# Class Field Theory

$K$ a number field $([K:\mathbb{Q}] < \infty)$.
$\bar{K}$ the algebraic closure of $K$.

$G_K = Gal(\bar{K}/K)$ (gal-group). It's a profinite group.

If $L/K$ is finite Galois, then $G_K \twoheadrightarrow Gal(L/K)$ by restriction.

(1954) Shafarevich: Fix $K$. Then any finite solvable group occurs as a Galois group of some $L/K$.

Open problem: Does every finite group $G$ occur as Galois group of some $L/K$? Fix $K$.

Class Field Theory: Describe the (finite) abelian extensions of $K$; i.e. $[L:K] < \infty$ normal and $Gal(L/K)$ is an abelian group.

-or-

Describe the maximal abelian quotient group of $G_K$.

(CFT) is also known for $K$ finite extensions of $\mathbb{F}_q(T)$.

Kronecker-Weber Thm: For $K = \mathbb{Q}$, let $L/\mathbb{Q}$ be a finite abelian extension. Then $\exists\, m \in \mathbb{Z}$ s.t. $L \subset \mathbb{Q}(\sqrt[m]{1})$.

For example, $L = \mathbb{Q}(\sqrt{p})$ $p$ odd prime, Then $L \subset \mathbb{Q}(\sqrt[p]{1})$ $(p \equiv 1\ (4))$ or $L \subset \mathbb{Q}(\sqrt[4p]{1})$ $(p \equiv 3\ (4))$.

Also, for $L/K$ abelian, want a rule for the decomposition of primes:
$\mathfrak{p}$ a prime ideal of $\mathcal{O}_K$. Then $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}$,
if $g = (L:K)$ then $\mathfrak{p}$ splits completely in $L$.

We'll see that $L/K$ abelian $\Leftrightarrow$ $\exists$ congruence criterion for decomposition of primes.

Example: $L = \mathbb{Q}(i)$, $p$ odd prime. Then $(p)$ splits completely $\Leftrightarrow p \equiv 1\ (4)$.
(So is the $p = x^2 + y^2$).

## Artin map

Provides an isomorphism btwn an object associated to $K$ and $Gal(L/K)$ ($L$ abelian).

- Finite fields.

$\mathbb{F}_q$, $q=p^a$, $p$ prime

Extensions of degree $f$: $\mathbb{F}_{q^f}/\mathbb{F}_q$. Know that $Gal(\mathbb{F}_{q^f}/\mathbb{F}_q)$ is cyclic of order $f$.

Also, there's a canonical generator $x \mapsto x^q$, $x \in \mathbb{F}_{q^f}$ (Frobenius automorphism).

Comments:

$(x+y)^q = x^q + y^q$ (char $K = p$).

Want to lift the Frobenius to characteristic 0.

Recall, $L/K$ Galois, finite. $\mathfrak{p}$ a prime of $\mathcal{O}_K$.

$p\mathcal{O}_L = (\mathfrak{P}_1 \cdots \mathfrak{P}_g)^e$, $f := (\mathcal{O}_L/\mathfrak{P} : \mathcal{O}_K/p)$. Then $e\cdot f\cdot g = (L:K)$

$G$ acts transitively on $S = \{\mathfrak{P}_1, \dots, \mathfrak{P}_g\}$ (Chinese RT argument).

The orbit/stabilizer formula is then:

$D_{\mathfrak{P}_i} := \{\sigma \in G : \sigma(\mathfrak{P}_i) = \mathfrak{P}_i\}$ (decomp. group of $\mathfrak{P}_i$).

$g = [G : D_{\mathfrak{P}_i}]$, so $|D_{\mathfrak{P}_i}| = e.f$ $\forall i$

Note also that $D_{\sigma\mathfrak{P}} = \sigma \mathfrak{P} \sigma^{-1}$.

Let also $I_{\mathfrak{P}} := \{\sigma \in D_p : \sigma\alpha \equiv \alpha \bmod \mathfrak{P} \ \forall \alpha \in \mathcal{O}\}$ (inertia subgroup of $\mathfrak{P}$).

Fix now $\mathfrak{P}$ of $L$ above $p$ of $K$. Have an inclusion $\mathcal{O}_K/p \hookrightarrow \mathcal{O}_L/\mathfrak{P}$.

Denote $\bar{k} := \mathcal{O}_K/p$, and $\bar{L} := \mathcal{O}_L/\mathfrak{P}$.

Suppose that $\sigma \in G$ and $\sigma(\mathfrak{P}) = \mathfrak{P}$ (i.e. $\sigma \in D_{\mathfrak{P}}$).

Then $\sigma$ defines a $\bar{K}$-aut of $\bar{L}$, by $\sigma(\alpha \bmod \mathfrak{P}) := \sigma(\alpha) \bmod p$

So $D_{\mathfrak{P}}$ acts on $\bar{L} = \mathcal{O}_L/\mathfrak{P}$.

Theorem: L/K a finite Galois extension. We have an exact sequence:
(0.1)

$$1 \to I_{\mathfrak{P}} \to D_{\mathfrak{P}} \xrightarrow{\varphi} Gal(\bar{L}/\bar{K}) \to 1$$
$$\sigma \mapsto \bar{\sigma}$$

Pf Show $\varphi$ is onto later.

Corollary: $|I_{\mathfrak{P}}| = e$ and $I_{\mathfrak{P}} \triangleleft G_{\mathfrak{P}}$, with cyclic quotient of order $f$.

Corollary: Suppose $e = 1$. ($I_{\mathfrak{P}}$ trivial). Then $D_{\mathfrak{P}} \cong Gal(\bar{L}/\bar{K})$. (cyclic).

From this, $\exists$ a unique element $\Phi_{\mathfrak{P}} \in D_{\mathfrak{P}}$ (generator) satisfying

$$\alpha^{\Phi_{\mathfrak{P}}} = \alpha^{q} \mod \mathfrak{P}, \quad \text{for } \alpha \in \mathcal{O}_L$$

$(q = |\bar{K}| = |\mathcal{O}_K/\mathfrak{p}| = N_{K/\mathbb{Q}}(\mathfrak{p}))$. (and note $\Phi_{\sigma\mathfrak{P}} = \sigma \Phi_{\mathfrak{P}} \sigma^{-1}$)

Suppose now L/K abelian. (still suppose $e=1$).
Then $\Phi_{\mathfrak{P}_i} = \Phi_{\mathfrak{P}_i}$ for all primes of L above $\mathfrak{p}$.

The Artin symbol is (def): $(\mathfrak{p}, L/K) = \Phi_{\mathfrak{P}}$ if $\mathfrak{P}$ over $\mathfrak{p}$.

Let $I_K$ := group of fractional ideals of K. (L/K abelian).
$I'_K$ := throw out those prime ideals ramified in L.

Then we have the Artin map $\omega_{L/K} : I'_K \to Gal(L/K)$.
defined as, $I = \prod_i \mathfrak{p}_i^{a_i}$ $(a_i \in \mathbb{Z})$ $\Rightarrow$ $\omega_{L/K}(I) = \prod_i (\mathfrak{p}_i, L/K)^{a_i}$.
↑ order is ok because $Gal(L/K)$ is abelian.

Facts:
1) Surjective
2) Ker $\omega_{L/K}$ can be described.

This will allow us to get a correspondence between finite abelian extensions of K and certain quotients of $I_K$.

## History

1920. Takagi got isomorphisms without the Artin map.

1927: Emil Artin proved reciprocity. (analytic)

1936: Chevalley introduced ideles.

1950's: Artin-Tate notes on CFT and cohomology of finite gps. (no analysis)

1960's: Lubin-Tate: explicit local reciprocity by formal groups.

More recent: modular forms, Galois representations ⇒ non-abelian CFT.

Example: $K=\mathbb{Q}(\zeta)$ where $\zeta=\zeta_m$ a primitive root of 1. ($m$ odd or $4|m$).

- $\mathrm{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/m\mathbb{Z})^{\times}$ where $\zeta^{\sigma_a}=\zeta^a$ $(a,m)=1$.

  $\sigma_a \longmapsfrom a \bmod m$

$p$ ramifies ⇔ $p|m$, so sps $p\nmid m$ and

$p\mathcal{O}_L = \mathfrak{P}_1 \cdots \mathfrak{P}_g$, $fg=\phi(m)$.

Let $\sigma$ be the Artin symbol $((p), L/\mathbb{Q})$, which sends $\zeta\mapsto\zeta^p$ $(p\nmid m)$.

$\sigma$ generates $D_{\mathfrak{p}}$, of order $f$.

Hence, $f$ is the smallest positive integer s.t. $p^f\equiv 1$ $(m)$.

More generally, take $(a)$ where $(a,m)=1$ ($a$ be a positive integer)

$((a), L/\mathbb{Q})$ sends $\zeta\mapsto\zeta^a$

And even more,

$((\frac{a}{b}), L/\mathbb{Q})$ sends $\zeta\mapsto\zeta^{ab^*}$ where $\left|\begin{array}{l} ab>0 \\ (ab,m)=1 \\ bb^*\equiv 1\ (m)\end{array}\right.$

Q: What's the kernel of $\omega$ in this case?

• Frobenius lifts from char $p$ to char $0$.

Recall the exact sequence $1 \to I_{\mathfrak{P}} \to D_{\mathfrak{P}} \xrightarrow{\pi} \mathrm{Gal}(\bar{L}/\bar{k}) \to 1$ (0.1)

$\sigma \mapsto \bar{\sigma}$

Pf/ (Following Serre's "Local Fields").

$\sigma \in D_{\mathfrak{P}}$, so $\sigma(\mathfrak{P}) = \mathfrak{P}$.

So ~~via~~ the map $\mathcal{O}_L \xrightarrow{\sigma} \mathcal{O}_L$, $\mathfrak{P}$ goes to $\mathfrak{P}$, so get an induced map $\bar{\sigma} : \mathcal{O}_L/\mathfrak{P} \to \mathcal{O}_L/\mathfrak{P}$, $\bar{\sigma}(\alpha \bmod \mathfrak{P}) = \sigma\alpha \bmod \mathfrak{P}$.

To show that $\pi$ is onto:

Case 1: $D_{\mathfrak{P}} = \mathrm{Gal}(L/k)$ $(g = 1)$:

Choose $a \in \bar{L}$ s.t. $\bar{L} = \bar{k}(a)$ (sep. extension of finite fld.).

(note $f = (\bar{L} : \bar{k})$). The $f$ conjugates ~~of~~ $s(a)$ for $s \in \mathrm{Gal}(\bar{L}/\bar{k})$ are distinct, so $s$ is determined by its action ~~of~~ on $a$.

Choose $\alpha \in \mathcal{O}_L$ s.t. $\alpha \bmod \mathfrak{P} = a$.

$$h(X) := \prod_{\sigma \in D_{\mathfrak{P}}} (X - \sigma\alpha) \in \mathcal{O}_L[X] \cap K(X) = \mathcal{O}_K[X].$$

Let $p = \mathfrak{P} \cap K$, and let $\bar{h}(X) = h(X) \bmod p$.

As $\bar{h}(a) = 0$, the min poly over $\bar{k}$ of $a$ divides $\bar{h}(X) \Rightarrow \bar{h}(s(a)) = 0$ $\forall s \in \mathrm{Gal}(\bar{L}/\bar{k})$

∴ Given $s \in \mathrm{Gal}(\bar{L}/\bar{k})$, $\exists \sigma \in D_{\mathfrak{P}}$ s.t. $X - \sigma\alpha \equiv X - sa \bmod \mathfrak{P}$.

∴ $\pi(\sigma) = s$ //

Case 2: General case.

Let still $\bar{L} = \bar{k}(a)$. By CRT, $\exists \alpha \in \mathcal{O}_L$ s.t. $\begin{cases} \alpha \equiv a \bmod \mathfrak{P} \\ \alpha \equiv 0 \bmod \sigma^{-1}\mathfrak{P} \ \forall \sigma \in G - D_{\mathfrak{P}} \end{cases}$

↑ ⇔ $\sigma\alpha \equiv 0 \bmod \mathfrak{P}$

Let $h(X) = \prod_{\sigma \in G} (X - \sigma\alpha) \in \mathcal{O}_K[X]$, so $\bar{h}(X) \in \bar{k}[X]$.

For $\sigma \notin D_{\mathfrak{P}}$, $X - \sigma\alpha \equiv X \bmod \mathfrak{P}$, so $\bar{h}(X) = X^N \prod_{\sigma \in D_{\mathfrak{P}}} (X - \pi(\sigma)\alpha)$, $N := |G| - |D_{\mathfrak{P}}|$

Apply case 1 to $\frac{\bar{h}(X)}{X^N}$

# Hilbert Class Field $K^{(1)}$ of $K$.

Df: $K^{(1)}/K$ is the maximal abelian extension of $K$ unramified over $K$.
(infinite primes also unramified, i.e. a real prime does not become complex).

**Theorem**: For $L = K^{(1)}$, then the Artin map $\omega : I_K \to Gal(K^{(1)}/K)$
$\uparrow$
deep! is onto with kernel $P_K$ = principal fractional ideals of $K$.
(so $Gal(K^{(1)}/K) \simeq Cl(K)$ ).

**Corollary**: a prime $\mathfrak{p}$ has order $f$ in $I_K/P_K$ where $f$ = order of $(\mathfrak{p}, K^{(1)}/K)$.
(in particular: $\mathfrak{p}$ is principal $\Leftrightarrow$ splits completely in $K^{(1)}$ ).

**Example**: $K = \mathbb{Q}(\sqrt{-5})$, $h(K) = 2$

Then $K^{(1)} = K(i)$.

Check the previous result by hand.

We also define $K^{(n+1)}$ = Hilbert Class Field of $K^{(n)}$ $(K^{(0)} = K)$

**Application**: Euler conjectured that for a prime $p$, $p = x^2 + 5y^2 \Leftrightarrow p = 5$ or $p \equiv 1, 9 \pmod{20}$

$\Rightarrow$ is elementary (work with congruences) $2p = x^2 + 5y^2 \Leftrightarrow p = 2$ or $p \equiv 3, 7 \pmod{20}$

$\Leftarrow$ Let $K = \mathbb{Q}(\sqrt{-5})$ which has a $\mathbb{Z}$-basis $1, \sqrt{-5}$. $N(x + y\sqrt{-5}) = x^2 + 5y^2$.
$(x, y \in \mathbb{Z})$.

$\Delta_K = -20$, so $2, 5$ are the exceptional primes. Also, $h(K) = 2$ (use Minkowski bound).

We want to determine the split primes in $K$.

$$\left(\frac{-5}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{5}{p}\right) \underset{\substack{\uparrow \\ \text{quad. rec.}}}{=} \left(\frac{-1}{p}\right)\left(\frac{p}{5}\right) .$$

$$\left(\frac{p}{5}\right) = \begin{cases} +1 & p \equiv \pm 1 \ (5) \\ -1 & p \equiv \pm 2 \ (5) \end{cases}$$

$$\left(\frac{-1}{p}\right) = \begin{cases} +1 & p \equiv 1 \ (4) \\ -1 & p \equiv -1 \ (4) \end{cases}$$

$$\text{Thus } \left(\frac{-5}{p}\right) = \begin{cases} +1 & p \equiv 1, 3, 7, 9 \ (20) \\ -1 & p \equiv \underset{(11, 13, 17, 19)}{\text{others}} \ (20) \end{cases}$$

Also, $\mathbb{Q}(\sqrt{-5}) \subseteq \mathbb{Q}(\sqrt{5}, i) \subseteq \mathbb{Q}(\sqrt[5]{1}, i) = \mathbb{Q}(\zeta_{20})$ .

Hence, $\exists\, x,y \in \mathbb{Z}$ st $p = x^2+5y^2 \iff p\mathcal{O}_K = \mathfrak{p}_p \mathfrak{p}_p'$ AND $\mathfrak{p}_p = (x+y\sqrt{-5})$ (assume $p \neq 2,5$).

Observe that $2\mathcal{O}_K = \mathfrak{p}_2^2$ and $\mathfrak{p}_2$ is not principal, so $\mathfrak{p}_2$ generates $Cl(K)$.

Now, exactly one of $\mathfrak{p}_p$ or $\mathfrak{p}_2\mathfrak{p}_p$ is principal. Hence the division into whether $p$ or $2p$ is a norm.

- if $p \equiv 3,7\ (20)$, then if $\mathfrak{p}_p$ were principal, then $p = x^2+5y^2 \equiv 1,9 \pmod{20} \Rightarrow !!$
  hence $\mathfrak{p}_p$ is not principal, hence $\mathfrak{p}_2\mathfrak{p}_p$ is principal

- if $p \equiv 1,9\ (20)$, then $2p = x^2+5y^2$, so $2p \equiv 2,18\ (20)$. But we know $x^2+5y^2 \equiv 2\cdot 3$ or $2\cdot 7 \Rightarrow !!$

Also, the inert primes are all principal. This proves Euler's conjecture.

An alternative solution: Use that $Cl(K) \simeq Gal(K^{(1)}/K) \overset{\checkmark}{=} Gal(K(i)/K)$. thanks to that $h(K)=2$!

Then, the decomposition of primes in $K(i)/K$ tells which prime ideals of $K$ are ppal.

## • Ray Classes (Lang, Chapter VI).

They generalize the ideal class group of $K$.

Sps $(K:\mathbb{Q}) = r_1 + 2r_2$, $r_1 = \#$ real embeddings $\sigma_v : K \hookrightarrow \mathbb{R}$
$r_2 = \#$ pairs of embeddings $\sigma_v : K \hookrightarrow \mathbb{C}$

For $\alpha \in K$, define $|\alpha|_v := |\sigma_v(\alpha)|$ ← usual absolute value in $\mathbb{R}$ or $\mathbb{C}$

Example: $K = \mathbb{Q}[X]/(X^3-2)$

$\sigma_{v_1} : K \to \mathbb{R}$, $a+bx+cx^2 \mapsto a + b\sqrt[3]{2} + c\sqrt[3]{4}$

$\sigma_{v_2} : K \to \mathbb{C}$, $a+bx+cx^2 \mapsto a + b\omega\sqrt[3]{2} + b\omega^2\sqrt[3]{4}$ where $\omega = e^{\frac{2\pi i}{3}}$

Def: A modulus (Lang calls it a "cycle") is $\mathfrak{m} = \mathfrak{m}_0\mathfrak{m}_\infty$ where

$\mathfrak{m}_0$ is an integral ideal of $K$, $\mathfrak{m}_\infty = \prod_{\substack{v \text{ real inf. prime} \\ \text{of } K,\ m(v)\in\{0,1\}}} v^{m(v)}$ (only the real primes!).

Example: $K = \mathbb{Q}(\alpha) = \mathbb{Q}[X]/(X^2-5)$

$\sigma_1\left(\frac{1+\alpha}{2}\right) = \frac{1+\sqrt{5}}{2} > 0$

$\sigma_2\left(\frac{1+\alpha}{2}\right) = \frac{1-\sqrt{5}}{2} < 0$.

← so we'll be able to impose positivity conditions.

Let $I(\mathfrak{m}) = I(\mathfrak{m}_0)$ = free abelian gp on prime ideals not dividing $\mathfrak{m}_0$.

$P(\mathfrak{m}) = I(\mathfrak{m}) \cap P_{\wedge \text{ principal ideals.}}$

Moving Lemma: Every ideal class contains an ideal relatively prime to $\mathfrak{m}_0$. ← for pf, use CRT.

Hence, $I(\mathfrak{m}) \longrightarrow I/P$ is onto with kernel $P(\mathfrak{m})$.

So $\dfrac{I(\mathfrak{m})}{P(\mathfrak{m})} \cong I/P$ ← ideal class group of $K$.

Localization.

$\mathfrak{p}$ a prime ideal in an integral domain $R$. Then $R_\mathfrak{p} := \{ \frac{a}{b} : a,b \in R, b \notin \mathfrak{p} \} \subseteq \mathrm{Frac}(R)$.

$R_p$ is a local ring (w/ maximal $\mathfrak{p}R_\mathfrak{p}$).

Ex: $\mathfrak{p} = (0)$, then $R_{(0)} = \mathrm{Frac}(R)$.

$R = \mathbb{Z}$, $p = (2)$, then $\mathbb{Z}_{(2)} = \{ \frac{a}{b} : b \text{ odd} \}$.

Multiplicative Congruence.

$K$, $\mathfrak{m} = \mathfrak{m}_0 \mathfrak{m}_\infty$, (where $\mathfrak{m}_0 = \prod \mathfrak{p}^{m(\mathfrak{p})}$, $\mathfrak{m}_\infty = \prod v^{m(v)}$)

$\alpha \in K^*$. We say $\alpha \equiv 1 \bmod^* \mathfrak{m}$ to mean that:

Suppose $p^{m(\mathfrak{p})} \| \mathfrak{m}_0$. Then it means:

- $\alpha - 1 \in \mathfrak{p}^{m(\mathfrak{p})} R_\mathfrak{p}$ if $p | \mathfrak{m}_0$
- $\sigma_v(\alpha) > 0$ if $v | \mathfrak{m}_\infty$.

