \begin{matrix} \text{Finite index closed} \\ \text{subgroups of } C_K \end{matrix} \right\}.$$

$$L \longmapsto N_{L/K}(C_L) \subseteq C_K. \quad (= N_L)$$

[Proof Omitted]

For $N \subset C_K$ closed & Finite index, the corresponding Abelian ext L/K is: the Class Field of N.

DEF 26] Let $\underline{m}$ modulus. The Class Field $K^{\underline{m}}$ for the Congruence subgroup of $C_K(\underline{m})$ is called the Ray Class Field, of modulus $\underline{m}$.

$\Rightarrow \exists$ Isom. $Gal(K^{\underline{m}}/K) \cong C_K / C_K(\underline{m})$.

Example] $K = \mathbb{Q}$, $\underline{m} = m\infty$. $\Rightarrow K^{\underline{m}} = \mathbb{Q}(\xi_m)$.

Note 1) $\underline{m} \mid \underline{m}' \Rightarrow K^{\underline{m}} \subseteq K^{\underline{m}'}$

2) $\exists$ bijection:

$\left\{\begin{matrix}\text{Closed Subgroups of} \\ \text{Finite idx in } C_K\end{matrix}\right\} \overset{1\text{-}1}{\longleftrightarrow} \left\{\begin{matrix}H \subseteq C_K, \text{ containing} \\ C_K(\underline{m}), \text{ some } \underline{m}\end{matrix}\right\}$.

Corollary 27 Any finite Abelian L/K is contained in some Ray class field, $L \subseteq K^{\underline{m}}$.

DEF 28 Subgroup $N \leq C_K$ *Norm Subgroup* if: $\exists L/K$ Finite Galois, $N_{L/K}(C_L) = N$.

Theorem 29 L/K Finite, Galois & $L^{ab} \subseteq L$ maximal Abelian ext of $K \subseteq L$. Then: $\boxed{N_{L^{ab}/K} C_{L^{ab}} = N_{L/K} C_L}$.

Proof $K \subseteq L^{ab} \subseteq L$. $\Rightarrow N_{L/K} C_L \subseteq N_{L^{ab}/K} C_{L^{ab}}$.

By 2nd Artin Reciprocity, have Isomorphism:

$$C_K / N_{L/K} C_L \cong Gal(L/K)^{ab} \cong Gal(L^{ab}/K) \cong \frac{C_K}{N_{L^{ab}/K} C_{L^{ab}}}$$

$$\Rightarrow [C_K : N_{L/K} C_L] = [C_K : N_{L^{ab}/K} C_{L^{ab}}].$$

$$\Rightarrow N_{L/K} C_L = N_{L^{ab}/K} C_{L^{ab}} \checkmark$$

Corollary 30 $[C_K : N_{L/K} C_L] \mid [L:K]$, and has equality $\Leftrightarrow L/K$ Abelian.

Prop 31 Norm groups are precisely: closed subgroups of C_K of finite index.

Proof [Sketch]. For L/K Finite Galois, by Artin Reciprocity $\sqrt{3}$

$N_{L/K} C_L$ Finite index (in C_K) & $[C_K : N_{L/K}(C_L)] = |\mathrm{Gal}(L/K)^{ab}|$

By Prop 14: $C_K \cong C_K^0 \times r_K$ & $C_L \cong C_L^0 \times r_L$.

With: $r_K \cong (\mathbb{R}_+, \times)$ & $r_L \cong (\mathbb{R}_+, \times)$.

Here, r_K is image, of: $(\mathbb{R}_+, \times) \to K_f \to \mathbb{I}_K \to C_K$,

for some infinite prime f.

~~representatives~~ representations for quotient $N: C_K \to \mathbb{R}_+^\times$.

$\Rightarrow$ Gives

$\Rightarrow$ r_K also gives ~~representatives~~ representations for quotient $N: C_L \to \mathbb{R}_+^\times$.

Thus: $C_L \cong C_L^0 \times r_K$

$\Rightarrow N_{L/K} C_L \cong N_{L/K} C_L^0 \times N_{L/K} r_K = N_{L/K} C_L^0 \times r_K^n$

$= N_{L/K} C_L^0 \times r_K$.

Now: $N_{L/K}$ Continuous

$\Rightarrow$ ~~$N_{L/K}$~~ $N_{L/K}(C_0)$ Compact $\Rightarrow$ closed, so $N_{L/K}(C_L)$ closed ✓

Theorem 32 [Decomposition Law II].

Let: L/K Abelian, degree n. & $\mathfrak{f} \subset \mathcal{O}_K$ Unram prime.

If $\pi \in K_\mathfrak{f}$ Uniformiser & $n_\mathfrak{f}(\pi) \in C_K$ Idele class rep.

by $n_\mathfrak{f}(\pi) = (1, \dots, \underset{\mathfrak{f}^{th}\text{ comp.}}{\pi}, \dots, 1)$

& f smallest number with $n_\mathfrak{f}(\pi)^f \in N_{L/K} C_L$.

Then: $\mathfrak{f}\mathcal{O}_L = P_1 \cdots P_r$, where $r = \frac{n}{f}$ & P_i distinct (degree f).

Proof: Later! [using Compatibility of local Artin map.]

Theorem 33 $\mathfrak{f} \subseteq \mathcal{O}_K$ unram in $L \Leftrightarrow U_\mathfrak{f} \subseteq N$ split completely in $L \Leftrightarrow K_\mathfrak{f}^\times \subseteq N$.] L/K Abelian $N = N_{L/K} C_L$

Algebraic NT: Lecture 22 | 13/03/2024

From last time: Global statements of CFT (Quotient) & idele-theoretic.

Let: K NF & $\underline{m}$ modulus of K, $\underline{m} = \prod_{\mathfrak{p}} \mathfrak{p}^{n_{\mathfrak{p}}}$.

Prop 34) The map $(\cdot): \mathbb{I}_K \longrightarrow I_K$

$$\alpha \longmapsto (\alpha) \equiv \prod_{\mathfrak{p} \nmid \infty} \mathfrak{p}^{v_{\mathfrak{p}}(\alpha_{\mathfrak{p}})}$$

induces Isomorphism: $\overline{(\cdot)}_{\underline{m}} : C_K / C_K(\underline{m}) \longrightarrow I_K(\underline{m}) / P_K(\underline{m})$.

Proof) Recall: $C_K = \mathbb{I}_K / K^*$ & $C_K(\underline{m}) = \mathbb{I}_K^{(\underline{m})} K^* / K^*$.

$\Rightarrow C_K / C_K(\underline{m}) \cong \mathbb{I}_K / \mathbb{I}_K(\underline{m}) K^*$.

So, need: $\forall \alpha$ idele class mod $\mathbb{I}_K(\underline{m}) K^*$: some representative α, mapped to $I_K(\underline{m})$ under $(\cdot)$.

Use: Approximation Theorem.

Find: $x \in K^*$, s.t. $\alpha_{\mathfrak{p}} \cdot x \equiv 1 \bmod \mathfrak{p}^{n_{\mathfrak{p}}} \quad \forall \mathfrak{p} \mid \underline{m}$

$\Rightarrow \alpha \cdot x = \alpha' \cdot \beta$, where: $\alpha'_{\mathfrak{p}} = 1 \quad \forall \mathfrak{p} \mid \underline{m}$

~~$\alpha'_{\mathfrak{p}} = \alpha_{\mathfrak{p}} x \quad \forall \mathfrak{p} \nmid \underline{m}$~~

and: ~~$\beta_{\mathfrak{p}} = \alpha_{\mathfrak{p}} x$ for $\mathfrak{p} \mid \underline{m}$~~, $\beta_{\mathfrak{p}} = \alpha_{\mathfrak{p}} x \equiv 1 \bmod \mathfrak{p}^{n_{\mathfrak{p}}}$

$\beta_{\mathfrak{p}} = 1$ for $\mathfrak{p} \nmid \underline{m}$.

$\Rightarrow \alpha' \in \mathbb{I}_K^{\langle m \rangle} \equiv \{\alpha \in \mathbb{I}_K : \alpha_{\mathfrak{p}} = 1 \ \forall \ \mathfrak{p} \mid \underline{m}\}$

$\beta \in \mathbb{I}_K(\underline{m})$.

Hence, $\alpha \in \mathbb{I}^{\langle \mathfrak{m} \rangle} \mathbb{I}_K(\mathfrak{m}) K^\times$.

$$\Rightarrow C_K / C_K(\mathfrak{m}) \cong \mathbb{I}_K / \mathbb{I}_K(\mathfrak{m}) K^\times \cong \frac{\mathbb{I}^{\langle \mathfrak{m} \rangle} \mathbb{I}_K(\mathfrak{m}) K^\times}{\mathbb{I}_K(\mathfrak{m}) K^\times}$$

$$\cong \frac{\mathbb{I}_\phi^{\langle \mathfrak{m} \rangle}}{\mathbb{I}^{\langle \mathfrak{m} \rangle} \cap \mathbb{I}_K(\mathfrak{m}) K^\times}$$

By def. of $\mathbb{I}^{\langle \mathfrak{m} \rangle}$: $\exists$ Surj. hom. $\mathbb{I}^{\langle \mathfrak{m} \rangle} \longrightarrow I_K(\mathfrak{m}) / P_K(\mathfrak{m})$

with Kernel $\mathbb{I}^{\langle \mathfrak{m} \rangle} \cap \mathbb{I}_K(\mathfrak{m}) K^\times$. $\quad \alpha \longmapsto (\alpha) \bmod P_K(\mathfrak{m})$

$\Rightarrow C_K / C_K(\mathfrak{m}) \cong I_K(\mathfrak{m}) / P_K(\mathfrak{m})$ ✓ $\quad \mathfrak{f}_{L/K} \mid \mathfrak{m}$.