Example: $K = \mathbb{Q}(\beta)$, $\beta^2 = 5$. $\mathfrak{m} = (2) \cdot v_1$, $\sigma_{v_1}(\beta) = +\sqrt{5}$.

Find $\alpha \equiv 1 \bmod^* \mathfrak{m}$ but not $\alpha \equiv 1 \bmod^* (2) v_1 v_2$.

For instance, $\alpha = \left( \frac{1+\beta}{2} \right)^3$ is a solution.

Good Reference: Jim Milne's notes on C.F.T.

Def $K_{\mathfrak m} = \{\alpha \in K : \alpha \equiv 1 \bmod^* \mathfrak m\}$. (it's a subgroup of $K^\times$).

$P_{\mathfrak m} = \{(\alpha) : \alpha \in K_{\mathfrak m}\}$ (it's a subgroup of $P_K$ = ppl ideals).

We have $P_{\mathfrak m} \subset P(\mathfrak m) \subset \overset{(= I(\mathfrak m_0))}{I(\mathfrak m)} \subset I$

← ideals relatively prime to $\mathfrak m_0$

Def The Ray Class gp mod $\mathfrak m$ is $I(\mathfrak m)/P_{\mathfrak m}$.

The cosets of $P_{\mathfrak m}$ are called <u>ray classes</u> mod $\mathfrak m$.

<u>Example</u>:

$K = \mathbb Q$, $\mathfrak m = (m)v_\infty$, $m \geq 1$.

Via the Artin map, there is an isomorphism:

$$\omega : I(\mathfrak m)/P_{\mathfrak m} \xrightarrow{\sim} \underset{\overset{\wr\wr}{(\mathbb Z/m\mathbb Z)^\times}}{\mathrm{Gal}(\mathbb Q(\zeta)/\mathbb Q)}, \quad \zeta = e^{2\pi i/m}.$$

Pf/ Recall that $\omega((p)) = ((p), \mathbb Q(\zeta)/\mathbb Q) = \mathrm{Frob}_p = [\zeta \mapsto \zeta^p] =: \sigma_p$

Then $\omega\left(\left(\frac{a}{b}\right)\right) = \sigma_{ab^*}$ $\left(\begin{matrix} ab > 0 \\ (ab, m) = 1\end{matrix}, \ bb^* \equiv 1\ (m)\right)$.

So $\omega$ is clearly onto. Identify the kernel!

Check it!

$\sigma_{ab^*} = 1 \iff ab^* \equiv 1 \bmod m \iff a(b^*b) \equiv b \bmod m \iff a \equiv b \pmod m \iff$

$\iff \frac{a}{b} \equiv 1 \bmod^* (m).v_\infty$

Thus $\ker \omega = P_{\mathfrak m}$.

<u>Later will see</u>: For a finite abelian extension $L/K$, we'll show $\exists$ modulus $\mathfrak m$ of $K$ s.t. $\ker \omega_{L/K} \supseteq P_{\mathfrak m}$ ($\mathfrak m$ will be called the conductor).

Proposition 1.3: $K$ a #field, $\mathfrak{m}=\mathfrak{m}_0\mathfrak{m}_\infty$ a modulus. Then:

$$I_K(\mathfrak{m})/P_{\mathfrak{m}} \text{ is a finite group of order } h_{\mathfrak{m}} = \frac{h\cdot\varphi(\mathfrak{m}_0)\, 2^{s(\mathfrak{m}_\infty)}}{[E:E_{\mathfrak{m}}]}$$

where:

- $h=h(K)$ is the class # of $K$.
- $\varphi(\mathfrak{m}_0) = \#\left(\mathcal{O}_K/\mathfrak{m}_0\right)^\times = \prod_{\mathfrak{p}\mid\mathfrak{m}_0}(N\mathfrak{p}-1)(N\mathfrak{p})^{m(\mathfrak{p})-1}$ $\quad\left(N=N_{K|\mathbb{Q}}\right).$ $\quad N\mathfrak{p} = \#\,\mathcal{O}_K/\mathfrak{p}$
- $s(\mathfrak{m}_\infty) = \#$ real primes dividing $\mathfrak{m}_\infty$.
- $E=\mathcal{O}_K^\times$, $\quad E_{\mathfrak{m}} = E\cap K_{\mathfrak{m}}$.

Note: if $(\alpha)$ and $\mathfrak{m}_0$ are relatively prime, then $\alpha^{2\varphi(\mathfrak{m}_0)} \equiv 1 \bmod^* \mathfrak{m}$ $\quad (\alpha\in\mathcal{O}_K)$

(Euler's theorem in elementary number theory). (the 2 is to make it positive)

So $E \supset$ ~~$E$~~. $E_{\mathfrak{m}} \supset E^{2\varphi(\mathfrak{m}_0)}$ $\Rightarrow$ finite index since $E$ is finitely generated.

(and hence $[E:E_{\mathfrak{m}}]$ is finite)

Proof

$$I(\mathfrak{m})/P_{\mathfrak{m}} \twoheadrightarrow I(\mathfrak{m})/P(\mathfrak{m}) \overset{\text{Moving lemma}}{\simeq} Cl(K)$$

We have an exact sequence then:

$$1 \to \overset{?}{\boxed{P(\mathfrak{m})/P_{\mathfrak{m}}}} \to I(\mathfrak{m})/P_{\mathfrak{m}} \to Cl(K) \to 1$$

Also,

$$\begin{tikzcd}
1 \arrow[r] & E \arrow[r] & K(\mathfrak{m}) \arrow[r] & P(\mathfrak{m}) \arrow[r] & 1 \\
1 \arrow[r] & E_{\mathfrak{m}} \arrow[r] \arrow[u, hook] & K_{\mathfrak{m}} \arrow[r] \arrow[u, hook] & P_{\mathfrak{m}} \arrow[r] \arrow[u, hook] & 1
\end{tikzcd}$$

(exact rows)

By the snake lemma, get exact sequence:

$$1 \to E/E_{\mathfrak{m}} \to \overset{?}{\boxed{K(\mathfrak{m})/K_{\mathfrak{m}}}} \to P(\mathfrak{m})/P_{\mathfrak{m}} \to 1$$

The middle term $K(m)/K_m$ has order ~~#~~ $\varphi(m_0)\cdot 2^{s(m_\infty)}$:

Using $\mathcal{O}_K/\mathfrak{p}^{m(\mathfrak{p})} \simeq R_\mathfrak{p}/\mathfrak{p}^{m(\mathfrak{p})}R_\mathfrak{p}$, and "CRT", we have:

$$1 \to K_m \to K(m) \xrightarrow{\beta} \prod_{\mathfrak{p}|m_0}\left(R_\mathfrak{p}/\mathfrak{p}^{m(\mathfrak{p})}R_\mathfrak{p}\right)^\times \times \prod_{v|m_\infty} \mathbb{R}^\times/\mathbb{R}^{\times 2} \to 1$$

$\beta$ is onto by the weak approximation thm (= CRT + positive conditions).

This completes the proof.

<u>Example</u>: For $K=\mathbb{Q}$, $m=(m)v_\infty$, ~~[illegible]~~

$$\underset{\substack{\uparrow}}{h_m} = \frac{1\cdot\varphi(m)\cdot 2^1}{[(\pm1):\{1\}]} = 1\cdot\varphi(m) = \#\left(\mathbb{Z}/m\mathbb{Z}\right)^\times .$$

ray class number (or order of the ray class gp).

<u>HW Problem</u>: Change this by $K=\mathbb{Q}$, $m=m_0=(m)$ and find $h_m$.

## Regulator of $K$:

Recall from alg. num th the proof of the Unit theorem:

$$K^\times \hookrightarrow \mathbb{R}^{r_1}\times\mathbb{C}^{r_2} \xrightarrow{\log} \mathbb{R}^{r_1+r_2}$$

$$\alpha \mapsto (\sigma_j\alpha) \longmapsto \operatorname{Log}\left(|\sigma_j\alpha|^{n_j}\right) \qquad \left(n_j=\begin{cases}1 & \text{real}\\ 2 & \text{complex}\end{cases}\right).$$

and then omit one of the $\sigma_j$ to get a lattice in $\mathbb{R}^{r_1+r_2-1}$.

Take $\varepsilon_1,\dots,\varepsilon_r$ $(r=r_1+r_2-1)$ a basis of $E/\text{torsion}$.

Then $R_K := \left|\det\left(\underset{\uparrow\, r\times r\text{ matrix}}{\log|\sigma_j\varepsilon_i|^{n_j}}\right)\right| \underset{\uparrow\,\text{it's a thm.}}{\neq} 0$ is the <u>regulator</u> of $K$.

Similarly, one can define the regulator $R_{\mathfrak{m}}$ of the subgroup $E_{\mathfrak{m}}$ of $E$.

Goal: If $c$ is a class of $I(\mathfrak{m})/P_{\mathfrak{m}}$, want to get an asymptotic formula for the # of integral ideals in $c$ of norm $\leq t$.
(will call it $j(c,t)$).
We will show that $j(c,t) = \rho_{\mathfrak{m}} t + O(t^{1-\frac{1}{n}})$ $\quad (n = (K:\mathbb{Q}))$.

- Dedekind $\zeta$ function:

Def: $\zeta_K(s) := \sum_{\mathfrak{a} \subseteq \mathcal{O}_K} \frac{1}{N(\mathfrak{a})^s}$ (simple pole at $s=1$)

we also define $\zeta_K(s;c) := \sum_{\mathfrak{a} \in C} \frac{1}{N(\mathfrak{a})^s}$ (partial zeta-function), for a given class $c \in Cl(K)$.

If $a_n$ = # integral ideals of norm $n$ in class $c$,
$$\zeta_K(s,c) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}.$$
we will estimate $\sum_{n \leq t} a_n$ $(= j(c,t))$ for $t$ large.

Theorem: Let $j(c,t)$ = # integral ideals in the ~~class~~ ray class $c \in I(\mathfrak{m})/P_{\mathfrak{m}}$ of norm $\leq t$.
Fix a modulus $\mathfrak{m}$ and a ray class $c \in I(\mathfrak{m})/P_{\mathfrak{m}}$.
Then $j(c,t) = \rho_{\mathfrak{m}} t + O(t^{1-\frac{1}{n}})$, $n = (K:\mathbb{Q})$.

[ $f(t) = O(g(t))$ means $\left|\frac{f(t)}{g(t)}\right|$ bounded as $t \to \infty$ ].

and: $\rho_{\mathfrak{m}} = \dfrac{2^{r_1} \cdot (2\pi)^{r_2} R_{\mathfrak{m}}}{\sqrt{|d_K|}\; w_{\mathfrak{m}} N(\mathfrak{m})}$ $\leftarrow$ regulator of $E_{\mathfrak{m}}$

$d_K = \mathrm{disc}(K)$.
$w_{\mathfrak{m}} = \#(\mu_K \cap E_{\mathfrak{m}})$
$N(\mathfrak{m}) = N(\mathfrak{m}_0) \cdot 2^{s(\mathfrak{m}_\infty)}$

Ref: Lang VI, Fröhlich-Taylor 274-294 (crisp).

~~(P)~~ Count lattice points in homogeneously expanding domains.

Example: $L = \mathbb{Z}^2 \subset \mathbb{R}^2$, $L = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$ $\big(\omega_1 = (1,0),\ \omega_2 = (0,1)\big)$.

$X$ = disc of radius 1, and for $t > 0$, $tX = \{tx : x \in X\}$.

Let $\lambda(t, X, L) = \#\{L \cap tX\}$.

Then $\lambda(t,X,L) = \pi t^2 + O(t)$.

Now let $L$ be a lattice in $\mathbb{R}^n$, spanned by $\omega_1, \dots, \omega_n$.

Let $X$ be a subset of $\mathbb{R}^n$ with "nice" boundary. (ie $(n-1)$-Lipschitz).

[Let $S$ be a subset of Euclidean space, $\varphi : S \to \mathbb{R}^n$ is <u>Lipschitz</u> if $\exists\, C$ s.t. $\forall x, y \in S$, $|\varphi(x) - \varphi(y)| \leq C|x-y|$.

A subset $T \subseteq \mathbb{R}^n$ is $k$-Lipschitz parametrizable if $\exists$ a finite number of Lipschitz maps $\varphi_j : I^k \to T \subset \mathbb{R}^n$ that cover $T$ $\big(I^k = [0,1]^k\big)$.]

$F$: fundamental domain for $L \subseteq \mathbb{R}^n$, $F = \left\{ \sum_{i=1}^{n} c_i \omega_i \,\middle|\, 0 \leq c_i < 1 \right\}$.

<u>Note</u>: $F$ contains <u>only one</u> lattice point.

So $\mathbb{R}^n = \biguplus_{\ell \in L} (\ell + F)$

<u>Theorem 1.4</u>: Let $X$ be measurable $\subseteq \mathbb{R}^n$, with $\partial X$ $(n-1)$-Lipschitz param., and let $L$ be a lattice in $\mathbb{R}^n$. Then,

$$\lambda(t, X, L) = \frac{\mathrm{vol}(X)\, t^n}{\mathrm{vol}(F)} + O(t^{n-1}).$$

Proof: Write $\lambda(t) := \lambda(t, X, L)$.

Let $m(t) = \# \{ \ell \in L \mid (\ell + F) \subseteq \text{interior of } tX \}$.

$b(t) = \# \{ \ell \in L \mid (\ell + F) \cap \partial(tX) \neq \emptyset \}$.

Then :

1) $m(t) \leqslant \lambda(t) \leqslant m(t) + b(t)$.

2) $\mathrm{vol}(F) \cdot m(t) \leqslant \mathrm{vol}(tX) = t^n \mathrm{vol}(X) \leqslant \big(m(t) + b(t)\big) \cdot \mathrm{vol}(F)$

So $m(t) \leqslant \dfrac{\mathrm{vol}(X)\, t^n}{\mathrm{vol}(F)} \leqslant m(t) + b(t)$.

Fact: $b(t) = O(t^{n-1})$ (by Lipschitz) ← see Lang

$$\left.\begin{array}{l} \text{Then } (1) \Rightarrow \lambda(t) = m(t) + O(t^{n-1}) \\ (2) \Rightarrow \dfrac{\mathrm{vol}\, X}{\mathrm{vol}\, F} t^n = m(t) + O(t^{n-1}) \end{array}\right\} \overset{\text{subtract}}{\Rightarrow} \lambda(t) = \frac{\mathrm{vol}\, X}{\mathrm{vol}\, F} t^n + O(t^{n-1})$$

Then, by the multiple embeddings, $K^\times \overset{\theta}{\hookrightarrow} \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \cong \mathbb{R}^n$.

Also, $\theta(\mathcal{O}_K)$ or $\theta(\mathfrak{a})$ is a lattice in $\mathbb{R}^n$ ($\mathfrak{a}$ a lattice).

For the sake of simplicity, take $\mathfrak{m} = (1)$ (i.e. ordinary class field).

Let $c \in I_K / P_K$

Theorem: $\displaystyle\lim_{t \to \infty} \frac{j(c,t)}{t} = \rho$, $\rho > 0$ independent of $c$, $\rho = \dfrac{2^{r_1} (2\pi)^{r_2} R_K}{\sqrt{|d_K|} \cdot \# \mu_K}$

From this, we will also get the theorem saying that the residue at $s = 1$ in $\zeta_K(s)$ is $\rho \cdot h_K$ ($h_K$ = class number).

Pf (of thm):

Note: Minkowski's bound states that if $t > C_K$, then $j(c,t) \geq 1$ $\forall c$.

This allows to transition to a lattice point problem:

- given a class $c$, pick an integral ideal $\mathfrak{b} \in c^{-1}$.

There's a bijection $\mathfrak{a} \longmapsto \mathfrak{a}\cdot\mathfrak{b} = \underset{\overset{\cap}{\mathcal{O}_K}}{(\alpha)}$ between $\{$integral ideals $\mathfrak{a} \in c\} \leftrightarrow \left\{\begin{array}{l}\text{principal}\\ \text{integral ideals}\\ \text{divisible by } \mathfrak{b}\end{array}\right\}$

Also, $N(\mathfrak{a}) \leq t \iff N(\mathfrak{a}\mathfrak{b}) = |N_{K/\mathbb{Q}}(\alpha)| \leq t \cdot N(\mathfrak{b})$.

We define an equivalence relation on $K^\times$, $\sim$, by:

$\alpha \sim \beta \iff \alpha = \beta u$, for $u \in E = \mathcal{O}_K^\times$.

Lemma 1.5: $j(c,t) = \#\{$equiv. classes of nonzero $\alpha \in \mathfrak{b}$ with $|N(\alpha)| \leq t \cdot N\mathfrak{b}\}$.

So we land in a lattice.

Example: $K = \mathbb{Q}(i)$, $h_K = 1$. So $j(c,t) = \#\{$equiv. classes of $a+bi \neq 0$, $a,b \in \mathbb{Z}$ s.t. $a^2+b^2 \leq t\}$

As $E = \langle i \rangle$, $E$ acts by rotating by ~~[illegible]~~ $90°$, so we are counting only lattice points on the first quadrant: $j(c,t) = \frac{\pi}{4}t + \underset{O(\sqrt{t})}{~~O(t^{a})~~}$

The problem is how to deal with the equivalence classes, when there are units of infinite order.

~~Example: K = real quadratic~~.

Let $\Gamma$ be a discrete subgroup of $\mathbb{R}^n$. $\Gamma$ acts on $\mathbb{R}^n$ by translation, so get $\mathbb{R}^n/\Gamma$

Def: A measurable set $D$ is a fundamental domain for the action of $\Gamma$ if:

(a) no 2 points of $D$ are equivalent under the action of $\Gamma$.

(b) every point in $\mathbb{R}^n$ is equivalent to some point in the closure of $D$, $\overline{D}$.

Example (K real quadratic). (More details in Fröhlich-Taylor).

$K = \mathbb{Q}(\beta)$, $\beta^2 = d > 0$.

$K \overset{\theta}{\hookrightarrow} \mathbb{R}^2$

$a+b\beta \mapsto (a+b\sqrt{d}, a-b\sqrt{d})$.

$\theta(\mathcal{O}_K)$ is a lattice in $\mathbb{R}^2$, and $\mathrm{vol}(\theta(\mathcal{O}_K)) = \sqrt{|d_K|}\cdot\cancel{2^{-r_2}}$ ?

Introduce a norm $N$ on $\mathbb{R}^2$ s.t. $N(\theta(\alpha)) = |N_{K|\mathbb{Q}}(\alpha)|$, $\alpha \neq 0$.

Let $(x,y) \in \mathbb{R}^2$. Define $N((x,y)) = |x\cdot y|$.

The units $u \in E$ of $K$ act on $\mathbb{R}^2$:

$$u\circ(x,y) = (\sigma_1(u)\cdot x, \sigma_2(u)\cdot y) = \theta(u)\cdot(x,y) \left(\begin{array}{l}\sigma_1(a+b\beta) = a+\sqrt{d}\,b \\ \sigma_2(a+b\beta) = a-\sqrt{d}\,b\end{array}\right)$$

Note $N(u\circ(x,y)) = N((x,y))$.

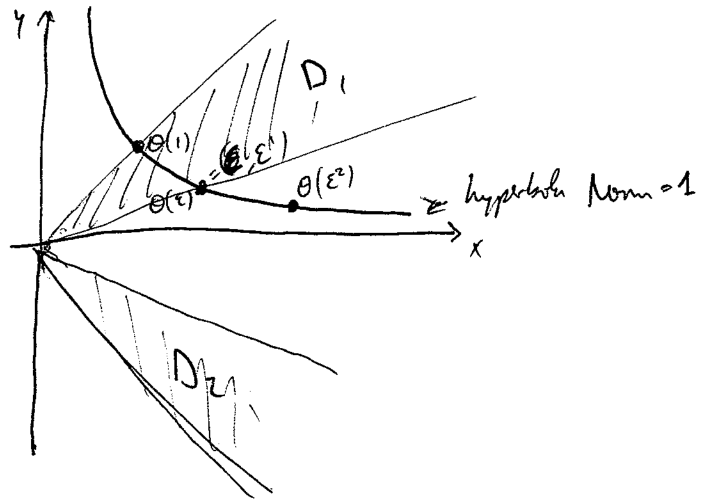
Want a fundamental domain for the action of $\theta(E)$ (or of $E$) on $\mathbb{R}^2$.

In this case, $E = \langle -1\rangle \times \langle \varepsilon\rangle$, $\varepsilon > 1$ the fundamental unit (by continued fractions).