Prop 35 | L/K Abelian ext. The Restriction to $N_{L/K} C_L / C_K(\mathfrak{m})$ of isomorphism of Prop 34 gives:

Isomorphism $\overline{(\cdot)}_{\mathfrak{m}} : \dfrac{N_{L/K} C_L}{C_K(\mathfrak{m})} \xrightarrow{\cong} \dfrac{T_{L/K}(\mathfrak{m})}{P_K(\mathfrak{m})}$

[~~where, recall, $T_{L/K}(\mathfrak{a}) = P_K(\mathfrak{a}) N_{L/K}(I_L(\mathfrak{m}))$~~]

Proof | Let $\mathbb{I}_L^{\langle \mathfrak{m} \rangle} = \{ \alpha \in \mathbb{I}_L : \alpha_\mathfrak{p} = 1 \ \forall \mathfrak{p} \mid \mathfrak{m} \}$

Similar to proof of Theorem 34: $\mathbb{I}_L = \mathbb{I}_L^{\langle \mathfrak{m} \rangle} \mathbb{I}_L(\mathfrak{m}) L^\times$

$$\Rightarrow \frac{N_{L/K} C_L}{C_K(\mathfrak{m})} = \frac{N_{L/K} \mathbb{I}_L K^\times}{\mathbb{I}_K(\mathfrak{m}) K^\times} = \frac{[N_{L/K} \mathbb{I}_L^{\langle \mathfrak{m} \rangle}] \mathbb{I}_K(\mathfrak{m}) K^\times}{\mathbb{I}_K(\mathfrak{m}) K^\times}$$

& The isomorphism from Prop 34:

$$\overline{(\cdot)}_{\mathfrak{m}} : C_K / C_K(\mathfrak{m}) = \frac{\mathbb{I}_K^{\langle \mathfrak{m} \rangle} \mathbb{I}_K(\mathfrak{m}) K^\times}{\mathbb{I}_K(\mathfrak{m}) K^\times} \cong I_K(\mathfrak{m}) / P_K(\mathfrak{m})$$

$\square$

associates: to each class $\alpha \in I_K^{\langle m \rangle}$, the class of ideal $(\alpha) = \prod_{\mathfrak{p} \nmid \infty} \mathfrak{p}^{v_{\mathfrak{p}}(\alpha_{\mathfrak{p}})} \in I_K(\underline{m})$.

& Elements of $N_{L/K} C_L / C_K(\underline{m})$ are: classes represented by: norm idele $N_{L/K} I_L^{\langle m \rangle} \subset I_K^{\langle m \rangle}$

These are mapped to: class of norm ideals $N_{L/K}(I_L(\underline{m})) \subset I_K(\underline{m})$.

$\Rightarrow$ Image of $N_{L/K} C_L / C_K(\underline{m})$ under $(\cdot)$ is $N_{L/K}(I_L(\underline{m})) P_K(\underline{m}) / P_K(\underline{m})$ ✓

The isom. $\overline{(\cdot)}_{\underline{m}} : C_K / C_K(\underline{m}) \longrightarrow I_K(\underline{m}) / P_K(\underline{m})$

gives Surjective hom. $(\cdot)_{\underline{m}} : C_K \longrightarrow I_K(\underline{m}) / P_K(\underline{m})$

with Kernel $C_K(\underline{m})$.

Since $I_K(\underline{m})$ ~~Biangen~~; by prime ideals $\mathfrak{p} \nmid \underline{m}$, we can describe $(\cdot)_{\underline{m}}$.

Let: $\underline{m}$ modulus, $\mathfrak{p} \nmid \underline{m}$ prime & $\pi \in K_{\mathfrak{p}}$ Unif.

& ~~$n_{\mathfrak{p}}(\pi) = (\ldots, 1, 1, \pi, 1, 1, \ldots)$~~.

↑ p'th coord

Then: $(\cdot)_{\underline{m}}$ takes: $n_{\mathfrak{p}}(\pi) \longmapsto$ Class of $\mathfrak{p}$ mod $P_K(\underline{m})$,

since: $(\!(n_{\mathfrak{p}}(\pi))\!) = \mathfrak{p}$.

Theorem 36 [Compatibility of 2 versions, Artin Recip. ($\mathfrak{f}_{L/K} \mid \mathfrak{m}$)]

Let: L/K Abelian, $\mathfrak{m}$ modulus of K, with $\mathfrak{f}_{L/K} \mid \mathfrak{m}$.

~~Let: $T_{L/K}(\mathfrak{m}) = N_{L/K}(I_L(\mathfrak{m}))P_K(\mathfrak{m})$.~~

Then: have following exact Commutative Diagram:

$$\begin{array}{ccccccccc} 1 & \to & N_{L/K}C_L & \to & C_K & \to & Gal(L/K) & \to & 1 \\ & & \downarrow (\cdot)_{\mathfrak{m}} & & \downarrow (\cdot)_{\mathfrak{m}} & & \downarrow id & & \\ 1 & \to & T_{L/K}(\mathfrak{m})/P_K(\mathfrak{m}) & \to & I_K(\mathfrak{m})/P_K(\mathfrak{m}) & \xrightarrow[\Phi_{\mathfrak{m}}]{(L/K)\cdot} & Gal(L/K) & \to & 1 \end{array}$$

Where: both $(\cdot)_{\mathfrak{m}}$'s are Surjective & Kernel $C_K(\mathfrak{m})$.

Overview of Local CFT.

Goal: Classify Finite, Abelian exts of local fields K.

Usually, finite exts of $\mathbb{Q}_p$, or $\mathbb{R}, \mathbb{C}$ (for us).

Let: K Local field, K^{sep}/K fixed Separable closure & K^{ab} = Maximal Abelian ext of $K \subset K^{sep}$.

$$\Rightarrow K^{ab} = \bigcup_{L \subset K^{sep}} L$$

L/K Finite Abelian.

Theorem 37 [Local Artin Reciprocity].

Let: K local field. Then, $\exists!$ Continuous hom

$$\theta_K : K^\times \longrightarrow Gal(K^{ab}/K)$$

with property that: $\forall L/K$ finite ext in K^{sep}, the hom. $\theta_{L/K} : K^\times \to Gal(L/K)$, given by composing θ_K with $Gal(K^{ab}/K) \twoheadrightarrow Gal(L/K)$, satisfies:

* If K non-Arch & L/K Unram $\Rightarrow \theta_{L/K}(\pi) = Frob_{L/K}$ for Any π uniformizer.
* The map $\theta_{L/K}$ Surjective, kernel $N_{L/K}(L^\times)$

$\Rightarrow$ Induces isom. $\boxed{K^\times/N_{L/K}(L^\times) \xrightarrow[\theta_{L/K}]{\cong} Gal(L/K).}$

Note: If L/K Unramified, then ~~k_L, k_K residue fields~~

$\Rightarrow Gal(L/K) \cong Gal(k_L/k_K)$.

& $Frob_{L/K}$ is Pre-image of $Frob \in Gal(k_L/k_K)$.

There is no analogue of moduli: $\Rightarrow$ deal with all Abelian exts, all at once. We replace quotients of Idele class groups by quotients of $K^\times$.

Corollary 38 The map $L \longrightarrow N_{L/K}(L^\times)$ defines inclusion-reversing bijection between:

$$\left\{\begin{array}{c}\text{Finite Abelian exts} \\ \text{of } L/K \text{ in } K^{ab}\end{array}\right\} \longleftrightarrow \left\{\begin{array}{c}\text{Norm groups} \\ \text{in } K^\times\end{array}\right\}.$$

& Every norm group of K has finite index in $K^\times$.

[In local setting: Norm group is Subgroup of $K^\times$, of form $N_{L/K}(L^\times)$, for L/K finite Abelian]

Theorem 39] [Local Existence Theorem].

Let: K Local field & H Finite index open subgroup of $K^\times$. Then: $\exists!$ ~~Isom~~. $L/K \subset K^{ab}/K$, with: $N_{L/K}(L^\times) = H$.

Next: Compatibility of Global CFT with local CFT.

Let: K NF, L/K Galois & $\mathfrak{p} \subset \mathcal{O}_K$, $\mathfrak{P} \subset \mathcal{O}_L$, $\mathfrak{P}|\mathfrak{p}$.

Recall: $\exists$ Embedding $\mathrm{Gal}(L_{\mathfrak{P}}/K_{\mathfrak{p}}) \hookrightarrow \mathrm{Gal}(L/K)$.

Algebraic NT: Lecture 23 | 13/03/2024

Today: Compatibility of Local & Global CFT.
& give: 2 versions of Artin recip.

Let: K NF, $\mathfrak{p} \subset \mathcal{O}_K$ prime ideal. Then, $\exists$ injection:
$\overline{n_{\mathfrak{p}}(\cdot)} : K_{\mathfrak{p}}^{\times} \hookrightarrow C_K$, by $\alpha_{\mathfrak{p}} \mapsto \overline{n_{\mathfrak{p}}(\alpha_{\mathfrak{p}})}$.

$[n_{\mathfrak{p}}(\alpha_{\mathfrak{p}}) = (\dots, 1, 1, \alpha_{\mathfrak{p}}, 1, 1, \dots)]$

Prop 40 Let L/K Abelian & $\mathfrak{P} \subset \mathcal{O}_L$, $\mathfrak{p} \subset \mathcal{O}_K$, $\mathfrak{P} \mid \mathfrak{p}$.
Then $\exists$ Commutative diagram:

$$\begin{array}{ccc} K_{\mathfrak{p}}^{\times} & \xrightarrow{(\cdot, L_{\mathfrak{P}}/K_{\mathfrak{p}})} & Gal(L_{\mathfrak{P}}/K_{\mathfrak{p}}) \\ \downarrow \overline{n_{\mathfrak{p}}(\cdot)} & & \downarrow \\ C_K & \xrightarrow{(\cdot, L/K)} & Gal(L/K) \end{array}$$