$N\varepsilon = \pm 1$. Assume $N\varepsilon = +1 = \varepsilon\varepsilon'$.

We write $\theta(\varepsilon) = (\varepsilon, \varepsilon')$.

Note that $N((x,y)) \leq t \Leftrightarrow |xy| \leq t$.



Claim: $D = D_1 \cup D_2$ is a fundamental domain for action of $E \circlearrowleft \mathbb{R}^2$.

(we don't need the other ~~2~~ quadrants, because we have $-1$ action).

Then, let $t$ increase. To calculate the area of $\{(x,y) \in D_1 : xy \leq t\}$, take the log of all the graphic...

__General case__: $K$, $S_\infty$ = infinite primes of $K$.

$$K \xrightarrow{\theta} \prod_{v \in S_\infty} K_v = \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} = \mathbb{R}^n \quad , \; n = (K:\mathbb{Q}).$$

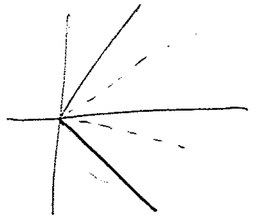
$\theta(\alpha) = (\sigma_v \alpha)$, $v \in S_\infty$.

Then $E$ acts on $\prod K_v$ by $u \circ (\xi_v) = (\sigma_v u \cdot \xi_v)$ $\quad (\xi_v \in K_v)$.

Also $N(\xi_v) = \prod_{v \in S_\infty} |\xi_v|^{n_v}$, $\quad n_v = \begin{cases} 1 & v \text{ real} \\ 2 & v \text{ complex} \end{cases}$.

__Remark__: in the case previously done ($K$ real quadratic):

$$K = \mathbb{Q}(\beta), \; \beta^2 = d > 0. \qquad K \overset{\theta}{\hookrightarrow} \mathbb{R} \times \mathbb{R}.$$



if $(x,y) \in \operatorname{im}\theta$, $(x,-y)$ ~~not necessar~~ is __not__ in im $\theta$, for otherwise $(2x,0) \in \operatorname{im}\theta \Rightarrow x = 0 \Rightarrow$ only point $(0,0)$.

__However__: the asymptotic counting works because we are just counting __areas__.

Let $c$ be an ideal class, $I \in c^{-1}$.

Let $D$ be a fundamental domain for the units ($E$) acting on $\prod_{v \in S_\infty} K_v^\times \simeq (\mathbb{R}^n)^\times$.

Let $\lambda(t, X, L) = \#(L \cap tX)$, $(t>0)$ for $\begin{cases} X \text{ a domain} \\ L \text{ a lattice} \end{cases}$.

Let $D(t) = \{\xi \in D : N(\xi) \leq t\}$.

Note: $D(t) = t^{\frac{1}{n}} D(1)$ $\qquad$ (note $D$ ~~is~~ a cone, so $tD = D$ for $t>0$).

$j(c,t)$ = # ideals in class $c$ of norm $\leq t$

Lemma 1.6. $j(c,t) = \lambda\left( (t\cdot N\mathcal{L})^{1/n}, D(1), \mathcal{L}\right)$.

Pf From 1.5, $j(c,t) = \#\{(\alpha) : \alpha\neq 0, \alpha\in\mathcal{L}, |N_{K/\mathbb{Q}}(\alpha)| \leq t\cdot N(\mathcal{L})\} =$

(let $L = \theta(\mathcal{L})$) $\quad = \#\{\mathcal{L}\cap D(t\cdot N(\mathcal{L}))\} = \lambda\left( (t(N\mathcal{L}))^{1/n}, D(1), \mathcal{L}\right)$ //

- Definition of the fundamental domain for the action $E \circlearrowright \mathbb{R}^n$

Write $E = \mu_K \times V$, $V \simeq \mathbb{Z}^{r_1+r_2-1}$ (Dirichlet's unit thm)

We will find a fund. domain for the action of $V$, and its volume.

For $E$, just divide by $\#\mu_K$.

Define a hom. of groups $\quad g : \prod_\infty K_v^\times \longrightarrow \prod_\infty \mathbb{R} = \mathbb{R}^{r_1+r_2}$

$$(\xi_v)_v \longmapsto \left( n_v \cdot \log \frac{|\xi_v|}{(N\xi)^{1/n}} \right)_v \qquad (n_v \in \{1,2\}).$$

which is called the "homogenized log map", as $g(t\xi) = g(\xi)$.

Also, $\operatorname{im} g \subseteq$ hyperplane $H = \{(x_v) : \sum x_v = 0\}$.

Let $\Lambda = g(\theta(V)) =$ "$g$(units)", $\Lambda$ is a lattice in $H$.

Let $F$ be a fundamental domain for $\Lambda$ in $H$, and define $D = g^{-1}(F)$.

Claim: $D$ is a fundamental domain for $V \circlearrowright \prod_\infty K_v^\times$.

Facts: 
- $\operatorname{vol}(D(1)) = 2^{r_1}\pi^{r_2} R_K$ (Lang, Chap VI)
- $\operatorname{vol}(\theta(\mathcal{L})) = N(\mathcal{L})\sqrt{|d_K|}\cdot 2^{-r_2}$. (early in Lang).

Collecting them: $j(c,t) \overset{1.6}{=} \frac{1}{|\mu_K|}\#\{\theta(\mathcal{L}) \cap (tN\mathcal{L})^{1/n} D(1)\} \overset{1.4}{=} \frac{1}{|\mu_K|}\frac{\operatorname{vol}(D(1))}{\operatorname{vol}(\theta(\mathcal{L}))}(tN\mathcal{L}) + O(t^{1-\frac{1}{n}})$

$$= \frac{1}{|\mu_K|}\frac{2^{r_1}\pi^{r_2}R_K}{\cancel{N(\mathcal{L})}\sqrt{|d_K|}}\, 2^{r_2}\,(t\cdot \cancel{N(\mathcal{L})}) + O(t^{1-1/n}) \Rightarrow \text{Thm 1.7.}$$

//

Now summing over the classes:

$$j(t) = \frac{2^{r_1}(2\pi)^{r_2} h_K R_K}{|\mu_K|\sqrt{|d_K|}}\, t + O\left(t^{1-1/n}\right).$$

So the only thing we still need to work on is the fundamental domain D.

Recall that we were looking for D, a fund. domain for the action of $\mathcal{O}(V)$ on $\prod_\infty K_v^\times$. We want also D to be a cone.

Recall the g map: $g : \prod_\infty K_v^\times \longrightarrow \prod_\infty \mathbb{R} \cong \mathbb{R}^{r_1+r_2}$

$$(\xi_v)_v \longmapsto \left(\dots, n_v \cdot \frac{\log|\xi_v|}{N(\xi)^{1/n}}, \dots\right) \qquad n_v = \begin{cases} 1 & v \text{ real} \\ 2 & v \text{ complex}\end{cases}$$

- g is a homomorphism
- $g(t\xi) = g(\xi)$ $t > 0$.
- $\operatorname{Im} g \subseteq H := \{(\dots x_v \dots) : \sum x_v = 0\}$.

Choose now a $\mathbb{Z}$-basis $\eta_1, \dots, \eta_r$ for V (fund. units). $(r = r_1 + r_2 - 1)$

Let $y_i := g(\mathcal{O}(\eta_i))$.

From the proof of the Unit Theorem, $\Lambda := y_1\mathbb{Z} \oplus \cdots \oplus y_r\mathbb{Z}$ is a lattice in H.

with a usual fundamental domain $F = \{\sum_{i=1}^r c_i y_i : 0 \leq c_i < 1\}$.

Let now $D := g^{-1}(F)$.

Claim: D is a fundamental domain for the action of $\mathcal{O}(V)$ on $\prod_\infty K_v^\times$.

Pf/ First, D is a cone: $tD = D$, $t > 0$ because g is homogeneous.

Also, $D(1)$ is bounded:

Let $D_0(1) = \{\xi \in D : N(\xi) = 1\}$. Observe that $D(1) = \{t D_0(1) : 0 < t \leq 1\}$.

So it suffices to show that $D_0(1)$ is bounded.

The map $g : D_0(1) \longrightarrow H$ sends $(\xi_v) \mapsto (\dots, \log|\xi_v|^{n_v}, \dots)$

And $g(D_0(1))$ is bounded $\Rightarrow$ $D_0(1)$ bounded. (because the inverse map is the exp. map).

$g(D_0(1)) = \{p \in F : \dots\}$ is bounded.

$\downarrow$

claim: $g^{-1}(F)$ contains coset reps of $\prod K_v^\times / \theta(V)$ :

Pf/ Show that

$$\begin{tikzcd} \prod K_v^\times \arrow[r, two heads, "g"] & H \\ \theta(V) \arrow[u, hook] \arrow[r, two heads, "g"] & \Lambda \arrow[u, hook] \end{tikzcd}$$

is onto

F is a fund. domain for ~~H~~ $H/\Lambda$ and g is onto $\Rightarrow$ ~~pf~~ claim. //

Next, we need to show that if $\exists u \in V$ s.t. $\theta(u)\cdot\eta = \xi$, the $\eta, \xi \in D$, then $u = 1$ (no duplicates).

Apply $g$ to it: $g(\theta(u)) + g(\eta) = g(\xi) \Rightarrow g(\theta(u)) = g(\xi) - g(\eta) \in \Lambda$

$\Rightarrow g(\xi) = g(\eta)$ since F is a fund. domain.

$g|_{\theta(V)}$ is injective

So $g(\theta(u)) = 0 \Rightarrow \theta(u) = 1 \Rightarrow u = 1$ because $g$ is injective on $\theta(V)$ (unit thm) //

Ref: check an alternative proof in B. Osserman's notes (google: fundamental domain volume).

---

## Dirichlet Series and Zeta-functions (chap VIII Lang)

Define $f(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$, $s \in \mathbb{C}$, $a_1, a_2, \dots$ sequence of complex numbers.

(Dirichlet & Dedekind used only $s \in \mathbb{R}$)

(eg $a_n = 1 \ \forall n$, get $\zeta(s) = \sum \frac{1}{n^s}$).

(eg $\zeta_K(s) = \sum_{(0) \neq \mathfrak{a} \subseteq O_K} \frac{1}{N(\mathfrak{a})^s}$).

~~Note~~ Example that, for instance $K = \mathbb{Q}(i)$, $(2) = (1-i)^2$, $p \equiv 1 \ (4) \Rightarrow (p) = \mathfrak{P}_1 \mathfrak{P}_2$

$p \equiv 3 \ (4) \Rightarrow (p) = \mathfrak{P}$

$\zeta_K(s) = \sum_{n \geq 1} \frac{a_n}{n^s}$, $a_n =$ # ideals of norm $n$.

it's a fact ↓ ← the character in the following page.

$$\zeta_{\mathbb{Q}(i)}(s) = 1 + \frac{1}{2^s} + \frac{1}{4^s} + \frac{2}{5^s} + \frac{1}{8^s} + \frac{1}{9^s} + \cdots + \frac{4}{65^s} = \zeta_{\mathbb{Q}}(s) \cdot L(s, \chi)$$

Also, if $f(s) = \sum \frac{a_n}{n^s}$, $g(s) = \sum \frac{b_n}{n^s}$, and $g(s) = f(s)$, then $a_n = b_n \ \forall n$.

Reference. Serre, "A Course in Arithmetic" (chapter ~~on~~ analytic theory).

Example
~~Define~~ the Dirichlet character $\chi : \mathbb{N} \to \{\pm 1\}$, $\chi(n) = \begin{cases} 0 & n \text{ even} \\ 1 & n \equiv 1\ (4) \\ -1 & n \equiv 3\ (4) \end{cases}$

$$L(s,\chi) = \sum_{n \geq 1} \frac{\chi(n)}{n^s} = 1 - \frac{1}{3^s} + \frac{1}{5^3} - \frac{1}{7^s} + \cdots$$

(and $\xi_{\mathbb{Q}(i)}(s) = \xi_{\mathbb{Q}}(s) \cdot L(s,\chi)$)

We want to show that there's a maximal open half-plane of convergence of $f(s)$.

(2.1) Abel Summation:

Given two sequences $\{a_n\}$, $\{b_n\}$ of complex numbers. Fix $m$, and for $n > m$, let $A_n := \sum_{k=m+1}^{n} a_k$, and set $A_m := 0$. Then:

$$\sum_{k=m+1}^{n} a_k b_k = \sum_{k=m+1}^{n-1} A_k (b_k - b_{k+1}) + A_n b_n$$

← discrete form of integration by parts.

Pf

$$\sum_{m+1}^{n} a_k b_n = \sum_{m+1}^{n} (A_k - A_{k-1}) \cdot b_k = \sum_{m+1}^{n} A_k b_k - \sum_{m}^{n-1} A_k b_{k+1} =$$

$$= \sum_{m+1}^{n-1} A_k (b_k - b_{k+1}) - A_m b_{m+1} + A_n b_n \quad //$$

(2.2) Lemma: $U$ an open subset of $\mathbb{C}$, and $\{f_n\}$ a sequence of holom. functions, ~~such that each $f_n$ converges uniformly~~ that converges uniformly to a function $f$ on all compact subsets of $U$.

Then $f$ is holomorphic on $U$, and $f_n' \to f'$, uniformly on compacts.

(We apply this to $f_n(s) = \sum_{k=1}^{n} \frac{a_k}{k^s}$)

(2.3) Lemma: $0 < \alpha < \beta$, $s \in \mathbb{C}$, $\sigma = \mathrm{Re}(s) > 0$. Then:

$$\left| e^{-\alpha s} - e^{-\beta s} \right| \leq \frac{|s|}{\sigma} \cdot \left( e^{-\alpha\sigma} - e^{-\beta\sigma} \right)$$

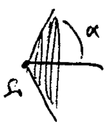
Pf $e^{-\alpha s} - e^{-\beta s} = s \cdot \int_\alpha^\beta e^{-xs}\, dx$. Taking $|\cdot|$, and use $|e^{-\alpha s}| = e^{-\alpha\sigma}$.

$$\Rightarrow \left| e^{-\alpha s} - e^{-\beta s} \right| \leq |s| \int_\alpha^\beta |e^{-x\sigma}|\, dx = \frac{|s|}{\sigma} \cdot \left( e^{-\alpha\sigma} - e^{-\beta\sigma} \right). \quad //$$

Corollary: Let $k \geq 2$, then with $\alpha = \log k$, $\beta = \log(k+1)$, we get:

$$\left| \frac{1}{k^s} - \frac{1}{(k+1)^s} \right| \leq \frac{|s|}{\sigma} \left( \frac{1}{k^\sigma} - \frac{1}{(k+1)^\sigma} \right) \quad //$$

(2.4) Theorem: If the series $f(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$ converges at $s = s_0$, then for any $0 \leq \alpha < \pi/2$, it converges uniformly in every domain of the form $\mathrm{Re}(s - s_0) \geq 0$, $|\measuredangle(s - s_0)| \leq \alpha$

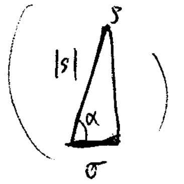


(a wedge).

Proof We may replace $s$ by $s - s_0$, so can assume $s_0 = 0$.

Then, by hypothesis, $\sum a_n$ converges.

In every domain of the form $\mathrm{Re}(s) \geq 0$, $\exists L > 0$ s.t $\frac{|s|}{\sigma} \leq L$. ($L = \sec\alpha$).



Given $\varepsilon > 0$, $\sum a_n$ converges $\Rightarrow \exists M$ s.t $n > m > M \Rightarrow \left| \sum_{m+1}^{n} a_k \right| = |A_n| < \varepsilon$.

Apply (2.1) (Abel sum) with $b_k = \frac{1}{k^s}$, get

$$\sum_{m+1}^{n} a_k b_k = \sum_{m+1}^{n-1} A_k (b_k - b_{k+1}) + A_n b_n$$

$$\left| \sum \frac{a_k}{k^s} \right| \underset{(2.3)}{\leq} \varepsilon \left( \sum_{m+1}^{n-1} \frac{|s|}{\sigma} \left( \frac{1}{k^\sigma} - \frac{1}{(k+1)^\sigma} \right) + \frac{1}{n^\sigma} \right) \leq \varepsilon \left( L \cdot \left( \frac{1}{(m+1)^\sigma} - \frac{1}{n^\sigma} \right) + 1 \right) \leq \varepsilon \cdot (L+1) \to 0.$$

<u>Cor 1</u>: If $f(s) = \sum \frac{a_n}{n^s}$ converges for $s = s_0$, then it converges for $\mathrm{Re}(s) > \mathrm{Re}(s_0)$, and the function thus defined is holomorphic there.

Pf Use (2.4) + (2.2). //

<u>Cor 2</u>: The set of convergence of $f(s)$ contains a maximal open half-plane $\mathrm{Re}(s) > \mathrm{Re}(s_0) = \sigma_0$ (includes $\sigma_0 = -\infty$, or $\sigma_0 = +\infty$).

The line $\{\mathrm{Re}(s) = \sigma_0\}$ is called the "<u>line of convergence</u>", and $\sigma_0$ is called the "<u>abscissa of convergence</u>".

<u>Ex</u>: $\sigma_0 = 1$ for $\zeta_{\mathbb{Q}}(s)$.

$\sigma_0 = 0$ for $L(\chi, s)$. $\left( \chi(n) = \begin{cases} 0 & \text{even} \\ 1 & n \equiv 1 \ (4) \\ -1 & n \equiv 3 \ (4) \end{cases} \right)$

<u>Cor 4</u> (identity principle): $\sum \frac{a_n}{n^s} = \sum \frac{b_n}{n^s} \Rightarrow a_n = b_n \ \forall n \geq 1$.

<u>Cor 3</u>: Let $\sigma_0 = \mathrm{Re}(s_0)$. Suppose that $\sum \frac{a_n}{n^{s_0}}$ converges.

Then $\lim_{s \to s_0} f(s) = f(s_0)$ ($s \to s_0$ in a wedge).

Pf Use uniform convergence //

<u>Pf of Cor 4</u>:

It is the same as $\sum_{n=1}^{\infty} \frac{a_n}{n^s} \equiv 0 \Rightarrow a_n = 0 \ \forall n$.

First, show $a_1 = 0$:

Let $s \to +\infty$ along the real axis. By uniform convergence, $f(s) \to a_1$. So $a_1 = 0$.

Hence $f(s) = \frac{a_2}{2^s} + \cdots$. Replace $f(s)$ by $2^s \cdot f(s)$ and repeat (induction) //

<u>Recall</u>: $g(n) = O(h(n)) \iff \exists C > 0$ s.t. $|g(n)| \leq C |h(n)|$ for suff. large $n$.

Suppose now that $f(s)$ converges for $s_0$, $\mathrm{Re}(s_0)=\sigma_1$. ← not necessarily the abscissa of convergence.

Then $a_n = O(n^{\sigma_1})$:

Pf $\sum \frac{a_n}{n^{s_1}}$ conv. $\Rightarrow \left|\frac{a_n}{n^{s_1}}\right| = \frac{|a_n|}{n^{\sigma_1}} \to 0 \Rightarrow a_n = O(n^{\sigma_1})$ //

Note: in fact, in this case $a_n = o(n^{\sigma_1})$ !

Conversely, suppose that $a_n = O(n^{\sigma_1})$. Then the series converges absolutely and uniformly in $\mathrm{Re}(s) \geq \sigma_1 + 1 + \delta$, $\delta > 0$:

Pf Use Weierstrass-M test:

Compare it to $\sum \frac{C}{n^{1+\delta}}$, using $\left|\frac{a_n}{n^s}\right| = \frac{|a_n|}{n^\sigma} \leq \frac{|a_n|}{n^{\sigma_0}} \cdot \frac{1}{n^{1+\delta}} \leq \frac{C}{n^{1+\delta}}$ //

Example: $L(s,\chi)$ satisfies this with $\sigma_1 = 0$, so get abs convergence for $\mathrm{Re}(s) \geq 1+\delta$.

(2.5) Theorem: Assume $\exists C > 0$, $\sigma_1 \geq 0$, s.t.:

$$\left|\sum_{i=1}^n a_i\right| \leq C n^{\sigma_1}.$$ Then the abscissa of conv. $\sigma_0$ of $\sum \frac{a_n}{n^s}$ is $\leq \sigma_1$.

Proof Take $n > m$, $B_n := \sum_{i=1}^n a_i$.