Corollary 41 L/K Abelian, $\alpha = (\alpha_{\mathfrak{p}}) \in \mathbb{I}_K$. Then:

$$(\alpha, L/K) = \prod_{\mathfrak{p}} (\alpha_{\mathfrak{p}}, L_{\mathfrak{P}}/K_{\mathfrak{p}}).$$

& For principal idele $x \in K^{\times}$, Product Formula

$$\prod_{\mathfrak{p}} (x, L_{\mathfrak{P}}/K_{\mathfrak{p}}) = 1.$$

Note that $(\alpha_{\mathfrak{p}}, L_{\mathfrak{P}}/K_{\mathfrak{p}}) \in Gal(L_{\mathfrak{P}}/K_{\mathfrak{p}}) \subset Gal(L/K)$, and $\alpha_{\mathfrak{p}}$ are units for almost all $\mathfrak{p}$, and the extensions $L_{\mathfrak{P}}/K_{\mathfrak{p}}$ are almost always unramified. So, the local

the local norm residue symbols are almost always 1
⇒ Product is well-defined.

Also: $D_{\mathfrak{P}|\mathfrak{p}} \cong \mathrm{Gal}(L_{\mathfrak{P}}/K_{\mathfrak{p}})$, and if $L_{\mathfrak{P}}/K_{\mathfrak{p}}$ unram, then $(\pi, L_{\mathfrak{P}}/K_{\mathfrak{p}}) = \mathrm{Frob}(L_{\mathfrak{P}}/K_{\mathfrak{p}}) = \left(\frac{L/K}{\mathfrak{p}}\right)$.

⇒ By Prop 40: $(\overline{n_{\mathfrak{p}}(\pi)}, L/K) = (\pi, L_{\mathfrak{P}}/K_{\mathfrak{p}}) = \left(\frac{L/K}{\mathfrak{p}}\right)$

Proof of Theorem 36 Consider:

$$\begin{array}{ccc} C_K/C_K(\mathfrak{m}) & \xrightarrow{(\cdot,\, L/K)} & \mathrm{Gal}(L/K) \\ \downarrow \overline{(\cdot)}_{\mathfrak{m}} & & \downarrow = \\ I_K(\mathfrak{m})/P_K(\mathfrak{m}) & \xrightarrow{f} & \mathrm{Gal}(L/K) \end{array}$$

If $\mathfrak{p} \subset \mathcal{O}_K$ & $\mathfrak{p} \nmid \mathfrak{m}$, and $\pi \in K_{\mathfrak{p}}$ unif, then: $\overline{(n_{\mathfrak{p}}(\pi))}_{\mathfrak{m}} = \mathfrak{p}$.
& $(\overline{n_{\mathfrak{p}}(\pi)}, L/K) = \left(\frac{L/K}{\mathfrak{p}}\right)$ (prop 40)

⇒ for $f = \left(\frac{L/K}{\cdot}\right)$, the square above commutes.

The remainder follows from Prop 34, 35 & Both versions of Artin Reciprocity. ✓

Theorem 42 [Decomposition Law, II]

Let: L/K Abelian, degree n. Let: $\mathfrak{p} \subset \mathcal{O}_K$ unram & $\pi \in K_{\mathfrak{p}}$ unif. Consider: $n_{\mathfrak{p}}(\pi) = (--, \underbrace{1, 1, \pi, 1, 1}_{f}, --)$
& $f \equiv$ Smallest number, with $\overline{n_{\mathfrak{p}}(\pi)}^{f} \in N_{L/K} C_L$.

Then, the prime $\mathfrak{p}$ factors in L into $r \equiv n/f$ distinct prime ideals $P_1, \dots, P_r$, each of degree f.

Proof] Since $\mathfrak{p}$ Unram: factors into distinct prime ideals in L, of equal degree, $\mathfrak{p}\mathcal{O}_L = P_1 \cdots P_r$.

By Reciprocity Law: $C_K / N_{L/K} C_L \cong Gal(L/K)$.

$\Rightarrow \overline{n_{\mathfrak{p}}(\pi)}$ mod $N_{L/K} C_L$ in $C_K / N_{L/K} C_L$ has: Same order (f) as $(\overline{n_{\mathfrak{p}}(\pi)}, L/K)$

& as $(\overline{n_{\mathfrak{p}}(\pi)}, L/K) = (\pi, L_{\mathfrak{p}}/K_{\mathfrak{p}}) \in Gal(L_{\mathfrak{p}}/K_{\mathfrak{p}}) \subset Gal(L/K)$.

& $(\pi, L_{\mathfrak{p}}/K_{\mathfrak{p}}) = Frob_{L_{\mathfrak{p}}/K_{\mathfrak{p}}}$

and, since $L_{\mathfrak{p}}/K_{\mathfrak{p}}$ unramified, Frob generates $Gal(L_{\mathfrak{p}}/K_{\mathfrak{p}})$ and so the order f coincides with degree $[L_{\mathfrak{p}} : K_{\mathfrak{p}}]$, which is the degree of P.

$\Rightarrow r = \#$ distinct prime ideals over $\mathfrak{p}$ satisfies: $n = rf$ ✓

Important: For proof of CFT, need Cohomology.