So
$$\sum_{m+1}^n \frac{a_k}{k^s} = \sum_{m+1}^n \frac{B_k - B_{k-1}}{k^s} \overset{\text{Abel summation trick}}{=} \sum_{m+1}^{n-1} B_k \underbrace{\left(\frac{1}{(k+1)^s} - \frac{1}{k^s}\right)}_{s\int_k^{k+1} \frac{dx}{x^{s+1}}} + \frac{B_n}{n^s} - \frac{B_m}{(m+1)^s}$$

and
$$\left|B_k \cdot s\int_k^{k+1} \frac{dx}{x^{s+1}}\right| \leq |s| \int_k^{k+1} C k^{\sigma_1} \cdot \frac{dx}{x^{\sigma+1}} \leq |s| C \int_k^{k+1} \frac{dx}{x^{\sigma-\sigma_1+1}}$$

$$\therefore \left|\sum_{m+1}^n \frac{a_k}{k^s}\right| \leq C \cdot |s| \int_{m+1}^\infty \frac{dx}{x^{\sigma-\sigma_1+1}} + \frac{C n^{\sigma_1}}{n^\sigma} + \frac{C m^{\sigma_1}}{(m+1)^\sigma}$$ (Recall $(\sigma-\sigma_1) \geq \delta > 0$).

The last two terms are $\leq \frac{C}{n^\delta} + \frac{C}{(m+1)^\delta}$.

The integral term is $\leq \frac{C|s|}{(m+1)^{\sigma-\sigma_0}} \frac{1}{\sigma-\sigma_0} \xrightarrow{m\to\infty} 0$.

(2.6) Theorem: About $\zeta(s) = \sum \frac{1}{n^s}$

i) The abscissa of convergence is $\sigma_0 = 1$.

ii) For $\delta > 0$, it converges absolutely for $\operatorname{Re}(s) \geq 1+\delta$.

iii) $\zeta(s)$ has an analytic continuation to $\operatorname{Re}(s) > 0$, and is holomorphic there except for a simple pole at $s=1$, with residue 1.

Pf We prove analytic continuation first:

Let $\zeta_2(s) = 1 - \frac{1}{2^s} + \frac{1}{3^s} - \frac{1}{4^s} = \sum_{n \geq 1} \frac{(-1)^{n+1}}{n^s}$.

For $\zeta_2(s)$, $\sum_{k=1}^{n} a_k = 1$ or $0$. So by (2.5), its abscissa of convergence is $\leq 0$

Actually, it is exactly 0 (because $\sum (-1)^n$ doesn't converge).

Notice that: $\left(1 - \frac{2}{2^s}\right)\zeta(s) = \zeta_2(s)$ (using abs. convergence for $\operatorname{Re}(s) > 1$).

This gives analytic cont. of $\zeta(s)$ to $\operatorname{Re}(s) > 0$. $\left( \zeta(s) = \frac{\zeta_2(s)}{1 - \frac{2}{2^s}} \right)$

To prove that $s=1$ is a pole with residue 1, will use complex analysis.

Claim: $\zeta(s)$ has no poles at $\operatorname{Re}(s)$ except at $s=1$.

Pf For $r = 2, 3, 4, \ldots$, define $\zeta_r(s) = 1 + \frac{1}{2^s} + \cdots + \frac{1}{(r-1)^s} - \frac{(r-1)}{r^s} + \frac{1}{(r+1)^s} + \cdots + \frac{1}{(2r-1)^s} - \frac{r-1}{(2r)^s} + \cdots$

Can check that $\zeta_r(s) = \left(1 - \frac{r}{r^s}\right)\zeta(s)$

Also, $\sum a_n$ for $\zeta_r$ are bounded by $r-1$.

$\therefore$ $\zeta_r$ has abscissa of convergence $=0$.

$\zeta(s) = \zeta_r(s) \Big/ \left(1 - \frac{1}{r^{s-1}}\right)$. If $\zeta(s)$ has a pole at $s \neq$ then $r^{s-1} = 1$

$2^{s-1} = 1 \Rightarrow s = 1 + \frac{2\pi i n}{\log 2}$, for some $n \in \mathbb{Z}$.

$3^{s-1} = 1 \Rightarrow s = 1 + \frac{2\pi i m}{\log 3}$, $m \in \mathbb{Z}$

$\Rightarrow \frac{n}{\log 2} = \frac{m}{\log 3} \Rightarrow n \log 3 = m \log 2$

$\Rightarrow 3^n = 2^m \Rightarrow n = m = 0$ //

(2.7) **Theorem**: Let $\{a_n\}$ a sequence, and $0 \leq \sigma_1 < 1$.

Assume $\exists$ nonzero $\rho$, $C > 0$ s.t.

$$\left| \sum_{k=1}^{n} a_k - \rho n \right| \leq C n^{\sigma_1} \quad \forall n \geq 1.$$

Then $f(s) = \sum_{k=1}^{\infty} \frac{a_k}{k^s}$ converges for $\mathrm{Re}(s) > 1$, and has analytic cont. for $\mathrm{Re}(s) > \sigma_1$, where it is analytic except for a simple pole at $s=1$, with residue $\rho$.

Pf

$|a_1 + \dots + a_n| \leq |\rho| n + O(n^{\sigma_1}) = O(n)$, so $f(s)$ converges for $\mathrm{Re}(s) > 1$.

Apply now (2.5) to $f(s) - \rho \zeta(s) =: g(s)$.

So $g(s)$ converges for $\mathrm{Re}(s) > \sigma_1$.

Then $f(s) = \underset{\substack{\text{analy. cont.} \\ \mathrm{Re}(s) > \sigma_1 \geq 0}}{g(s)} + \underbrace{\rho \zeta(s)}$ $\uparrow$ analytic cont $\mathrm{Re}(s) > 0$

And also $f(s)$ has a simple pole at $s=1$ with residue $\rho$:

$$\lim_{s \to 1} (s-1) f(s) = \lim_{s \to 1} \cancelto{0}{(s-1)} g(s) + \rho \lim_{s \to \infty} (s-1) \zeta(s) = \rho . 1 = \rho.$$

Let $K$ be a number field, $c$ an ideal class.

$$\zeta_K(s,c) = \sum_{\substack{\mathfrak{a} \subseteq \mathcal{O}_K \\ \mathfrak{a} \in c}} \frac{1}{N(\mathfrak{a})^s} \quad \text{(partial zeta function).}$$

We found that $j(c,t) = \#$ ideals in $c$ with norm $\leq t\}$.

Let $a_n = \#$ ideals in $c$ of norm $n$.

Then $\zeta_K(s,c) = \sum_{k=1}^{\infty} \frac{a_k}{k^s}$.

Then $j(c,n) = \sum_{k=1}^{n} a_k$. We had $j(c,t) = \rho t + O(t^{1-\frac{1}{N}})$ for $N = [K:\mathbb{Q}]$.

Recall that $\rho$ is independent of $c$.

(2.8) Theorem:

a) $\zeta_K(s,c)$ has an analytic continuation for $\mathrm{Re}(s) > 1 - \frac{1}{N}$, where it is analytic except for a simple pole at $s=1$, with residue $\rho$.

b) $\zeta_K(s)$ has a similar result, but with residue $h\rho$, $h = \# Cl(K)$.

Pf/ Direct from (2.7). //

Now let $\mathfrak{m} = \mathfrak{m}_0 \cdot \mathfrak{m}_\infty$ be a modulus, and let $c \in I(\mathfrak{m}) / \underbrace{P_{\mathfrak{m}}}_{\{(\alpha) :\ \alpha \equiv 1 \bmod^* \mathfrak{m}\}}$.

Consider the partial zeta function:

$$\zeta_K(s, c, \mathfrak{m}) = \sum \frac{1}{N(\mathfrak{a})^s}$$ where the sum runs over $\{\mathfrak{a} \in c : (\mathfrak{a}, \mathfrak{m}_0) = 1\}$.

This function has a residue, say $\rho_{\mathfrak{m}}$ at $s=1$ (see Lang).

Let $h_{\mathfrak{m}} = \#\left( I(\mathfrak{m}) / P_{\mathfrak{m}} \right)$.

We want to compare $h \cdot \rho$ with $h_{\mathfrak{m}} \cdot \rho_{\mathfrak{m}}$.

Euler Product:

Know that $\zeta(s) = \sum \frac{1}{n^s} = \prod_p (1 - p^{-s})^{-1}$, $\mathrm{Re}(s) > 1$.

Also, $\zeta_K(s) = \sum \frac{1}{N(\mathfrak{a})^s} = \prod_{\substack{\mathfrak{p} \neq 0 \\ \text{prime ideals}}} \left(1 - N(\mathfrak{p})^{-s}\right)^{-1}$ (because $\mathcal{O}_K$ is a Dedekind domain → UFD).

Observe that

$$\zeta_K(s) = \left( \sum_{c \in I(\mathfrak{m})/P_{\mathfrak{m}}} \zeta_K(s, c, \mathfrak{m}) \right) \cdot \prod_{\mathfrak{p} | \mathfrak{m}_0} \left( \frac{1}{1 - N(\mathfrak{p})^{-s}} \right).$$

Let $s \to 1^+$ and multiply by $s-1$. Get:

$$h \cdot \rho = h_{\mathfrak{m}} \rho_{\mathfrak{m}} \cdot \prod_{\mathfrak{p} | \mathfrak{m}_0} \left(1 - N(\mathfrak{p})^{-1}\right)^{-1}$$ ← formula for $h_{\mathfrak{m}}/h$. ↙ it's an integer!

- Infinite Products

Suppose $\{a_n\}$ a sequence with $a_1 = 1$.
It is multiplicative if $a_n a_m = a_{nm}$ whenever $(n,m)=1$

Lemma 2.9: Suppose $\{a_n\}$ is multiplicative and bounded. Then:

$$\sum \frac{a_n}{n^s} = \prod_{p \text{ prime}} \left( 1 + \frac{a_p}{p^s} + \frac{a_{p^2}}{p^{2s}} + \cdots \right)$$

(and the Dirichlet series is absolutely convergent for $Re(s)>1$).

Pf/ Let $S$ be a finite set of primes. Let $\mathbb{N}(S) = \{ n \in \mathbb{N} : p \mid n \Rightarrow p \in S \}$.

Then $$\sum_{n \in \mathbb{N}(S)} \frac{a_n}{n^s} = \prod_{p \in S} \left( 1 + \frac{a_p}{p^s} + \frac{a_{p^2}}{p^{2s}} + \cdots \right)$$

Now let $S$ increase ← that's NOT a proof!

→ Furthermore, if $a_{p^k} = (a_p)^k$ $\forall p$ (completely multiplicative),

then $$\sum \frac{a_n}{n^s} = \prod_p \left( 1 - \frac{a_p}{p^s} \right)^{-1}.$$

Now let again $\zeta(s) = \prod_p (1-p^{-s})^{-1}$, $Re(s)>1$.

$$\log \zeta(s) = -\sum_p \log\left(1 - \frac{1}{p^s}\right) = \sum_p \sum_{m=1}^{\infty} \frac{1}{m p^{ms}} = \sum_p \left( \frac{1}{p^s} + \sum_{m=2}^{\infty} \frac{1}{m p^{ms}} \right)$$

The series $\displaystyle\sum_p \sum_{m=2}^{\infty} \frac{1}{m p^{ms}}$ is absolutely and uniformly convergent

for $\sigma = Re(s) \geq \frac{1}{2} + \delta$, $\delta > 0$.

define $r = \frac{1}{p^\sigma}$

Estimate: $$\sum_{m=2}^{\infty} \frac{1}{m p^{m\sigma}} \leq \frac{1}{2} \sum_{m=2}^{\infty} \frac{1}{p^{m\sigma}} = \cdots = \frac{1}{2} \frac{r^2}{1-r} < \frac{1}{2} r^2 = \frac{1}{2} \frac{1}{p^{2\sigma}}.$$

So $\displaystyle\sum_p \sum_{m \geq 2} (\;) \leq \frac{1}{2} \sum_n \frac{1}{n^{2\sigma}}$ ⇒ converges.

Hence the pole comes from $\displaystyle\sum_p \frac{1}{p^s}$. Taking $s \to 1$, we get $\sum \frac{1}{p}$ diverges.

Note: Hecke (1917) proved the functional equation for $\zeta_K(s)$ (which implies meromorphic extension). (see the corresp. chapter in Lang).

Consider $\log\left(\prod_{\mathfrak{p}} \frac{1}{1-\frac{1}{(N\mathfrak{p})^s}}\right) = \sum_{\mathfrak{p}} \sum_{m=1}^{\infty} \frac{1}{m\, N(\mathfrak{p})^{ms}}$ $(Re(s)>1)$

Write it as $\sum_{\mathfrak{p}} \frac{1}{(N\mathfrak{p})^s} + \sum_{\mathfrak{p}} \sum_{m\geq 2} \frac{1}{m(N\mathfrak{p})^{ms}}$

Suppose $\mathfrak{p} \cap \mathbb{Z} = (p)$. Then $N(\mathfrak{p}) = p^{f_{\mathfrak{p}}} \Rightarrow \frac{1}{(N\mathfrak{p})^{\sigma}} \leq \frac{1}{p^{\sigma}}$ $(\sigma = Re(s))$

and at most $(K:\mathbb{Q})$ primes $\mathfrak{p}$ divide $p$.

Therefore, $\sum_{m\geq 2} \frac{1}{m(N\mathfrak{p})^{m\sigma}}$ is dominated by $(K:\mathbb{Q}) \cdot \sum_{m\geq 2} \frac{1}{p^{m\sigma}}$ (converges for $\sigma>1$).

Therefore, $\log \zeta_K(s) = \sum_{\mathfrak{p}} \frac{1}{N(\mathfrak{p})^s} + g(s)$, $g(s)$ bounded for $s$ near $1$.

(Notation: Suppose $f_1, f_2$ have a singularity at $s=1$. Write $f_1 \sim f_2$ if $f_1 - f_2$ is analytic at $s=1$.)

(So we can say $\zeta(s) \sim \frac{1}{s-1}$, $\log \zeta(s) \sim \sum_p \frac{1}{p^s}$)

And so $\zeta_K(s) \sim \frac{\rho h}{s-1}$; $\log \zeta_K(s) \sim \log\left(\frac{1}{s-1}\right) \sim \sum_{\mathfrak{p}} \frac{1}{(N\mathfrak{p})^s} \sim \sum_{\substack{\mathfrak{p} \\ \text{of degree } 1 \\ (\text{i.e. } f_{\mathfrak{p}}=1)}} \frac{1}{(N\mathfrak{p})^s}$.

- Dirichlet Series

Recall $L(\chi, s) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$ ($\chi$ a Dirichlet character).

Character groups

$G$ a finite abelian group.

$\hat{G} := \mathrm{Hom}(G, \mathbb{C}^{\times})$. (Character group)

$\hat{G}$ is an abelian group ( $(\chi_1\chi_2)(x) = \chi_1(x)\cdot\chi_2(x)$ ).

If $g^k = 1$ ($g \in G$), $\chi \in \hat{G}$, then $\chi^k(g) = \chi(g^k) = \chi(1) = 1 \Rightarrow \chi(g) \in \mu_k$.

(could so write $\hat{G} = \mathrm{Hom}(G, \mu_m)$ where $m = \#G$ ).

Theorem: Let $G$ be a finite abelian gp. Then $G \simeq \hat{G}$ (non-canonically)

Pf/ Case 1: $G$ cyclic, $G = \langle g_0 \rangle$ of order $d$.

Each $\chi \in \hat{G}$ is determined by $\chi(g_0) \in \mu_d$

Suppose $\chi_j \in \hat{G}$, satisfy $\chi_j(g_0) := e^{\frac{2\pi i j}{d}}$. ($0 \le j < d$)

These are $d$ distinct characters and there cannot be more.

Case 2: Write $G = G_1 \times \dots \times G_t$, $G_j$ cyclic. $1 \le j \le t$.

Then we have $\hat{G} \simeq \hat{G}_1 \times \dots \times \hat{G}_t$. (easy check)

For a subgroup $H \subseteq G$, have

$$\begin{tikzcd}
\mathrm{res} : \mathrm{Hom}(G, \mathbb{C}^{\times}) \arrow[r] \arrow[d, phantom, "\shortparallel"] & \mathrm{Hom}(H, \mathbb{C}^{\times}) \\
\hat{G} \arrow[r] & \hat{H}
\end{tikzcd}$$

Theorem: $H$ sbgp of finite ab. $G$, then exact the sequence:

$$1 \to H \to G \to G/H \to 1$$

Gives an exact sequence:

$$1 \to \widehat{G/H} \to \hat{G} \to \hat{H} \to 1.$$

Pf of thm (direct):

$$1 \longrightarrow (G/H)^\wedge \longrightarrow \hat{G} \xrightarrow{r} \hat{H} \longrightarrow 1$$

to show $r$ onto, we'll show that $|\ker r|$ is correct:

$$\ker r = \{\chi \in \hat{G} : \chi(H) = 1\} \quad (= H^\perp).$$

To $\chi \in \ker r$, associate $\bar{\chi} \in (G/H)^\wedge$ by $\bar{\chi}(gH) = \chi(g)$ $(g \in G)$.

Conversely, to $\psi \in (G/H)^\wedge$, associate $\chi \in \ker r$ by $\chi(g) := \psi(gH)$.

We have then $\ker r \simeq (G/H)^\wedge$.

Then $r$ is onto because $|\operatorname{Im} r| = \frac{|\hat{G}|}{\ker r} = \frac{|\hat{G}|}{|(G/H)^\wedge|} = |H| = |\hat{H}|$.

(2.11) Lemma: Let $G$ be a finite abelian group, $\chi \in \hat{G}$. Then:

a) $$\sum_{g \in G} \chi(g) = \begin{cases} |G| & \text{if } \chi = 1 \\ 0 & \text{otherwise} \end{cases}$$

b) $$\sum_{\chi \in \hat{G}} \chi(g) = \begin{cases} |G| & \text{if } g = 1 \\ 0 & \text{otherwise} \end{cases}$$

Proof

(a) $\chi \neq 1$ (if $\chi = 1$, result is obvious).

Then $\exists g_0 \in G$, $\chi(g_0) \neq 1$. Then:

$$\sum_g \chi(g) = \sum_g \chi(gg_0) = \underset{\neq 1}{\chi(g_0)} \cdot \sum_g \chi(g) \Rightarrow \sum \chi(g) = 0.$$

(b) $g \neq 1$. Then $\exists \chi_0$ s.t $\chi_0(g) \neq 1$. Then do the same.

Hint: consider $(G/\langle g_0 \rangle)^\wedge$

Recall that Dirichlet chars are usually def on $(\mathbb{Z}/m\mathbb{Z})^\times$.

Consider the modulus $\mathfrak{m} = (m)\cdot V_\infty$. Then know that $(\mathbb{Z}/m\mathbb{Z})^\times \simeq I(\mathfrak{m})/P_\mathfrak{m}$ (r. class gp)

So now let $\chi$ be a character of $I_K(\mathfrak{m})/P_\mathfrak{m}$ (finite abelian group!).

(for a given modulus $\mathfrak{m}$).

Then have $\underset{\text{L-series}}{L_\mathfrak{m}}(s,\chi) = \sum \frac{\chi(\mathfrak{a})}{(N\mathfrak{a})^s}$ where the sum goes over $\mathfrak{a}$ s.t $(\mathfrak{a},\mathfrak{m})=1$

$$\left( L_\mathfrak{m}(s,\chi) = \prod_{\mathfrak{p}\nmid \mathfrak{m}_0} \left(1 - \frac{\chi(\mathfrak{p})}{(N\mathfrak{p})^s}\right)^{-1} \right).$$

This converges absolutely and uniformly for $\mathrm{Re}(s) \geq 1+\delta$, $\delta > 0$.

**Theorem (2.12):** $K$ a number field, $(K:\mathbb{Q}) = N$, $\chi \neq 1$ a character of $I_K(\mathfrak{m})/P_\mathfrak{m}$.

Then $L_\mathfrak{m}(s,\chi)$ converges for $\mathrm{Re}(s) > 1 - \frac{1}{N}$ and is analytic there.

(e.g. $1 - \frac{1}{3^s} + \frac{1}{5^s} - \cdots$ converges for $\mathrm{Re}(s) > 0$).

Proof:

$$\sum_{\substack{N\mathfrak{a}\leq n \\ (\mathfrak{a},\mathfrak{m})=1}} \chi(\mathfrak{a}) = \sum_{c \in I_\mathfrak{m}/P_\mathfrak{m}} \chi(c) \underbrace{\left(\sum_{\substack{\mathfrak{a}\in c \\ N\mathfrak{a}\leq n}} 1\right)}_{j(c,n)} = \sum_{c\in I_\mathfrak{m}/P_\mathfrak{m}} \chi(c)\left(\rho_\mathfrak{m}\cdot n + O(n^{1-\frac{1}{N}})\right) =$$

$$= \left(\rho_\mathfrak{m}\cdot n \cdot \sum_c \chi(c)\right) + O(n^{1-\frac{1}{N}}) \underset{\uparrow}{=} O(n^{1-\frac{1}{N}})$$ . Apply the (2.5) for the conclusion.