Let: G finite group & A ~~some~~ G-module. The Cohomology groups $H^q(G, A)$, $q \in \mathbb{Z}$, where.

⊛ $H^0(G, A) = A^G / N_G A$, where

$A^G = \{a \in A : \sigma a = a \ \forall \sigma \in G\}$ fixed group

& $N_G(A) = \{$

$$H^1(G,A) = \frac{\{\chi : G \to A : \chi(\sigma\tau) = \sigma(\chi(\tau)) + \chi(\sigma)\}}{\{\chi_a : G \to A : \chi(\sigma) = \sigma(a) - a, \text{ fixed } a \in A\}}.$$

$\Rightarrow$ Have seen Hilbert 90: if L/K Galois, then $H^1(\mathrm{Gal}(L/K), L^\times) = 1$.

Cohomology of the Idele Group.

Let: L/K Galois, $G = \mathrm{Gal}(L/K)$. S = finite set of primes of K & $\mathbb{I}_L^S = \prod_{\mathfrak{P}\mid\mathfrak{p}\in S} L_{\mathfrak{P}} \times \prod_{\mathfrak{P}\mid\mathfrak{p}\notin S} U_{\mathfrak{P}}$.

Consider: $\mathbb{I}_L^{\mathfrak{p}} \equiv \prod_{\mathfrak{P}\mid\mathfrak{p}} L_{\mathfrak{P}}^\times$ & $U_L^{\mathfrak{p}} \equiv \prod_{\mathfrak{P}\mid\mathfrak{p}} U_{\mathfrak{P}}$, as subgroups of $\mathbb{I}_L^S$.

If $\alpha \in \mathbb{I}_L^{\mathfrak{p}}$, this has component 1 at all primes not above $\mathfrak{p}$

& Same for $U_L^{\mathfrak{p}}$, and in addition: only units at components lying above $\mathfrak{p}$.

These $\mathbb{I}_L^{\mathfrak{p}}$, $U_L^{\mathfrak{p}}$ are G-modules and product of G-mods:

$$\mathbb{I}_L^S = \prod_{\mathfrak{p}\in S} \mathbb{I}_L^{\mathfrak{p}} \times \prod_{\mathfrak{p}\notin S} U_L^{\mathfrak{p}}.$$

Theorem 42 1) $H^q(G, \mathbb{I}_L^{\mathfrak{p}}) \cong H^q(D_{\mathfrak{P}\mid\mathfrak{p}}, L_{\mathfrak{P}}^\times)$

& If $\mathfrak{p}$ unramified then $H^q(G, U_L^{\mathfrak{p}}) = 1$

2) Suppose S contains all ram primes. Then:

$$H^q(G, \mathbb{I}_L^S) \cong \prod_{\mathfrak{p}\in S} H^q(D_{\mathfrak{P}\mid\mathfrak{p}}, L_{\mathfrak{P}}^\times)$$

& $H^q(G, \mathbb{I}_L) \cong \bigoplus_f H^q(D_{P|f}, L_P^\times)$.

Norm Theorem for ideles:

Corollary 43] An idele $\alpha \in \mathbb{I}_K$ is the Norm of some $\beta \in \mathbb{I}_L$ iff each $\alpha_f \in K_f^\times$ is norm of some $\beta_f \in L_P^\times$ for some $P|f$. ($\Leftrightarrow$ norm of some $\beta_P \in L_P^\times$ for ANY $P|f$) ($\Leftarrow$ Has a Local norm, everywhere.)

Use: Theorem 42, for $q=0$, & explicit description of $H^q(G, \mathbb{I}_L) \cong \bigoplus_f H^q(D_{P|f}, L_P^\times)$:

Proof) [

Note: $H^0(G, \mathbb{I}_L) = \mathbb{I}_L^G / N_G(\mathbb{I}_L) = \mathbb{I}_K / N_G(\mathbb{I}_L)$

& $H^0(D_{P|f}, L_P^\times) = K_f^\times / N_{D_{P|f}}(L_P^\times)$.

By Theorem 42: $\mathbb{I}_K / N_G \mathbb{I}_L \cong \bigoplus_f K_f^\times / N_{D_{P|f}}(L_P^\times)$

For $\alpha \in \mathbb{I}_K$: isom. takes: its class, mod $N_G(\mathbb{I}_L)$, to its Components $\overline{\alpha_f}$ (Theorem 42).

& Have: $\overline{\alpha_f} \equiv \alpha_f \bmod N_{D_{P|f}}(L_P^\times)$.

& $\alpha = 1 \Leftrightarrow \overline{\alpha_f} = 1 \ \forall f$ (since have $\cong$)

$\Rightarrow \alpha \in N_G(\mathbb{I}_L) \Leftrightarrow \alpha_f \in N_{D_{P|f}} L_P^\times \ \forall f$.

Algebraic NT: Lecture 24* 15/03/2024

Overview of Proof of Artin Reciprocity.

Let: L/K Abelian, $\mathfrak{m}$ modulus of K div. by all ram primes, s.t. exponents of $\mathfrak{p} \mid \mathfrak{m}$ is sufficiently large.