(Recall that if $\chi \neq 1$, on fin. ab gp $G$, then $\sum_{c\in G} \chi(c) = 0$.)

//

- Dirichlet density

Let $K$ be a number field. A subset $S$ of prime ideals of $K$ has Dirichlet density $\delta(S)$ if the following limit exists:

$$\delta(S) := \lim_{s \to 1^+} \left( \frac{\sum_{\mathfrak{p} \in S} \frac{1}{(N\mathfrak{p})^s}}{\sum_{\text{all } \mathfrak{p}} \frac{1}{(N\mathfrak{p})^s}} \right) \left( = \lim_{s \to 1^+} \frac{\sum_{\mathfrak{p} \in S} \frac{1}{(N\mathfrak{p})^s}}{\log\left(\frac{1}{s-1}\right)} \right)$$

we saw that $\log \frac{1}{s-1}$ has a [illegible] form as the other denominator.

Fact: If the natural density exists, then it equals the Dirichlet density.

(see pf. in Prachar, Apostol or Serre).

Trivial: $0 \leq \delta(S) \leq 1$.

Let $S_K = \{$ primes of $K$ of degree $1$ $(N\mathfrak{p} = p)\}$.

Then:

Lemma: $\delta(S_K) = 1$, and if $T$ is a subset of primes, $\delta(T) = \delta(T \cap S_K)$.

Def: $L/K$ a finite extension. A prime $\mathfrak{p}$ of $K$ splits completely (s.c) in $L$ if $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1 \cdots \mathfrak{P}_g$, $g = (L:K)$, $\mathfrak{P}_i$ distinct primes of $L$.

Lemma: if $L/K$ is Galois, then $\mathfrak{p}$ s.c. in $L \Leftrightarrow \begin{cases} \mathfrak{p} \text{ unramified in } L \\ \text{and} \\ \exists \mathfrak{P} \text{ of } L \text{ s.t. } N_{L/K}\mathfrak{P} = \mathfrak{p} \end{cases}$

Def Define $\mathrm{Split}(L/K) = \{ \mathfrak{p}$ of $K$ st $\mathfrak{p}$ s.c. in $L \}$.

Example: $m > 1$, then $\mathrm{Split}\left(\mathbb{Q}(\sqrt[m]{1})/\mathbb{Q}\right) = \{ p$ primes s.t $p \equiv 1 \pmod{m} \}$.

Example, $\mathrm{Split}\left(\mathbb{Q}(\sqrt{5})/\mathbb{Q}\right) = \{ p$ st $p \equiv \pm 1 \, (5) \}$

Rk; in Marcus, pg 91 he proves that there are $\infty$ly many primes $\equiv 1 \pmod{m}$.

(2.13) Theorem: $L/K$ galois. Then

$$\delta(\mathrm{Split}(L/K)) = \frac{1}{(L:K)}$$

Pf Let $S_L^\circ := \{\mathfrak{P} \in S_L : \mathfrak{P} \text{ unramified over } K\}$.

~~Have~~ the norm mapping $N_{L/K} : S_L^\circ \longrightarrow S_K \cap \mathrm{Split}(L/K)$

Check: it is onto, and $(L:K)$-to-$1$.

Then: $$\sum_{\mathfrak{P}\in S_L^\circ} \frac{1}{(N_{L/\mathbb{Q}}\mathfrak{P})^s} = (L:K)\cdot \sum_{\mathfrak{p}\in S_K\cap \mathrm{Split}(L/K)} (N_{K/\mathbb{Q}}\mathfrak{p})^s \qquad (\mathrm{Re}(s)>1).$$

Thus $\delta(S_L^\circ) = (L:K)\cdot \delta(S_K \cap \mathrm{Split}(L/K)) = (L:K)\cdot\delta(\mathrm{Split}(L/K))$.

$\delta(S_L^\circ) = \delta(S_L) = 1$

So $\delta(\mathrm{Split}(L/K)) = \frac{1}{(L:K)}$ //

Look at the map $N_{L/K} : I_L \longrightarrow I_K$, consider then $I_K(\mathfrak{m})$, $I_L(\mathfrak{m})$.

Let $\eta(\mathfrak{m}) = N_{L/K}(I_L(\mathfrak{m}))$, which is a subgroup of $I_K(\mathfrak{m})$.

Main Theorem: $L/K$ abelian. Have the Artin map $\omega : I_K(\mathfrak{m}) \longrightarrow \mathrm{Gal}(L/K)$.

1) $\omega$ is onto.

2) $\exists\, \mathfrak{m}$ s.t. $\omega(P_\mathfrak{m}) = 1$. (existence of conductor).

2') $\omega(\eta(\mathfrak{m})) = 1$

3) $(I_K(\mathfrak{m}) : \eta(\mathfrak{m})P_\mathfrak{m}) \leq (L:K)$ (universal norm inequality).

Corollary: $$I_K(\mathfrak{m})\big/\eta(\mathfrak{m})P_\mathfrak{m} \simeq \mathrm{Gal}(L/K).$$

(2.14) Theorem (Weber): $L/K$ Galois, $\mathfrak{m}$ a modulus of $K$.

Let $\mathfrak{N}_{L/K}(\mathfrak{m}) := N_{L/K}(I_L(\mathfrak{m}))$. Then,

$$(I_K(\mathfrak{m}) : P_{\mathfrak{m}}\mathfrak{N}_{L/K}(\mathfrak{m})) \le (L:K).$$

We will prove (2.14) using:

(2.15) Prop: $\delta(K\text{-primes} \cap P_{\mathfrak{m}}\mathfrak{N}(\mathfrak{m})) = \dfrac{1}{(I(\mathfrak{m}) : P_{\mathfrak{m}}\mathfrak{N}(\mathfrak{m}))}$

Show how (2.15) $\Rightarrow$ (2.14):

Note $\text{split}(L/K) \subseteq P_{\mathfrak{m}}\mathfrak{N}(\mathfrak{m}) \cup \overbrace{\{\text{primes } \mathfrak{p} : \mathfrak{p} \mid \mathfrak{m}\}}$ ← a finite set

So $$\underset{\overset{\|(2.13)}{\frac{1}{(L:k)}}}{\delta(\text{split}(L/K))} \le \delta(K\text{-primes} \cap P_{\mathfrak{m}}\mathfrak{N}(\mathfrak{m})) \overset{(2.15)}{=} \frac{1}{(I(\mathfrak{m}) : P_{\mathfrak{m}}\mathfrak{N}(\mathfrak{m}))}$$ //

(Proof of 2.15)

Let $H := P_{\mathfrak{m}}\mathfrak{N}_{L/K}(\mathfrak{m})$, $h' := (I(\mathfrak{m}) : H)$. (note that it's finite $\le h_{\mathfrak{m}}$).

Any character $\chi$ of $I(\mathfrak{m})/H$ can be lifted to a character on $I(\mathfrak{m})/P_{\mathfrak{m}}$, by $I(\mathfrak{m})/P_{\mathfrak{m}} \longrightarrow I(\mathfrak{m})/H \xrightarrow{\chi} \mathbb{C}$, and still call it $\chi$.

Form the Dirichlet series: $$L_{\mathfrak{m}}(s,\chi) = \sum_{(\mathfrak{a},\mathfrak{m})=1} \frac{\chi(\mathfrak{a})}{(N\mathfrak{a})^s} = (s-1)^{r(\chi)} \cdot b(s,\chi)$$

(where $b(1,\chi) \neq 0$ and $r(\chi) = \begin{cases} -1 & \chi = \chi_0 \\ \ge 0 & \chi \neq \chi_0 \end{cases}$)

Taking logs: $\log L_{\mathfrak{m}}(s,\chi) \sim -r(\chi) \cdot \log \dfrac{1}{s-1}$

But also we know $$\log L_{\mathfrak{m}}(s,\chi) \sim \sum_{\mathfrak{p} \nmid \mathfrak{m}} \frac{\chi(\mathfrak{p})}{(N\mathfrak{p})^s} = \sum_{c \in I(\mathfrak{m})/H} \chi(c) \cdot \sum_{\mathfrak{p} \in c} \frac{1}{(N\mathfrak{p})^s}$$

↓

We now sum over all characters $\chi$ on $I(m)/H$, to get:

$$-\log\left(\frac{1}{s-1}\right)\sum_{\chi} r(\chi) \sim \sum_{\chi}\left(\sum_{c}\chi(c)\sum_{p\in c}\frac{1}{(Np)^s}\right) = \sum_{c}\left(\overbrace{\sum_{\chi}\chi(c)}^{\text{usually } 0\ (c\neq 1!)}\right)\cdot\sum_{p\in c}\frac{1}{(Np)^s} =$$

$$= h'\cdot\sum_{p\in H}\frac{1}{(Np)^s}.$$

So:

$$\frac{1}{h'}\log\left(\frac{1}{s-1}\right)\left(1-\sum_{\chi\neq\chi_0} r(\chi)\right) \sim \sum_{p\in H}\frac{1}{(Np)^s}$$

Divide both sides by $\log\left(\frac{1}{s-1}\right)$ and let $s\to 1^+$, to get, by definition of Dirichlet density $\delta$:

$$\delta_H := \delta\left(K\text{-primes} \cap H\right) = \frac{1}{h'}\left(1-\sum_{\chi\neq\chi_0} r(\chi)\right).$$

Note $\delta_H > 0$, since $H = \mathfrak{N}(m)\cdot P_m$ contains the split primes (with a finite number of exceptions). (and split primes have positive density!)

For $\chi\neq\chi_0$, $r(\chi)\geq 0$ and integer. Thus $r(\chi)=0$ $\forall\, \chi\neq\chi_0 \Rightarrow$ ✓
(which implies $L_m(1,\chi)\neq 0$ for $\chi\neq\chi_0$)

Corollary (of proof):
Given a Galois extension $L/K$, and $\chi\neq\chi_0$ a character of $I(m)/P_m\mathfrak{N}(m)_{L/K}$, then $L_m(1,\chi)\neq 0$.

Caution!: we have not yet proved that for $\chi\neq\chi_0$ character of $I(m)/P_m$, that $L_m(1,\chi)\neq 0$, because we have not yet shown that $\exists\, L/K$ Galois with $\mathfrak{N}(m)\subseteq P_m$ (so that $P_m\mathfrak{N}(m)=P_m$).

However, for the special case $K=\mathbb{Q}$, $L=\mathbb{Q}(\sqrt[m]{1})$ and $m=(m)\infty$, then we know that the norms are in $P_m$.

Hence $L_m(1,\chi)\neq 0$ ($\chi\neq\chi_0$ character on $I(m)/P_m \simeq (\mathbb{Z}/m\mathbb{Z})^{*}$).

## Idea on "How to remove the $\mathfrak{m}$"

For each prime $v$ of $K$ (finite or infinite), let $K_v$ be the completion of $K$ at $v$. Consider $\prod_{v \text{ prime of } K} K_v^\times$, note that $K^* \hookrightarrow \prod K_v^\times$ (diagonally).

Def The idèle group $J_K \subseteq \prod K_v^\times$, ~~st. [illegible]~~

Actually $K^\times \hookrightarrow J_K$, and can define a norm $N_{L/K} : J_L \to J_K$ (using local norms).

Then (2.14) takes the form: $\boxed{\left(J_K : K^\times N_{L/K}(J_L)\right) \leq (L:K).}$ (*)

Def The idèle group is defined as follows:

Let $a=(a_v) \in \prod_v K_v^\times$, $a_v \in K_v^\times$.

Let $\mathcal{O}_v$ = valuation ring of $K_v$ for $v$ finite; $\mathcal{O}_v^\times$ = units of $\mathcal{O}_v$.

Let $\mathcal{O}_v^\times := K_v^\times$ for $v$ infinite primes. ($= \mathbb{R}^\times, \mathbb{C}^\times$).

Then $J_K = \{ a = (a_v) : a_v \in \mathcal{O}_v^\times$ for all but finitely-many $v \}$.

$L/K$ Galois, $K \subseteq L' \subseteq L$ where $L'$ = max abelian ext. of $K$ in $L$.

Then $\left(J_K : K^\times N_{L/K}(J_L)\right) = (L' : K)$ (so have equality for abelian).

But this result is difficult (we'll prove it later).

Next, assuming results from CFT, we'll prove the theorem on the density of primes in arithmetic progressions.

In fact, assume that $\forall$ sgp $H$ st $I_K(\mathfrak{m}) \supseteq H \supseteq P_{\mathfrak{m}}$, then $\exists$ an abelian extension $L/K$ with $H = \mathfrak{N}_{L/K}(\mathfrak{m}) P_{\mathfrak{m}}$.

(we will prove this result later).

Assuming this,

Theorem 2.16: $L_{\mathfrak{m}}(1,\chi) \neq 0$, $\chi \neq \chi_0$ for $\chi \in \left(I_K(\mathfrak{m})/H\right)^{\wedge}$.

Corollary: $I_K(\mathfrak{m}) \supseteq H \supseteq P_{\mathfrak{m}}$. Then the set of $K$-primes in $c_0 \in I(\mathfrak{m})/H$ has a (Dirichlet) density of $\dfrac{1}{(I_K(\mathfrak{m}):H)} =: \dfrac{1}{h'}$.

Pf/ Note that we know this already for $c_0 = 1 = H/H$.

Standard trick: for $\chi \in \left(I(\mathfrak{m})/H\right)^{\wedge}$,

$$\log L_{\mathfrak{m}}(s,\chi) \sim \sum_{\mathfrak{p} \nmid \mathfrak{m}} \frac{\chi(\mathfrak{p})}{(N\mathfrak{p})^s} = \sum_{c \in I(\mathfrak{m})/H} \chi(c) \cdot \sum_{\mathfrak{p} \in c} \frac{1}{(N\mathfrak{p})^s}$$

Multiply by $\chi(c_0^{-1})$ and sum over $\chi$:

$$\sum_{\chi} \chi(c_0^{-1}) \log L_{\mathfrak{m}}(s,\chi) \sim \sum_{\chi} \sum_{c} \chi(cc_0^{-1}) \sum_{\mathfrak{p} \in c} \frac{1}{(N\mathfrak{p})^s} =$$

$$= \sum_{c} \underbrace{\left(\sum_{\chi} \chi(cc_0^{-1})\right)}_{\substack{= 0 \text{ for } c \neq c_0 \\ = h' \text{ for } c \not\equiv c_0}} \cancel{\sum_{c}} \sum_{\mathfrak{p} \in c} \frac{1}{(N\mathfrak{p})^s}$$

So we get $h' \displaystyle\sum_{\mathfrak{p} \in c_0} \frac{1}{(N\mathfrak{p})^s}$ for RHS.

On the LHS, $L_{\mathfrak{m}}(1,\chi) \neq 0$ for $\chi \neq \chi_0$. Hence

$$LHS \sim \log L_{\mathfrak{m}}(s,\chi_0) \sim \log \frac{1}{s-1} \Rightarrow \log \frac{1}{s-1} \sim h' \sum_{\mathfrak{p} \in c_0} \frac{1}{(N\mathfrak{p})^s}$$

The result follows taking the limit as $s \to 1$. //

Special case: $K=\mathbb{Q}$, $L=\mathbb{Q}(\zeta_m)$, $\mathfrak{m}=(m)\infty$, then:

$$I(\mathfrak{m})/H = I_\mathfrak{m}/P_\mathfrak{m} \simeq (\mathbb{Z}/m\mathbb{Z})^\times . \quad \left(\text{because we know } P_\mathfrak{m} = P_\mathfrak{m}\cdot \mathbf{N}_{L/\mathbb{Q}}(\mathfrak{m})\right).$$

So given integer $a$, $(a,m)=1$, then $\exists$ infinitely-many primes $p\equiv a \pmod m$. (And their density is $\frac{1}{\phi(m)}$).

- Characterize Galois extensions $L$ of $K$ by means of $\mathrm{Split}(L/K)$ $\left(=\{\mathfrak{p} \text{ of } K \text{ st } \mathfrak{p} \text{ splits completely in } L\}\right)$.

(2.18) Theorem (Bauer):

Let $M, L$ be Galois extensions of $K$. TFAE:

a) $L\subseteq M$ — should be written $\prec$: $S,T$ sets of primes of $K$. Then $S\prec T$ means $\exists\, S_0\subseteq S$ with density $0$ s.t. $S\setminus S_0\subseteq T$.

b) $\mathrm{Split}(M/K) \underset{\prec}{\cancel{\subseteq}} \mathrm{Split}(L/K)$

pf/ a ⇒ b trivial.

b ⇒ a:

Example: $M=\mathbb{Q}(\zeta_8)$, $L=\mathbb{Q}(\sqrt{-2})$.

$$\left.\begin{array}{l}\mathrm{Split}(M/\mathbb{Q}) = \{p : p\equiv 1\ (8)\}.\\ \mathrm{Split}(L/\mathbb{Q}) = \{p : \left(\frac{-2}{p}\right)=1\} = \{p : p\equiv 1,3 \pmod 8\}.\end{array}\right\} \overset{\text{Bauer}}{\Rightarrow} L\subseteq M.$$

Example: $\mathbb{Q}(\zeta_{20})\supset\mathbb{Q}(i,\sqrt5)\supset\mathbb{Q}(i)$. Look at $\mathrm{Split}(\ /\mathbb{Q})$. (exercise)

Before proving Bauer, we show that the Artin map is onto.

(2.17) Theorem: Let $L/K$ be an abelian extension and $\omega_{L/K}: I_K(\mathfrak{m})\longrightarrow \mathrm{Gal}(L/K)$ be the Artin map ($\mathfrak{m}$ divisible by primes $\mathfrak{p}$ ramified in $L/K$).

(recall that $\omega(\mathfrak{p}) = (\mathfrak{p}, L/K) := (\mathfrak{P}, L/K)$, $\mathfrak{P}$ dividing $\mathfrak{p}$).

Then $\omega$ is onto.

Proof:

Review first the decomposition gp $D_\mathfrak{p} (= D_\mathfrak{P}) = \{ \sigma \in Gal(L/K) : \sigma\mathfrak{P} = \mathfrak{P} \}$.

Then recall $D_\mathfrak{p} = \langle (\mathfrak{p}, L/K) \rangle$ if $\mathfrak{p}$ is unramified (cyclic of order $f$).

Also, $L^{D_\mathfrak{P}}$ = decomposition field

Fact: $\mathfrak{p}$ splits completely in $L^{D_\mathfrak{P}}/K$.

Let now $H := \mathrm{im}\,\omega \subseteq Gal(L/K)$.

Note that $\forall \mathfrak{p} \nmid m$, $D_\mathfrak{p} \subseteq H$. ($H$ is generated by all $(\mathfrak{p}, L/K)$).

$$\begin{tikzcd}
L \arrow[d, dash] \\
L^{D_\mathfrak{p}} \arrow[d, dash] \\
L^H \arrow[d, dash] \\
K
\end{tikzcd}$$

So if $\mathfrak{p} \nmid m$, then $\mathfrak{p}$ splits completely in $L^H/K$.

Hence $\delta(Split(L^H/K)) = 1 \underset{(2.13)}{\Rightarrow} 1 = \frac{1}{h'} \Rightarrow h' = 1 \Rightarrow L^H = K \Rightarrow H = Gal(L/K)$

## (2.18) Bauer's Theorem

$M, L$ Galois ext of $K$, then $L \subseteq M \Leftrightarrow Split(M/K) \prec Split(L/K)$.

Pf/ $\Rightarrow$ ✓

$\Leftarrow$) Consider:

$$\begin{tikzcd}
 & LM \arrow[dl, dash] \arrow[dr, dash] & \\
L \arrow[dr, dash] & & M \arrow[dl, dash] \\
 & K &
\end{tikzcd}$$

Fact (Marcus, p107, Thm 31): $Split(LM/K) = Split(M/K) \cap Split(L/K)$.

Thus, if $Split(M/K) \prec Split(L/K)$, then

$$\delta(Split(LM/K)) = \delta(Split(M/K))$$

So $\frac{1}{(LM:K)} = \frac{1}{(M:K)} \Rightarrow L \subseteq M$.

Remark: only need to assume that $M/K$ is a Galois extension.

Fact: $L/K$ an extension, and $L'$ = its normal closure. Then $Split(L/K) = Split(L'/K)$.

) Tchebotarev's Theorem: (density on nonabelian extensions $L/K$).

Q: Given $\sigma \in Gal(L/K)$, does it exist $\mathfrak{P}$ of $L$ such that $(\mathfrak{P}, L/K) = \sigma$ ?

Abelian case:

(2.19) Thm: The set of primes $\mathfrak{p}$ of $K$ s.t unramified in $L$ $(L/K$ abelian$)$, and s.t $(\mathfrak{P}, L/K) = \sigma$ ($\sigma$ given $\sigma \in Gal(L/K)$) has (Dirichlet) density $\frac{1}{(L:K)}$.

Proof: Assume $\exists$ sgp $H \subseteq I_K(\mathfrak{m})$ and a modulus $\mathfrak{m}$ s.t.

$$\omega_{L/K} : I_K(\mathfrak{m})/H \cong Gal(L/K). \qquad (H = N(\mathfrak{m}) \cdot P_{\mathfrak{m}}).$$

By Cor. to (2.16), we know that the density of primes in each class $c \in I_K(\mathfrak{m})/H$ is

$$\frac{1}{(I_K(\mathfrak{m}) : H)}.$$

Then take $\mathfrak{p}$ with $\omega(\mathfrak{p}) = \sigma$ to conclude the result. //

Ref: Nice book by F. Lemmermeyer, on Reciprocity Laws.

Non-abelian case: Let $G = Gal(L/K)$. For $\sigma \in G$, let $\mathcal{C}_\sigma$ = conjugacy class of $\sigma$, ie $\mathcal{C}_\sigma = \{\tau \sigma \tau^{-1} : \tau \in G\}$. (the conjugacy classes partition $G$).

If $\mathfrak{P}$ is over $\mathfrak{p}$, then $\mathfrak{P}^\tau = \{x^\tau : x \in \mathfrak{P}\}$ does also divide $\mathfrak{p}$. Also,

$$(\mathfrak{P}^\tau, L/K) = \tau (\mathfrak{P}, L/K) \tau^{-1}.$$

(2.20) Tchebotarev: $L/K$ Galois ext, $G = Gal(L/K)$, and let $C$ be any subset of $G$ stable under conjugation. Let $S = \{\mathfrak{p}$ of $K : \mathfrak{p}$ unram. in $L$ ; $\exists\, \mathfrak{P} \underset{L}{|} \mathfrak{p}$ with $(\mathfrak{P}, L/K) \in C\}$

Then $\delta(S) = \frac{|C|}{|G|}$

Rk: enough to prove it for $C$ a conjugacy class, as any subset of $G$ stable under conjugation is a union of conjugacy classes, and in the equation $\delta(S) = \frac{|C|}{|G|}$ both sides are additive.

Example: (Deuring): $L$ = splitting field of $X^3-2$, $L = \mathbb{Q}(\sqrt[3]{2}, \zeta_3)$.

Then $Gal(L/\mathbb{Q}) = S_3$.

$p$ unramified in $L$.

1) $p\mathcal{O}_L = P_1 \cdots P_6$. class $\{1\}$ → $\delta = \frac{1}{6}$.

2) $p\mathcal{O}_L = P_1 P_2 P_3$ $(f=2)$ class $\{(12),(13),(23)\}$ → $\delta = \frac{1}{2} \left(= \frac{3}{6}\right)$

3) $p\mathcal{O}_L = P_1 P_2$ $(f=3)$ class $\{(123),(132)\}$ → $\delta = \frac{2}{6} = \frac{1}{3}$

One obtains the type of $p$ by factoring $X^3-2$ mod $p$ $(p \neq 2,3)$.

Try with the first 3000 primes: get $\frac{490}{3000}$, $\frac{1512}{3000}$, $\frac{996}{3000}$.

Ref: Lagarias & Odlyzko, "Effective Tschebotarev". 1977 Durham proceedings on Alg. Number Fields (edited by Fröhlich).

Pf of Tchebotarev (due to Deuring + Milne + Lang + Ullom ...): (see Milne's notes pgs 216-217).

Recall $S = \{p$ of $K : p$ unram. in $L$ and $\exists$ prime $\mathfrak{P}$ prime of $L$ over $p$ : $(\mathfrak{P}, L/K) \in C\}$.

Proof: By the remarks, one can assume that $C$ is a conjugacy class of $\sigma \in G$.

Say $f$ = order of $\sigma$.

Let $\Sigma = L^{\langle\sigma\rangle}$ (fixed field). Hence $L/\Sigma$ is a cyclic extension.

$$\begin{tikzcd}[row sep=small] L \arrow[d, dash] & \mathfrak{P} \arrow[d, dash] \\ \Sigma \arrow[d, dash] & \mathfrak{Q} = \mathfrak{P} \cap \Sigma \arrow[d, dash] \\ K & p \end{tikzcd}$$

Assume $\exists$ modulus $m$ of $\Sigma$ s.t. $Gal(L/\Sigma) \overset{\text{Artin map}}{\simeq} I_\Sigma(m) / P_m N_{L/\Sigma}(m)$

(the reciprocity law for cyclic ext)

Omit the ramified primes and the divisors of $m$.

$\mathfrak{P} \mid \mathfrak{Q} \mid \mathfrak{p}$.

Define:

- $S_{\Sigma,\sigma} := \{\Sigma\text{-primes } \mathfrak{Q} : (\mathfrak{Q}; L/\Sigma) = \sigma \text{ and } f(\mathfrak{Q}\mid\mathfrak{p}) = 1\}$

By the abelian case (2.(9)), $\delta(\{\mathfrak{Q} \text{ of } \Sigma : (\mathfrak{Q}, L/\Sigma) = \sigma\}) = \frac{1}{(L:\Sigma)} = \frac{1}{f}$

and it follows that $\delta(S_{\Sigma,\sigma}) = \frac{1}{f}$ (the primes w/ $f>1$ have density $0$).

Define also:

- $S_{K,\sigma} = S \; (= \{K\text{-primes } \mathfrak{p} : \exists\, \mathfrak{P} \text{ of } L \text{ s.t. } (\mathfrak{P}, L/K) = \sigma\})$.
- $S_{L,\sigma} = \{L\text{-primes } \mathfrak{P} : (\mathfrak{P}, L/K) = \sigma\}$.

We are trying to show that $\delta(S_{K,\sigma}) = \dfrac{|\mathcal{C}_\sigma|}{|G|}$ ($\mathcal{C}_\sigma$ = conj. class of $\sigma$).

Two claims:

a) The map $\mathfrak{P} \mapsto \mathfrak{Q} = \mathfrak{P} \cap \Sigma$ defines a bijection $S_{L,\sigma} \longleftrightarrow S_{\Sigma,\sigma}$

b) The map $\mathfrak{P} \mapsto \mathfrak{p} = \mathfrak{P} \cap K$ defines a $d$-to-$1$ map (+onto) $S_{L,\sigma} \twoheadrightarrow S_{K,\sigma}$, where $d = \dfrac{g}{|\mathcal{C}_\sigma|}$, $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1 \cdots \mathfrak{P}_g$ //.

Assuming these claims, then it follows that the map $S_{\Sigma,\sigma} \to S_{K,\sigma}$ taking $\mathfrak{Q} \mapsto \mathfrak{Q} \cap K$ is onto and $d$-to-$1$.

For such primes $\mathfrak{Q}$, then $N_{\Sigma/K}(\mathfrak{Q}) = \mathfrak{p}$, so the absolute norms of $\mathfrak{Q}$ and $\mathfrak{p}$ are equal. Thus the series

$$\sum_{\mathfrak{p} \in S_{K,\sigma}} \frac{1}{(N(\mathfrak{p}))^s} = \frac{1}{d} \sum_{\mathfrak{Q} \in S_{\Sigma,\sigma}} \frac{1}{(N(\mathfrak{Q}))^s} \sim \frac{1}{d}\left(\frac{1}{f} \log \frac{1}{s-1}\right) = \frac{|\mathcal{C}_\sigma|}{\underbrace{\boxed{g \cdot f}}_{|G|}} \log \frac{1}{s-1}$$

//

Pf of the claims:

(a) $S_{L,\sigma} \to S_{\Sigma,\sigma}$ bijection:

First show $\mathfrak{P} \cap \Sigma \in S_{\Sigma,\sigma}$:

Let $\sigma = (\mathfrak{P}, L/K)$

~~$\forall \alpha \in \mathcal{O}_L, \alpha^\sigma = \alpha^{(\mathfrak{P}, L/K)} \equiv \alpha^{N\mathfrak{p}} \mod \mathfrak{P}$~~

~~Note now that, as $N\mathfrak{p} = NQ$, $\alpha^\sigma \equiv \alpha^{NQ} \equiv \alpha^{(Q, L/\Sigma)} \mod \mathfrak{P}$~~

(key: $\Sigma$ is the decomposition field of $\mathfrak{P} \Rightarrow f(Q/\mathfrak{p}) = 1$).

So then it is onto and $\mathfrak{P} \cap \Sigma \in S_{\Sigma,\sigma}$.)

The map is injective because $f(\mathfrak{P}, L/\Sigma) = [L:\Sigma] \Rightarrow \exists!$ prime $L$ above $Q$ //

(b) $\mathfrak{P} \mapsto \mathfrak{p} = \mathfrak{P} \cap K$ is $d$-to-1 onto:

General Lemma (2.21): $X, Y$ finite $G$-sets (sets with action of $G$), and assume $Y$ transitive (1 orbit). Let $\theta: X \to Y$ onto s.t. $\theta(\tau x) = \tau\theta(x)$ $\forall \tau \in G$ $\forall x \in X$ (ie a morphism of $G$-sets).

Then $\forall y \in Y$, $\#\theta^{-1}(\{y\}) = \dfrac{|X|}{|Y|}$.

Pf Let $S = \theta^{-1}(\{y\})$, $S' = \theta^{-1}(\{y'\})$, $y, y' \in Y$. Suppose $\theta(x) = y$.

Then by transitivity, $\exists \tau \in G$ s.t. $y' = \tau y$, so $\theta(\tau x) = \tau\theta(x) = \tau y = y'$.

Thus $\tau S \subseteq S' \Rightarrow |\tau S| \leq |S'| \Rightarrow |S| \leq |S'|$. By reversing, $|S| = |S'|$. //

$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1 \cdots \mathfrak{P}_g$, let $X = \{\mathfrak{P}_1, \ldots, \mathfrak{P}_g\}$, $Y = \{(\mathfrak{P}_i, L/K) : i = 1..g\} (= \mathcal{C}_\mathfrak{p})$.

$\theta(\mathfrak{P}_i) = (\mathfrak{P}_i, L/K)$. $(\theta(\mathfrak{P}_i^\tau) = \tau(\mathfrak{P}_i, L/K)\tau^{-1})$.

Applying the lemma, then $\theta$ is $d = \dfrac{|X|}{|Y|} = \dfrac{g}{|\mathcal{C}_0|}$ - to - 1.

So $\forall \mathfrak{p} \in S_{K,\sigma}$, exactly $d$ elements $\mathfrak{P}_i$ in $\{\mathfrak{P}_1, \ldots, \mathfrak{P}_g\}$ have the same Frobenius. //

Application (Lang, 2nd ed, pg 170).

Let $f(X) \in K[X]$ be irreducible.

Suppose that $f(X)$ has a root mod $\mathfrak{p}$ for a set of $K$-primes $\mathfrak{p}$s of density $1$.

Then $f$ has a root in $K$, hence $f$ is linear.

(or)

Suppose $f(x)$ has a root in $K_{\mathfrak{p}}$ (completion) for a set of primes of density $1$.

then $f$ has a root in $K$.

## Local Fields.

(See Fröhlich and Taylor; or Janusz, or N. Koblitz GTM 58 "p-adic numbers", ...).

~~Let~~ $K$ be a field. An abs value on $K$ is a function $K \to \mathbb{R}$,

$x \mapsto |x|$ s.t.
1) $|x| \geq 0$, $|x| = 0 \iff x = 0$
2) $|x \cdot y| = |x||y|$
3) $|x+y| \leq |x| + |y|$.

If stronger, 3') $|x+y| \leq \max\{|x|, |y|\}$ then it is called non-archimedean.

We exclude the trivial abs. value, $|x| = 1 \ \forall x \neq 0$.

$|\cdot|$ defines a topology on $K$, with distance $x$ to $y$ def. by $|x-y|$.

*Def*: Two A.V.'s $|\cdot|_1, |\cdot|_2$ are *equivalent* if they define the same topology.
(ie iff $\exists \alpha > 0$, s.t. $\forall x \in K$, $|\alpha|_1 = |\alpha|_2^{\alpha}$)

*Thm* (Ostrowski): Inequivalent A.V.'s on $\mathbb{Q}$ are given by $|\cdot|_\infty$ (usual) and one for each prime $p$, $|x|_p = p^{-r}$ if $x = p^r \frac{a}{b}$, $r \in \mathbb{Z}$, $p \nmid ab$.

Notice that if integers $N, M$ are s.t. $N \equiv M \bmod p^t$, $t$ *large*, then $|N-M|_p$ is *small*.

Let $(K, |\cdot|)$ a field with a given non-archimedean a.v.

Define the valuation ring $\{x \in K : |x| \leq 1\}$.

It's a local ring, with maximal ideal $\{x \in K : |x| < 1\}$.

We'll assume $\{|x| : x \in K^\times\} = \{c^n : n \in \mathbb{Z}\}$ (for some $0 < c < 1$).

Completion (K. Hensel).

(by analogy with $\mathbb{C}[T]$, $\overset{\text{nonzero}}{\text{primes}}$ have the form $(T-b)$ ⇝ completion leads $\mathbb{C}[[T]]$, power series).

If $K$ is a number field. The non-archimedean AV ⟺ prime ideals of $\mathcal{O}_K$.

$(K, |\cdot|)$ can be completed to $(\hat{K}, |\cdot|)$.

taking $\hat{K} = \{\text{Cauchy sequences}\} / \{\text{those with limit } 0\}$ ↙ maximal ideal ← it's a field.

$K \hookrightarrow \hat{K}$ densely via the constant Cauchy sequence $a \mapsto [(a, a, a, \dots)]$.

$\mathbb{R}$ = completion of $(\mathbb{Q}, |\cdot|_\infty)$

$\mathbb{Q}_p$ = completion of $(\mathbb{Q}, |\cdot|_p)$.

$\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x|_p \leq 1\}$, with unit group $\mathbb{Z}_p^\times = \{x \in \mathbb{Q}_p : |x|_p = 1\}$.

$p\mathbb{Z}_p$ maximal ideal $= \{x \in \mathbb{Q}_p : |x|_p < 1\}$.

Also. $p^i\mathbb{Z}_p / p^{i+1}\mathbb{Z}_p \cong p^i\mathbb{Z} / p^{i+1}\mathbb{Z}$ $\forall i \geq 0$.

Let $K$ be a number field (finite ext. of $\mathbb{Q}$)

The a.v. $(\mathbb{Q}, |\cdot|_p)$ can be extended to $K$, to get $(K, |\cdot|_v)$. One can then complete $(K, |\cdot|_v)$ to get $K_v$.

The extension $(K, |\cdot|_v)$ comes from a (nonzero) prime ideal $\mathfrak{p}$ in $\mathcal{O}_K$, because if the valuation ring $\mathcal{O} = \{x \in K : |x|_v \leq 1\}$ with max'l ideal $\mathfrak{m}$, then ~~(P~~ $\mathfrak{m} \cap \mathcal{O}_K$ is a nonzero prime ideal $\mathfrak{p}$, ~~[illegible]~~ of $\mathcal{O}_K$. (note $\mathcal{O}_K \subset \mathcal{O}$).

In fact, $\mathcal{O}$ = localization of $\mathcal{O}_K$ at $\mathfrak{p}$.

Conversely, each nonzero prime ideal of $\mathcal{O}_K$ gives a non-archimedean a.v.

$$\begin{tikzcd} & K_v \arrow[d, no head] \\ K \arrow[ur] \arrow[d, no head] & \mathbb{Q}_p \\ \mathbb{Q} \arrow[ur] & \end{tikzcd}$$

$\mathfrak{p}$ a prime ideal of $\mathcal{O}_K$ over $(p)$, $K_v = K_{\mathfrak{p}}$ (completion of $K$ at $|\ |_{\mathfrak{p}}$)

Then $K_v \supseteq \mathcal{O}_v = \{x \in K_v : |x|_v \leq 1\} \supseteq \mathfrak{P}_v = \{x \in K_v : |x|_v < 1\}$.

Write $c^{\mathbb{Z}} = \{c^n : n \in \mathbb{Z}\}$ (and choose $\pi \in \mathfrak{P}_v$ with maximal abs. value $c$).

Have the exact sequence:

$$\overset{\mathbb{Z} \leftarrow (\text{projective})}{} $$

$$1 \longrightarrow \mathcal{O}_v^\times \longrightarrow K_v^\times \longrightarrow \overset{\cong}{c^{\mathbb{Z}}} \longrightarrow 1$$

$$x \longmapsto |x|_v$$

This sequence is split, by sending $c^n \mapsto \pi^n$.

Hence $K_v^\times \simeq \mathbb{Z} \times \mathcal{O}_v^\times$.

So fix the element $\pi \in K_v$, and every element $x \in K_v^\times$ can be written uniquely as $x = \pi^r u$, $r \in \mathbb{Z}$, $u \in \mathcal{O}_v^\times$.

(3.1) Lemma: $\mathcal{O}_v = \left\{ \sum_{j=0}^{\infty} a_j \pi^j \text{ where } a_j \in S \right\}$, $S$ a (fixed) set of coset representatives of $\mathcal{O}_v / \mathfrak{P}_v$ and the limit of the partial sums is taken in $\mathcal{O}_v$.

Pf (sketch):

$\alpha \in \mathcal{O}_v$. $\alpha \equiv a_0 \bmod \mathfrak{P}_v$ $(a_0 \in S)$, or $|\alpha - a_0| < 1$

Let $\alpha_1 = \dfrac{\alpha - a_0}{\pi}$. Define $a_1 \in S$ by $\alpha_1 \equiv a_1 \bmod \mathfrak{p}_v$.

//

Hensel's Lemma (easy case):

$f(x) \in \mathcal{O}_v[x]$, and suppose $\exists \alpha_0 \in \mathcal{O}_v$ s.t $f(\alpha_0) \equiv 0 \bmod \mathfrak{p}_v$, $f'(\alpha_0) \not\equiv 0 \bmod \mathfrak{p}_v$

(i.e $\alpha_0$ is a simple root of $f(x)$ mod $\mathfrak{p}_v$) $\uparrow$ $|f'(\alpha_0)|_v = 1$.

Then $\exists! \alpha \in \mathcal{O}_v$, $\alpha \equiv \alpha_0 \bmod \mathfrak{p}_v$, $f(\alpha) = 0$.

Example: Suppose that $\mathcal{O}_v/\mathfrak{p}_v = \mathbb{F}_q$ (residue field is always a finite field).

Then $\mathcal{O}_v$ contains the $(q-1)$st roots of $1$

(in Hensel's lemma, take $f(X) = X^{q-1} - 1$, $\alpha_0 = 1$).

Conclude that $\mu_{q-1} \cup \{0\}$ is a set of coset reps of $\mathcal{O}_v/\mathfrak{p}_v$.

$K_v$ is a topological field (field + topology, + continuous $(+, \cdot)$).

(3.2) Prop: a) $\mathcal{O}_v$, $\mathfrak{p}_v$ are compact. $\leftarrow$ caused by the fact $\mathcal{O}_v/\mathfrak{p}_v$ finite.

b) $\mathcal{O}_v^\times$ is also compact.

Note: $K_v \longrightarrow \mathbb{R}$ is continuous (almost by definition)
$x \longmapsto |x|_v$

Hence, $\mathcal{O}_v$ is a closed subgroup (inverse image of a closed).

Also, $\mathcal{O}_v = \{x \in K_v : |x|_v < \frac{1}{c}\} \Rightarrow \mathcal{O}_v$ is also open.

Have a homeomorphism $\mathcal{O}_v \xrightarrow{\cdot \pi} \mathfrak{p}_v$. So $\mathfrak{p}_v$ is also open and closed.

Pf (of 3.2):

(a) Let $\{V_\alpha\}$ be an open cover of $\mathcal{O}_v$, ($V_\alpha$ open sets in $K_v$).

Let $S$ be a (finite) set of coset reps of $\mathcal{O}_v/\mathfrak{p}_v\mathcal{O}_v$: $\mathcal{O}_v = \bigcup_{a \in S}(a + \pi\mathcal{O}_v)$.

Spse $\nexists$ finite subcover. Then $\exists a_0 \in S$: $a_0 + \pi\mathcal{O}_v$ has no finite subcover.

$a_0 + \pi\mathcal{O}_v = \bigcup_{a \in S}(a_0 + a\pi + \pi^2\mathcal{O}_v)$ and repeat $\downarrow$

we get $\alpha = a_0 + a_1\pi + a_2\pi^2 + \cdots \in \mathcal{O}_v$.

Let $\lambda_0$ s.t $\alpha \in V_{\lambda_0}$. $V_{\lambda_0}$ open $\Rightarrow \exists_j$ s.t $\alpha + \pi^j\mathcal{O}_v \subseteq V_{\lambda_0}$.