Then: $\phi_{L/K,\mathfrak{m}} : I_K(\mathfrak{m}) \longrightarrow Gal(L/K)$ is Surjective, with Kernel $T_{L/K}(\mathfrak{m})$.

Steps). ⊛ Prove it for Cyclic extensions first.

⊛ In general: set $G = G_1 \times \cdots \times G_s$ & $L = E_1 \cdots E_s$ for $E_i = L^{H_i}$, and H_j is such that $G = G_j \times H_j$.

& Use properties of the Artin map.

Have already proven:

⊛ Artin map is Surjective

⊛ $[I_K(\mathfrak{m}) : T_{L/K}(\mathfrak{m})] \leq [L:K]$.

To prove Cyclic case: need to first show equality for

$[I_K(\mathfrak{m}) : T_{L/K}(\mathfrak{m})] = [L:K]$.

& Also need: if $\ker(\phi_{L/K,\mathfrak{m}}) \subseteq T_{L/K}(\mathfrak{m})$ then

$\ker(\phi_{L/K,\mathfrak{m}}) = T_{L/K}(\mathfrak{m})$.

Use fact that: $\ker(\phi_{L/K,\mathfrak{m}})$ & $T_{L/K}(\mathfrak{m})$ have same index in $I_K(\mathfrak{m})$, because $\phi_{L/K,\mathfrak{m}}$ is Surjective onto group, order $[L:K]$. ∎

Let: $h = [I_K(\underline{m}) : T_{L/K}(\underline{m})]$

then: $h = a(\underline{m})\, n(\underline{m})\, q(L^S)$, where: $[S = \{\mathfrak{p} \subset \mathcal{O}_K : \mathfrak{p} | \underline{m}_0\}]$

* $a(\underline{m}) = [K^\times : N(L^\times) K_{\underline{m},1}]$
* $n(\underline{m}) = [K_{\underline{m},1} \cap i^{-1}(N(I_L(\underline{m}))) : K_{\underline{m},1} \cap N(L^\times)]$

where (recall) $K_{\underline{m},1} = \{\alpha \in K^\times : \alpha \equiv 1 \bmod \underline{m}_0$ & $\sigma(\alpha) > 0 \ \forall \sigma | \underline{m}_\infty\}$

& $i : K^\times \longrightarrow P_K$,
$\alpha \longmapsto \mathcal{O}(\alpha)$ (ideal gen. by α)

$q(L^S)$ = Herbrand Quotient:

$L^S = \{\alpha \in L^\times : i(\alpha)$ div. by only primes in $S\}$

So, need: $h \geq [L:K]$.

Cohomology of Cyclic Groups.

Let: $G = Gal(L/K)$ & $\sigma \in G$ generator. (Order n)

Write: $\Delta \equiv 1 - \sigma$ & $N \equiv 1 + \sigma + \cdots + \sigma^{n-1}$.

Let: A be G-module, $\Delta(a) = a - \sigma(a)$ (or: $a/\sigma(a)$)

$N(a) = a + \sigma(a) + \cdots + \sigma^{n-1}(a)$

Can observe, $N\Delta = \Delta N = 0$, so $Im(N) \subset Ker(\Delta)$
$Im(\Delta) \subset Ker(N)$

DEF] $H^0(G,A) = Ker(\Delta)/Im(N)$

$H^1(G,A) = Ker(N)/Im(\Delta)$.

Properties If $f: A \to B$ hom. of G-modules, then there are homs $f_i: H^i(A) \to H^i(B)$, $i = 0, 1$ (or in general)

& If $0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$ Exact, then: $\exists \delta_0, \delta_1$

s.t. $$\begin{array}{ccccc} H^0(A) & \xrightarrow{f_0} & H^0(B) & \xrightarrow{g_0} & H^0(C) \\ & & & & \downarrow \delta_0 \\ H^1(C) & \xleftarrow{g_1} & H^1(B) & \xleftarrow{f_1} & H^1(A) \end{array}$$ $\delta_1 \uparrow$

Exact Hexagon.

DEF Let: A G-module. The Herbrand Quotient is:

$$q(A) \equiv \frac{|H^1(A)|}{|H^0(A)|}$$ (if both Finite, in which case say defined).

Lemma If $0 \to A \to B \to C \to 0$ Exact, and any 2 of $q(A), q(B), q(C)$ are defined, then All 3 are defined & satisfy $q(B) = q(A)q(C)$.

Let: m modulus div. by all Ram primes.

& Consider: I_L & $I_L(m)$ as G-modules, and: map

$$j_m: I_L \to I_L(m), \quad \mathfrak{p} \mapsto \begin{cases} \mathfrak{p} & \text{if } \mathfrak{p} \nmid m \\ 1 & \text{if } \mathfrak{p} \mid m \end{cases}$$

$$f_m: L^\times \to I_L(m), \quad f_m = j_m \circ i \Rightarrow L^S = \ker f_m$$

$\Rightarrow$ Exact sequence $1 \to L^S \to L^\times \xrightarrow{f_m} I_L(m) \to V \to 1$

(for some quotient group V that makes sequence exact).