But then $\alpha + \pi^j\mathcal{O}_v = a_0 + a_1\pi + \cdots + a_{j-1}\pi^{j-1} + \pi^j\mathcal{O}_v \subseteq V_{\lambda_0}$,

which contradicts $\alpha + \pi^j\mathcal{O}_v$ has no finite subcover. //

As $\mathcal{O}_v \simeq \mathfrak{P}_v$, then $\mathfrak{P}_v$ is also compact.

(b) $\mathcal{O}_v = \mathfrak{P}_v \sqcup \mathcal{O}_v^\times$. Let $\{V_\lambda\}$ be any open cover of $\mathcal{O}_v^\times$. Adding $\mathfrak{P}_v$ (open), covers $\mathcal{O}_v \Rightarrow$ V.

(or note $\mathcal{O}_v^\times = \{x \in K_v^\times : |x_v| = 1\}$ $\leftarrow$ closed subset of $T_2$ is compact).

$\mathcal{O}_v \supseteq \mathfrak{P}_v \supseteq \mathfrak{P}_v^2 \supseteq \cdots$

$\mathcal{O}_v^\times \supseteq 1 + \mathfrak{P}_v \supseteq 1 + \mathfrak{P}_v^2 \supseteq \cdots$

and $$\boxed{\frac{\mathcal{O}_v^\times}{1+\mathfrak{P}_v} \simeq \left(\mathcal{O}_v/\mathfrak{P}_v\right)^\times} \;;\quad \frac{\mathfrak{P}_v^k}{\mathfrak{P}_v^{k+1}} \overset{\text{(add)}}{\phantom{x}} \simeq \frac{(1+\mathfrak{P}_v^k)}{(1+\mathfrak{P}_v^{k+1})} \text{ (mult)}$$

$x \longmapsto 1 + x$ (iso as groups).

<u>Basic fact</u>: $[M:K_v] = n$, then A.V. on $K_v$ extends uniquely to $M$.

$$\begin{tikzcd} M \arrow[d, dash] \\ K_v \arrow[d, dash] \\ \mathbb{Q}_p \end{tikzcd}$$

$\alpha \in M \to \|\alpha\| := |N_{M/K_v}(\alpha)|_v^{\frac{1}{n}}$.

## Main Theorem of Local C.F.T.

Suppose that $L_w/K_v$ is a finite abelian extension of local fields.

$$\begin{tikzcd} L_w \arrow[d, dash] \\ K_v \arrow[d, dash] \\ \mathbb{Q}_v \end{tikzcd}$$

then $K_v^\times / N_{L_w/K_v}(L_w^\times) \xrightarrow[\sim]{\omega} \mathrm{Gal}(L_w/K_v)$

$\uparrow$ reciprocity

and the mapping $L_w \longrightarrow N_{L_w/K_w}(L_w^\times)$ is a inclusion-reversing bijection

between $\{\text{finite abelian extensions of } K_v\} \Leftrightarrow \{\text{open subgps of } K_v^\times \text{ of finite index}\}$

$L_w \mapsto N_{L_w/K_v}(L_w^\times)$

This can be proved using local theory, and $\omega$ can be given explicitly, using the Lubin-Tate formal groups. (Lubin's thesis, 1960's).

It can also be deduced from the global theory (our approach).

(see also 2nd ed. of Lang's book).

Example:

$\mathbb{Q}_p(\sqrt[p]{1}) = L_w \supseteq \mathcal{O}_w$ $\quad$ $\mathrm{Gal}(L_w/\mathbb{Q}_p)$ cyclic of order $p-1$.

$\Big|\, p-1$

$\mathbb{Q}_p$

If $\zeta = \sqrt[p]{1}$, then $N(\overset{\pi}{1-\zeta}) = p$.

Can check that $N(\mathcal{O}_w^\times) = \{x \in \mathbb{Z}_p^\times : x \equiv 1 \bmod p\mathbb{Z}_p\} = 1 + p\mathbb{Z}_p$.

Therefore, as $L_w^\times = \langle \pi \rangle \times \mathcal{O}_w^\times$. So $N(L_w^\times) = \langle p \rangle \times N(\mathcal{O}_w^\times)$ $(\subseteq \langle p \rangle \times \mathbb{Z}_p^\times)$

$N(L_w^\times) = \langle p \rangle \times (1 + p\mathbb{Z}_p)$ $\qquad$ $\mathbb{Z}_p^\times = \mu_{p-1} \times (1 + p\mathbb{Z}_p)$

$$\text{Then, } \mathbb{Q}_p^\times / N(L_w^\times) = \frac{\langle p \rangle \times \mathbb{Z}_p^\times}{\langle p \rangle \times (1 + p\mathbb{Z}_p)} \simeq \frac{\mathbb{Z}_p^\times}{1 + p\mathbb{Z}_p} \simeq \mu_{p-1}$$

(3.3) Prop: Let $L_w/K_v$ be a finite extension, $n = [L_w : K_v]$.

Then $n = e \cdot f$, $f = [\mathcal{O}_w/P_w : \mathcal{O}_v/P_v]$, $P_v\mathcal{O}_w = P_w^e$. (Local rings!)

~~Proof~~ Let $\kappa = \mathcal{O}_v/P_v$. Let $d = \dim_\kappa\left(\mathcal{O}_w/P_v\mathcal{O}_w\right)$. Then:

$$\mathcal{O}_w \supset P_w \supset P_w^2 \supset \cdots P_w^e = P_v\mathcal{O}_w .$$

Then $\forall j$, $\mathcal{O}_w/P_w \simeq P_w^j/P_w^{j+1}$ as $\kappa$-vectorspaces, as if $(\pi_w)$ ~~a p~~ $=P_w$,

dim $f$ $\nearrow$ $\quad x \longmapsto x\cdot\pi_w^j$

$\therefore$ $d = e \cdot f$.

On the other hand, let $\alpha_1, \ldots, \alpha_n \in \mathcal{O}_w$ be a $\mathcal{O}_v$-basis of $\mathcal{O}_w$. (exists because $\mathcal{O}_w$ is a f.gen torsion free module over the PID $\mathcal{O}_v$).

(In the global case, $\mathcal{O}_L$ is not a free $\mathcal{O}_K$-module, just projective).

Write $\overline{\alpha_i}$ for $\alpha_i$ mod $P_v\mathcal{O}_w$. Then check that $\overline{\alpha_1}, \ldots, \overline{\alpha_n}$ are a basis for $\mathcal{O}_w/P_v\mathcal{O}_w$. Hence $n = e \cdot f$ //

Preliminary results on $N_{L_w/K_v}(k_w^\times)$:

(3.4) Lemma: In $K_v$, given $n \geq 1$, $\exists\, t \geq 1$ s.t. $1 + P_v^t \subseteq (\mathcal{O}_v^\times)^n$. $\swarrow$ Stopp.

Hence $(\mathcal{O}_v^\times)^n$ is an open subgroup of finite index in $\mathcal{O}_v^\times$.

(Note: if $x \in \mathcal{O}_v$, $x \equiv 1 \bmod \pi_v^t$ ($t$ suff. large) then $\exists\, y \in \mathcal{O}_v^\times : y^n = x$. $\leftarrow$ this is what lemma says.)

Pf (idea). Apply Hensel's lemma (the general case) to the polynomial

$h(X) = X^n - u$, where $u$ is a (given) elt. $u \equiv 1 \pmod{\pi_v^t}$.

$h' = nX^{n-1}$, $\alpha_0 = 1$. So we need that ~~that X h'~~ $|h(\alpha_0)|_v < |h'(\alpha_0)|_v^2$

i.e. $|1-u| < |n|^2 \Rightarrow$ ~~get~~ get, given $n$, a lower bound for $t$. //

Ex: for $\mathbb{Q}_2$: if $a \equiv 1 \bmod 8\mathbb{Z}_2$, then $a = b^2, b \in \mathbb{Q}_2$.

So we've got $1+\mathfrak{p}_v^t \subseteq (\mathcal{O}_v^\times)^n \subseteq N(\mathcal{O}_w^\times)$

(Note that, if $n = [L_w : K_v]$, then $N_{L_w/K_v}(L_w^\times) \supseteq (K_v^\times)^n$)

Fact: Let $K_v$ be any local field. Then given an integer $f \geq 1$, $\exists$ unique unramified extension $L_w$ of $K_v$ of degree $f$.

Moreover, $L_w/K_v$ is Galois with cyclic Galois group.

(See Cassels-Frohlich).

(Let $q = |\mathcal{O}_v/\mathfrak{p}_v|$. Then $L_w = K_v(\zeta)$, $\zeta$ primitive $(q^f-1)$-root of $1$).

(3.5) Theorem: Let $L_w/K_v$ be the unramified extension of degree $f$. Then:

a) The Norm: $\mathcal{O}_w^\times \longrightarrow \mathcal{O}_v^\times$ is onto.

b) $N(L_w^\times) = \langle \pi \rangle^f \times \mathcal{O}_v^\times$, where $\pi$ is any prime elt. of $\mathcal{O}_v$. (from (a))

Example: $[\mathbb{Q}_p(i) \overset{\text{unramified}}{:} \mathbb{Q}_p] = 2$, $p \equiv 3 \pmod 4$. (p odd).

Then $N(\mathbb{Q}_p(i)^\times) = \langle p^2 \rangle \times \mathbb{Z}_p^\times \overset{\text{index 2}}{\subset} \mathbb{Q}_p^\times$

Pf/ Uses the

(3.6) Lemma: a) Norm: $\mathbb{F}_{q^f}^\times \longrightarrow \mathbb{F}_q^\times$ is onto. (easy to prove). see Hungerford.

b) Trace: $\mathbb{F}_{q^f} \longrightarrow \mathbb{F}_q$ is onto.

Since $L_w/K_v$ is unramified, then we can use $\pi_v$ as a prime elt. of $L_w$.

Given then $u \in \mathcal{O}_v^\times$, we'll find a sequence $x_0, x_1, \dots \in \mathcal{O}_w$ s.t ~~$N(x_0\pi$~~

$$N\left(x_0 \prod_{i=1}^{\infty} (1 + x_i \pi^i)\right) = u.$$

First, by (3.6.a), $\exists\, x_0 \in \mathcal{O}_w^\times$ s.t $N(x_0) \equiv u \bmod \mathfrak{p}_v$. (as $\mathbb{F}_q = \mathcal{O}_v/\mathfrak{p}_v$, $\mathbb{F}_{q^f} = \mathcal{O}_w/\mathfrak{p}_w$).

(cont'd pf)

So $\frac{u}{N(x_0)} \equiv 1 + c_1\pi \pmod{\mathfrak{p}_v^2}$, $c_1 \in \mathcal{O}_v$. let $G = Gal(L_w/K_v)$ $\pi \in K_v$

Note that for $x \in \mathcal{O}_w$, $\boxed{N(1+x\pi^t) = \prod_{\sigma\in G}(1+x\pi^t)^\sigma = \prod_{\sigma\in G}(1+x^\sigma\pi^t) \equiv}$

$\boxed{\equiv 1 + \pi^t \,\text{Trace}(x) \pmod{\mathfrak{p}_v^{t+1}}}$

By (3.6.b), $\exists\, x_1 \in \mathcal{O}_w$ s.t. $\text{Trace}(x_1) \equiv c_1 \mod \mathfrak{p}_v$.

So $\frac{u}{N(x_0)N(1+x_1\pi)} \equiv 1 + c_2\pi^2 \pmod{\mathfrak{p}_v^3}$. Repeat (induction). //

(3.7) Theorem: $L_w/K_v$ unramified of degree $f$.

Let $\theta : K_v^\times \longrightarrow Gal(L_w/K_v)$.

$x = \pi^{v(x)}\underset{\overset{\cap}{\mathcal{O}_v^\times}}{u} \mapsto \sigma^{v(x)}$, where $\sigma$ = Frobenius of $L_w/K_v$ = lift from the Frob coming from the residue fields

Then $\theta$ is onto, with kernel $N(L_w^\times)$.

Proof

Claim: $\ker\theta = N(L_w^\times)$.

Pf Earlier, we showed $N(L_w^\times) = \mathcal{O}_v^\times \times \langle \pi^f \rangle$ ($\pi$ any prime of $K_v$). //

(3.8) Theorem: $L/K$ finite degree extension of number fields.

Suppose $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1}\cdots\mathfrak{P}_g^{e_g}$, $f_i := [\mathcal{O}_L/\mathfrak{P}_i : \mathcal{O}_K/\mathfrak{p}]$, and consider the completions $K_\mathfrak{p}$, $L_{\mathfrak{P}_i}/K_\mathfrak{p}$. Then

(i) $L_{\mathfrak{P}_i}$ is an extension of $K_\mathfrak{p}$ of degree $e_if_i$

(ii) $e_i$ is the ramification index of $L_{\mathfrak{P}_i}/K_\mathfrak{p}$

$f_i$ is the degree of the residue field extension for $L_{\mathfrak{P}_i}/K_\mathfrak{p}$.

(iii) $K_\mathfrak{p}\otimes_K L \simeq \prod_i L_{\mathfrak{P}_i}$ iso as $K_\mathfrak{p}$-algebras. (So $[L:K] = \sum^g [L_{\mathfrak{P}_i}:K_\mathfrak{p}]$)

Pf See Serre, "Corps Locaux", Chap II, §3, pg 40. //

Rk: if $L = K(\alpha)$, and $h(x) = \text{minpol}_K(\alpha)$, write

$$h(x) = \prod_{i=1}^{g} h_i(x), \quad h_i \in K_{\mathfrak{p}}[x] \text{ irreducible.}$$

Then
$$A = K_{\mathfrak{p}} \otimes_K L = K_{\mathfrak{p}} \otimes_K \frac{K[X]}{(h)} \cong \frac{K_{\mathfrak{p}}[X]}{(h)} \overset{\overset{\text{CRT}}{\downarrow}}{\cong} \prod_{i=1}^{g} \frac{K_{\mathfrak{p}}[X]}{(h_i)} \simeq \prod_{i=1}^{g} L_{\mathfrak{P}_i}$$

(3.9) Prop: (Linear algebra)

a) For each $\alpha \in L$, the char. polynomial of $\alpha$ acting on the $K$-space $L$ is $\prod_{i=1}^{g}$ (char poly of $\alpha$ acting on $L_{\mathfrak{P}_i}$ as a $K_{\mathfrak{p}}$-space).

b) Hence
- $N_{L/K}(\alpha) = \prod_{i=1}^{g} N_{L_{\mathfrak{P}_i}/K_{\mathfrak{p}}}(\alpha)$
- $Tr_{L/K}(\alpha) = \sum_{i=1}^{g} Tr_{L_{\mathfrak{P}_i}/K_{\mathfrak{p}}}(\alpha)$.

Pf/ Ex //

(3.10) Prop: if $L/K$ is Galois, $G = Gal(L/K)$, then if $\mathfrak{P}$ is a prime of $\mathcal{O}_L$, $\mathfrak{p} = \mathfrak{P} \cap K$, Then:

$$L_{\mathfrak{P}}/K_{\mathfrak{p}} \text{ is Galois and } Gal(L_{\mathfrak{P}}/K_{\mathfrak{p}}) \simeq D_{\mathfrak{P}} \left( = \{\sigma \in G : \sigma(\mathfrak{P}) = \mathfrak{P}\} \right)$$

decomp group, order e.f

Pf/ Let $j_{\mathfrak{P}} : D_{\mathfrak{P}} \longrightarrow Gal(L_{\mathfrak{P}}/K_{\mathfrak{p}})$ ← aut. gp, even if the ext is not normal!

be defined by continuity, i.e. if $\sigma \in D_{\mathfrak{P}}$, and $L_{\mathfrak{P}} = \dfrac{\text{Cauchy sequences corresp to } \mathfrak{P}}{\{a_n \to 0\}}$

Then $[\{b_n\}] \in L_{\mathfrak{P}} \Rightarrow j\sigma([\{b_n\}]) := [\{c_n\}]$ where $c_n = \sigma(b_n)$.

If $\sigma \in D_{\mathfrak{P}}$, then $\{c_n\}$ is Cauchy for $\mathfrak{P}$ and map is well-defined.

As $\sigma$ fixes $K$, $j_{\mathfrak{P}}(\sigma) \in Gal(L_{\mathfrak{P}}/K_{\mathfrak{p}})$

- $j_{\mathfrak{P}}$ injective: if $j_{\mathfrak{P}}(\sigma) = 1$, then $\sigma\{b_n\} = \{b_n\}$, $b_n := \alpha \in L \ \forall n. \Rightarrow \sigma$ fixes $\alpha \ \forall\alpha$ $\Rightarrow \sigma = 1$.
- $|D_{\mathfrak{P}}| = ef$, and $[L_{\mathfrak{P}} : K_{\mathfrak{p}}] = ef \geq Gal(L_{\mathfrak{P}}/K_{\mathfrak{p}}) \Rightarrow$ Galois ext + iso! //

# Chapter IV: Ideles (and Adeles).

Idea:

$$\begin{tikzcd} & L_\beta = L_w \arrow[dl, dash] \arrow[dd, dash] \\ L \arrow[dd, dash] & \\ & K_\beta = K_v \arrow[dl, dash] \\ K & \end{tikzcd}$$

We've just seen that that $e$'s and $f$'s can be seen in the local extension.

But the Unit thm + Class number is not seen there (PID's).

What we'll do is consider all primes $v$ of $K$ at once, where $v$ is either finite/infinite.

First try: Define $M_K = \{v$ primes of $K\}$

and $\prod_v K_v^\times$. Each $K_v^\times$ is locally compact, but the product is not.
← too big.

Def: $J_K = \{ (a_v) : a_v \in K_v^\times$, and $a_v \in \mathcal{O}_v^\times$ for all but finitely-many $v \}$.
local units
a.a.v (almost all $v$)

(often one defines $\mathcal{O}_v^\times := K_v^\times$ if $v$ is infinite).

Have a map $i : K^\times \hookrightarrow J_K$ by $i(\alpha) = (a_v)$, $a_v = \alpha \ \forall v \in M_K$.

(e.g. $K = \mathbb{Q}$, $\alpha = -\frac{3 \cdot 5 \cdot 2^2}{11} \in \mathbb{Q}^\times$. Then $\alpha \in \mathbb{Z}_p^\times$ for $p \neq 2, 3, 5, 11$).

Def $i(K^\times)$ is called the principal ideles.

Def $J_K / K^\times = C_K$, group of idele classes.

Let $U_K$ be the sgp of $J_K$ defined by $U_K := \prod_{v \in S_\infty} K_v^\times \times \prod_{v \notin S_\infty} \mathcal{O}_v^\times$

(where $S_\infty = \{$infinite primes of $K\}$).

Let $\varphi : J_K \longrightarrow I_K$ = ideal ~~gp~~ of $K$

$(a_v)_v \longmapsto \prod_{v \text{ finite}} \mathfrak{p}_v^{v(a_v)}$ where $\mathfrak{p}_v$ prime of $\mathcal{O}_K$ corresponding to $v$.

Rk: $\varphi : J_K \twoheadrightarrow I_K$ is onto, and $\ker \varphi = U_K$.

So $J_K / U_K \simeq I_K$.

eg: $K = \mathbb{Q}$, $(t, a_2, a_3, a_5, a_7, \dots)$ $t \in \mathbb{R}$, $a_p \in \mathbb{Q}_p$.

$$\varphi(1.1, 4, 6, 6, 1, 1, 1, \dots) = (2^2)\cdot(3)\cdot(5)^0\cdot(7)^0 \cdots = (12).$$

(4.1) Prop: $J_{\mathbb{Q}} \cong i(\mathbb{Q}^\times) \times \mathbb{R}^\times_{>0} \times \prod_{p \text{ primes}} \mathbb{Z}_p^\times$ (as multiplicative gps, and $i : K^\times \hookrightarrow J_K$ diag. embedding)

Pf Map $J_{\mathbb{Q}} \underset{i}{\overset{f}{\rightleftarrows}} \mathbb{Q}^\times$ by idele $a = (t, a_2, a_3, a_5, \dots)$ where $t \in \mathbb{R}$, $a_p \in \mathbb{Q}_p^\times$, $a_p \in \mathbb{Z}_p^\times$ for a.a.p.

Define $f(a) := \text{sign}(t) \cdot \prod_p p^{v_p(a_p)}$

(finite product since $v_p(a_p) = 0$ a.a.p.).

$f$ is a gp hom, and onto, clearly. (in $J_K$, mult is componentwise).

We have $i : \mathbb{Q}^\times \hookrightarrow J_{\mathbb{Q}}$, and $f\left(i\left(\frac{a}{b}\right)\right) = \frac{a}{b}$, so it's a splitting.