Why $h = a(m)\, n(m)\, q(L^S)$??

Prop i) $H^0(I_L(\underline{m})) = I_K(\underline{m})/N(I_L(\underline{m}))$

ii) $H^1(I_L(\underline{m})) = 1$

iii) $H^0(L^\times) = K^\times/N(L^\times)$

iv) $H^1(L^\times) = 1$ [Hilbert Thm 90]

DEF If $g: A \to B$ hom, then $\mathrm{coker}(g) = B/\mathrm{im}(g)$.

Let diagram:

$$\begin{array}{ccccccccc}
 & & & & N(L^\times)K_{\underline{m}}/N(L^\times) & \to & T_{L/K}(\underline{m})/N(I_L(\underline{m})) & \to & X \to 1 \\
 & & & & \downarrow d_5 & & \downarrow d_6 & & \downarrow d_7 \\
1 & \to & \ker(f_0) & \to & H^0(L^\times) & \xrightarrow{f_0} & H^0(I_L(\underline{m})) & \to & \mathrm{coker}(f_0) \to 1 \\
 & & \downarrow d_1 & & \underset{K^\times/N(L^\times)}{\downarrow d_2} & & \underset{I_K(\underline{m})/N(I_L(\underline{m}))}{\downarrow d_3} & & \downarrow d_4 \\
1 & & \ker(g) & \to & K^\times/N(L^\times)K_{\underline{m},1} & \xrightarrow{g} & I_K(\underline{m})/T_{L/K}(\underline{m}) & \to & \mathrm{coker}(g) \to 1
\end{array}$$

Diagram Chase:

- $\mathrm{coker}(g) \cong \mathrm{coker}(f_0)$ [since $X = 1$]
- $|\ker(f_0)| = |\ker(g)| \cdot n(\underline{m})$
- $\dfrac{|\mathrm{coker}(f_0)|}{\ker(f_0)} = q(L^S)$ [Using Hexagon theorem]

$$\begin{aligned}
\& \; h &= |\mathrm{im}(g)|\,|\mathrm{coker}(g)| \\
&= a(\underline{m})\,\frac{|\mathrm{coker}(g)|}{|\ker(g)|} = a(\underline{m})\,n(\underline{m})\,\frac{|\mathrm{coker}(f_0)|}{|\ker(f_0)|}. \\
&= a(\underline{m})\,n(\underline{m})\,q(L^\times).
\end{aligned}$$

Next Show: $q(\mathcal{C}^S) = \dfrac{[L:K]}{\left(\prod_{\mathfrak{p}\mid \underline{m}_0} e_{\mathfrak{p}} f_{\mathfrak{p}}\right)\cdot 2^{r_0}}$, ($r_0$ = # Ramified infinite primes.

& $a(\underline{m}) = \left(\prod_{\mathfrak{p}\mid \underline{m}_0} e_{\mathfrak{p}} f_{\mathfrak{p}}\right) 2^{r_0}$

Together: $h = [L:K]\, n(\underline{m})$.

But: $h \le [L:K]$, hence, get $n(\underline{m}) = 1$ & $h = [L:K]$ ✓

Using $n(\underline{m}) = 1$, can show:

Hasse's Norm Theorem | If L/K Cyclic, then an element of K is a norm from $L \iff$ is Local norm at any prime.

Next need to show: $\ker(\Phi_{L/K,\underline{m}}) \subseteq T_{L/K}(\underline{m})$.

Use: $\ker(\Phi_{L/K,\underline{m}}) = T_{L/K}(\underline{m})$ in specific cases, e.g.

- $\mathbb{Q}(\xi_m)/\mathbb{Q}$
- If true for $(L/K, \underline{m})$ then true for $(EL/E, \underline{m}_E)$ for any E/K finite.
- If true for $(L/K, \underline{m})$ then true for $(L/K, \underline{m}\underline{n})$
- $K(\mathcal{O}_{\underline{m}})/K$ ($\underline{m} = m\infty$, extended to K) and any $K \subseteq E \subseteq K(\mathcal{O}_{\underline{m}})$.

Theorem [Artin's Lemma]
L/K Cyclic, $\mathfrak{p} \subset \mathcal{O}_K$ Unramified, $s \in \mathbb{N}_0$. Then: $\exists m \in \mathbb{N}$

coprime to S, and some ext F/K, such that:

1) $L \cap F = K$

2) $L \cap K(\xi_m) = K$

3) $L(\xi_m) = F(\xi_m)$.

4) $\mathfrak{p}$ splits completely in F.

All these can be Generalised to Abelian extensions.

Existence Theorem

- Reduction to some type of Congruence Subgroups
- Reduce to some ground field
- Show: If it holds for some field containing suitable roots of unity, then it's true for Any fields.
- Kummer Theory: L/K is a Kummer ext (n-ext) if: $Gal(L/K)$ has exponent n & K contains some primitive n^{th} root of unity.