Check: $\ker f = \mathbb{R}^\times_{>0} \times \prod_p \mathbb{Z}_p^\times$, so done. //

We often omit the $i(K^\times)$. Then $J_{\mathbb{Q}} / \mathbb{Q}^\times \overset{\text{product topology}}{=} \mathbb{R}^\times_{>0} \times \prod_p \mathbb{Z}_p^\times$ (idele class gp).

Note: $\mathbb{R}^\times_{>0}$ is the connected component of $J_{\mathbb{Q}}/\mathbb{Q}^\times$ (the conn. comp containing $1$).

Note: $\prod_p \mathbb{Z}_p^\times = \text{Gal}(\mathbb{Q}^{ab}/\mathbb{Q})$, $\mathbb{Q}^{ab}$ = max abelian ext. of $\mathbb{Q}$.

$$\left(\mathbb{Q}^{ab} = \bigcup_{m \geq 1} \mathbb{Q}(\sqrt[m]{1}) \Rightarrow \text{Gal}(\mathbb{Q}^{ab}/\mathbb{Q}) = \varprojlim (\mathbb{Z}/m\mathbb{Z})^\times \overset{CRT}{=} \prod_p \mathbb{Z}_p^\times.\right.$$

## • Topology on ideles

Ref: [E. Weiss] "Alg. Num. Theory": careful statement of $^{\text{background for}}$ topological groups..

G a group, and a top. space s.t $G \times G \to G$, $(g,h) \mapsto gh$ and $G \to G$, $g \mapsto g^{-1}$ are continuous. We say then that $G$ is a topological group.

Examples: $\mathbb{R}^+$, $\mathbb{R}^\times$, $Gl_n(\mathbb{R})$, or: $K_v$, $K_v^\times$, $Gl_n(K_v)$, ...

Fix $a \in G$. Then $\begin{array}{c} G \to G \\ g \mapsto a\cdot g \end{array}$ is a homeomorphism.

So we can reduce to looking at nbhds of 1.

Restricted direct product (aka direct sum)

$\{v\}$ an index set.

$G_v$ locally compact topological groups (or rings),

Then $G_v \supset H_v$ : $H_v$ defined for almost all $v$, $H_v$ compact open sbgp of $G_v$.

Then define the restricted direct product as

$$\prod_v (G_v, H_v) := \{(g_v)_v : g_v \in G_v,\ g_v \in H_v \text{ for a.a. } v\}.$$

Rk: ideles: take $G_v = K_v^\times$, $H_v = \mathcal{O}_v^\times$. → write $J_K$

adeles: take $G_v = k_v$, $H_v = \mathcal{O}_v$ (rings). → write $\mathbb{A}_K$

Topology on rst. direct product:

Recall if $\{X_v\}$ top. spaces, $X = \prod X_v$, then the product topology is given by a basis of open sets $\prod_v Y_v$, $Y_v$ open in $X_v$ and $Y_v = X_v$ a.a.v.

Have that the product of compact spaces is compact.

On $G = \prod_v (G_v, H_v)$. Let $S_\infty = \{v : H_v \text{ not defined}\}$.

Let $S \supseteq S_\infty$ be a finite set of $v$'s.

Define now $G_S = \underbrace{\prod_{\substack{v\in S \\ \wedge \text{ bnd } v\text{'s}}} G_v}_{\text{loc-compact}} \times \underbrace{\prod_{v\notin S} H_v}_{\text{compact}}$ $\Rightarrow$ $G_S$ is locally compact ~~w~~with the product topology.

Now decree that $G_S$ is an open of $G$ $\forall S$. (note $G = \bigcup_S G_S$).

<u>Ex</u>: $J_S = \prod_{v\in S} k_v^\times \times \prod_{v\notin S} \mathcal{O}_v^\times$, $J_{S_\infty} = \prod_{v\in S_\infty} k_v^\times \times \prod_{v\notin S_\infty} \mathcal{O}_v^\times$.

For $k=\mathbb{Q}$, $J_{S_\infty} = \mathbb{R}^\times \times \prod_p \mathbb{Z}_p^\times$, $J_{\mathbb{Q}} = \mathbb{Q} \underset{\substack{\uparrow \\ \text{not a direct product.}}}{\cdot} J_{S_\infty}$

In fact, $J_{S_\infty} \cap K^\times = (\mathcal{O}_K)^\times$. ($\alpha \in K^\times$ belongs to $J_{S_\infty} \Leftrightarrow \alpha$ p-adic unit $\forall$ prime ideals $\mathfrak{p}$)
$\Leftrightarrow \alpha$ is a unit.

Let $I_K$ = gp of fractional ideals of $K$ (free ab. on the prime ideals).

<u>(4.2) Prop</u>: $\exists$ hom $\theta : J_K \twoheadrightarrow I_K$, onto with kernel $J_{S_\infty}$.

sending $(a_v) \longmapsto \prod_{\mathfrak{P}_v} \mathfrak{p}_v^{v(a_v)}$ (where $\mathfrak{P}_v$ is a prime ideal of $\mathcal{O}_K$).

Pf Clear

Furthermore, Let $P_K$ = gp of principal ideals of $K$.

Then $\theta(K^\times) = P_K$, thus: $\boxed{J_K \big/ K^\times J_{S_\infty} \simeq I_K \big/ P_K}$ ← ideal class gp

<u>Rk</u>: on HW, $\exists S \supset S_\infty$ s.t. $J_K = k^\times J_S$ !

<u>(4.3) Prop</u>: $K^\times$ is a discrete subgroup of $J_K$, hence closed! (contrast: $K^\times$ dense in $\prod_{v\in T} K_v^\times$)
$T$ finite set of primes.

Pf $J_{S_\infty} = \prod_{v\in S_\infty} K_v^\times \times \prod_{v\notin S_\infty} \mathcal{O}_v^\times$. We'll find a nbhd ~~th~~ $U$ of $1$ in $J_{S_\infty}$ s.t. $U \cap K^\times = \{1\}$.

Define $U := \left\{ (a_v) : \begin{cases} |a_v - 1| < \varepsilon & \text{if } v\in S_\infty \\ |a_v| = 1 & \text{if } v \notin S_\infty \end{cases} \right\}$ $(0<\varepsilon<1)$

Suppose $\overset{\neq 1}{\alpha} \in U \cap K^\times$, Apply the product formula to $\alpha - 1$: $1 = \prod_v |\alpha - 1|_v$ ← suitably normalized.

↓

(cont pf):

So $1 = \overbrace{\prod_{v\in S_\infty}|\alpha-1|_v}^{<1} \times \overbrace{\prod_{v\notin S_\infty}|\alpha-1|_v}^{\leq 1} \Rightarrow$ contradiction. //

Thus, can form the topological group $J_K/K^\times$ with closed points (as $K^\times$ is closed).

Note: $J_{\mathbb{Q}}/\mathbb{Q}^\times \simeq \mathbb{R}^\times_{>0} \times \prod_p \mathbb{Z}_p^\times$ is not compact, because of $\mathbb{R}^\times_{>0}$.

Define $\|\cdot\|$ on $J_K$ by $\|(a_v)\| := \prod_v |a_v|_v^{n_v}$, suitably normalized, and

such that $n_v = \begin{cases} (K_v : \mathbb{Q}_p) & \text{if } p \text{ finite} \\ 1 & \text{if } K_v = \mathbb{R} \\ 2 & \text{if } K_v = \mathbb{C} \end{cases}$ ($|\cdot|_v$ extends that of $\mathbb{Q}_p$ to $K_v$ with $|p|_p = \frac{1}{p}$)

Then $\|\cdot\|$ is ~~an absolute value on~~ is a norm, onto: $J_K \longrightarrow \mathbb{R}^\times_{>0}$, $a \longmapsto \|a\|$, (continuous)

and $J_K^0 := \{a \in J_K : \|a\| = 1\}$ (Lang calls it $J^0$, others call it $J^1$).

We want to find an splitting of this map, $j : \mathbb{R}^\times_{>0} \longrightarrow J_K$, $t \longmapsto (t_v)$, (continuous)

where we set $t_v = \begin{cases} t^{\frac{1}{n}} & \text{if } v \in S_\infty \\ 1 & \text{otherwise} \end{cases}$. Verify that $\|j(t)\| = t$, using

that $\sum_{v\in S_\infty} n_v = (K : \mathbb{Q})$.

Thus we can write $J_K \simeq \mathbb{R}^\times_{>0} \times J^0$. Note $K^\times \subseteq J^0$ by the product formula.

(4.7) Theorem: $J^0/K^\times$ is compact.

Remark: this theorem is equivalent to:

(1) Finiteness of the class number

+

(2) Unit theorem.

Pf: we will thus assume finite class # + unit thm..

Recall $\theta : J_K \to I_K$ (ideal gp). is onto with kernel $J_{S_\infty} = \prod_{v\in S_\infty} K_v^\times \times \prod_{v\notin S_\infty} \mathcal{O}_v^\times$

$$(a_v) \mapsto \prod_{v\notin S_\infty} \mathfrak{p}_v^{v(a_v)}$$

Consider now $\theta_1 : J_K^0 \twoheadrightarrow I_K$ (ie. $a\in J_K$, then $\exists\, a' \in J^0$ s.t. $\theta(a)=\theta(a')$).

check this

Call $J^0_{S_\infty} := \ker\theta_1 = J_K^0 \cap J_{S_\infty}$.

So have exact $1 \to J^0_{S_\infty} \to J_K^0 \to I_K \to 1$.

Modding-out by $K^*$, get
$$1 \to \frac{J^0_{S_\infty}K^\times}{K^\times} \to \frac{J^0}{K^\times} \xrightarrow{\theta} \underbrace{\frac{I_K}{P_K}}_{\text{finite gp.}} \to 1$$

Rk: given an exact seq: $1 \to A \to B \to C \to 1$, then $B$ cpt $\Leftrightarrow$ $A$ cpt & $C$ cpt.

So as $I_K/P_K$ is finite, we just need to prove that $\frac{J^0_{S_\infty}K^\times}{K^\times}$ is compact.

By isomorphism thms, which also hold for topological gps,
$$\frac{J^0_{S_\infty}K^\times}{K^\times} \simeq \frac{J^0_{S_\infty}}{K^\times \cap J^0_{S_\infty}} = \frac{J^0_{S_\infty}}{E_K} \quad \text{as} \quad E_K = \text{unit gp} = \mathcal{O}_K^\times.$$

Recall pf. of the unit thm: the Log map sends $\prod_{v\in S_\infty} K_v^\times \longrightarrow \mathbb{R}^{r_1+r_2}$
$$(a_v) \longmapsto (\dots, n_v \log|a_v|_v, \dots)$$

When we restrict to elements of norm 1 (ie $\prod |a_v|^{n_v} = 1$), get:

$$\text{Log} : \Big(\prod_\infty K_v^\times\Big)^0 \twoheadrightarrow H, \text{ and } \operatorname{im}\text{Log} = H = \{(z_v) \in \mathbb{R}^{r_1+r_2} : \sum_{v\in S_\infty} z_v = 0\}.$$

Factoring-out by $E_K$, and noting the exactness of $1 \to \mu_K \to E \to \log E \to 1$, get:

~~$\Big(\prod_\infty K_v^\times\Big)^0 / E_K \longrightarrow$~~
$$1 \to \underbrace{(\pm 1)^{r_1} \times (S^1)^{r_2}}_{(\mu_K)} \to \frac{\big(\prod K_v^\times\big)^0}{E_K} \to \frac{H}{\log E_K} \to 1$$

By the unittheorem, $\log E$ is a lattice of full rank $(r_1+r_2-1)$ in $H$. (equiv. to saying that $H/\log E$ is compact). Thus $\big(\prod_\infty K_v^\times\big)^0/E_K$ is compact. Extend log to $J_{S_\infty}$ by saying $a_v \to 0$ if $v \notin S_\infty$.

Let now $b=(b_w) \in J_L$. Define $a = N_{L/K}(b)$, $a=(a_v)\in J_K$ by:

$$a_v := \prod_{w|v} N_{L_w/K_v}(b_w) \qquad (\text{check that } a \in J_K)$$

Then Norm : $J_L \to J_K$ is a gp homomorphism (check).

One defines the Trace : $\mathbb{A}_L \to \mathbb{A}_K$ in a similar way.

With this definition, ideal (recall $id((a_v)) = \prod_{v \text{ finite prime}} \mathfrak{p}_v^{v(a_v)}$).

$$\begin{tikzcd}
L^\times \arrow[r, hook] \arrow[d, "N"'] & J_L \arrow[r, "id"] \arrow[d, "\text{Norm}"] \arrow[dl, phantom, "\circlearrowleft\ (\text{by } 3.10)"] & I_L \arrow[d, "N"] \arrow[dl, phantom, "\circlearrowleft"] \\
K^\times \arrow[r, hook] & J_K \arrow[r, "id"] & I_K
\end{tikzcd}$$

idele class gps

$$C_L \qquad C_K$$

This induces then a norm in the quotient: $N : J_L/L^\times \longrightarrow J_K/K^\times$

Later we'll see that if $L/K$ is abelian, $[L:K] < \infty$, then $\mathrm{Gal}(L/K) \underset{\substack{\uparrow \\ \text{reciprocity}}}{\cong} \dfrac{C_K}{N_{L/K}(C_L)}$.

Recall now the ray class gp for $K$, given a modulus $\mathfrak{m}$. ($\mathfrak{m}=1 \Rightarrow$ ideal class gp).

$I(\mathfrak{m})/P_\mathfrak{m}$ (finite group).

$I(\mathfrak{m})$ = frac. ideals rel. prime to $\mathfrak{m}_0$.
$P_\mathfrak{m} = \{(\alpha), \alpha \in K^\times : \alpha \equiv 1 \bmod^* \mathfrak{m}\}$.

We want to find quotients of the idele group.

If $\alpha \in K^\times$, $\alpha \equiv 1 \bmod^* \mathfrak{m}$ means
$$\begin{cases} i_v(\alpha) > 0 & \text{if } i_v : K \to K_v = \mathbb{R},\ v \mid \mathfrak{m}_\infty \\ v_\mathfrak{p}(\alpha - 1) \geq v_\mathfrak{p}(\mathfrak{m}_0) & \text{if } \mathfrak{p} \mid \mathfrak{m}_0 . \end{cases}$$

Then if $K_\mathfrak{m} = \{\alpha \in K^\times : \alpha \equiv 1 \bmod^* \mathfrak{m}\}$, $K_\mathfrak{m} \twoheadrightarrow P_\mathfrak{m}$, we can define also:

$J_\mathfrak{m} \ni (a) \Leftrightarrow a_v > 0$ if $v \mid \mathfrak{m}_\infty$ and $v_\mathfrak{p}(a_v - 1) \geq v_\mathfrak{p}(\mathfrak{m}_0)$ if $\mathfrak{p} \mid \mathfrak{m}_0$.

<u>Note</u>: $K_\mathfrak{m} = J_\mathfrak{m} \cap K^\times$.

cont'd pf

We finally get a map, $\tilde{\theta} : J_{S_\infty} \to H$.

$$\begin{tikzcd}
1 \arrow[r] & (\pm 1)^{r_1} \times (S^1)^{r_2} \times \prod_{v \notin S_\infty} \mathcal{O}_v^\times \arrow[r] & J_\infty^0 \arrow[r] & H \arrow[r] & 0 \\
1 \arrow[r] & \mu_n \arrow[r] \arrow[u, "f"] & E \arrow[r] \arrow[u, "g"] & \log E \arrow[r] \arrow[u, "h"] & 0
\end{tikzcd}$$

By the snake lemma, $0 \to \text{coker } f \to \overset{J_\infty^0/E}{\overset{\parallel}{\text{coker } g}} \to \text{coker } h \to 0$. Thus get the result as $\left((\pm 1)^{r_1} \times (S^1)^{r_2} \times \prod_{v \notin S_\infty} \mathcal{O}_v^\times\right) / \mu_n$ and $H / \log E$ are compact.

Weak approximation

$K$ a number field, $S$ a finite set of primes (finite or infinite).

Given $a_v \in K_v$ for $v \in S$, and $\varepsilon > 0$, then $\exists\, \alpha \in K$ s.t. $|\alpha - a_v|_v < \varepsilon \;\; \forall v \in S$.

Pf. See Lang pg 35-36.

Define Norm: $J_L \to J_K$, where $L/K$ is a finite extension.

(3.10): $N_{L/K}(\alpha) = \prod_{w|v} N_{L_w/K_v}(\alpha)$) $\forall \alpha \in L$. (using $K_v \otimes_K L \simeq \prod_{w|v} L_w$).

Example: $L = \mathbb{Q}(i)$, $K = \mathbb{Q}$. $L \simeq \mathbb{Q}[x]/(x^2+1)$.

Take $p \equiv 1 \ (4)$. So $p$ splits in $L$. By Hensel's lemma, $\exists\, j \in \mathbb{Q}_p : j^2 = -1$.

$$\mathbb{Q}_p \otimes_{\mathbb{Q}} \frac{\mathbb{Q}[x]}{(x^2+1)} \simeq \frac{\mathbb{Q}_p[x]}{(x^2+1)} \underset{\underset{CRT}{\uparrow}}{=} \frac{\mathbb{Q}_p[x]}{(x-j)} \oplus \frac{\mathbb{Q}_p[x]}{(x+j)} = L_{w_1} \oplus L_{w_2}$$

Let now $a + bx \mod (x^2+1) \in \frac{\mathbb{Q}[x]}{(x^2+1)}$. We get $T = \begin{cases} a+bx \pmod{x-j}, \\ a+bx \pmod{x+j} \end{cases}$

So $T = (a+bj, a-bj) \in L_{w_1} \oplus L_{w_2}$.

The product of local norms is $(a+bj)(a-bj) = a^2 + b^2$

The global norm of $a + bx \mod (x^2+1)$ is $a^2+b^2$, in accordance with (3.10).

(4.8) $\boxed{a}$ <u>Moving lemma</u>: $\mathfrak{m}$ modulus of $K$, then $J_\mathfrak{m}/K_\mathfrak{m} \cong J/K^\times$.  $(J=J_K)$.

Pf $J_\mathfrak{m} \hookrightarrow J \longrightarrow J/K^\times$. Ker $= J_\mathfrak{m} \cap K^\times = K_\mathfrak{m}$ so it's injective.

Need to show that it's surjective.

Let $a=(a_v)$ be an idele. Suffices to prove that $\exists\, \alpha \in K^\times$ s.t. $\frac{\alpha}{a} \equiv 1 \bmod^* \mathfrak{m}$ in $J$.

(this proves that $\frac{1}{a} \in$ image).

By weak approximation, $\exists\, \alpha \in K^\times$ s.t $|\alpha - a_v|_v < \varepsilon$ for all $v \in S =$ "primes" dividing $\mathfrak{m}$.

(choose $\varepsilon$ later).

$\frac{\alpha}{a_v} = 1 + \frac{\alpha - a_v}{a_v}$ can be made arbitrarily close to $1$ in $K_v$.

So $\exists\, \alpha \in K^\times$ : $\frac{\alpha}{a} \in J_\mathfrak{m}$. //

$\boxed{b}$ $J_K = K^\times J_\mathfrak{m}$

pf direct from (a) /

"<u>More subgroups of $J_K$</u>"

Recall that $1 + \hat{\mathfrak{p}}_v^j$ $j \geq 1$ is a system of nbhds of $1$ in $K_v^\times$ $(\hat{\mathfrak{p}}_v = \mathfrak{p}_v \mathcal{O}_v)$.

Write $\mathfrak{m} = \prod_{v | \mathfrak{m}_0} \mathfrak{p}_v^{m(v)} \cdot \mathfrak{m}_\infty$.

Define
$$W_\mathfrak{m}(v) := \begin{cases} \mathbb{R}_{>0}^\times & \text{if } v | \mathfrak{m}_\infty \\ 1 + \hat{\mathfrak{p}}_v^{m(v)} & \text{if } v | \mathfrak{m}_0 \\ \mathcal{O}_v^\times & \text{if } v \nmid \mathfrak{m} \quad (\text{recall } \mathcal{O}_v^\times := K_v^\times \text{ if } v \text{ infinite}). \end{cases}$$

Define now $W_\mathfrak{m} := \prod_v W_\mathfrak{m}(v)$, which is an open set inside $J_\mathfrak{m}$.

$W_\mathfrak{m} = \{(a_v) : v | \mathfrak{m} \Rightarrow a_v$ satisfies a congruence condition, and $v \nmid \mathfrak{m}$ $a_v$ is a local unit$\}$.

(4.8) (b) $J_{\mathfrak{m}} / K_{\mathfrak{m}} W_{\mathfrak{m}} \cong I(\mathfrak{m}) / P_{\mathfrak{m}}$

Proof $J_{\mathfrak{m}} \xrightarrow{id} I(\mathfrak{m})$ with kernel $W_{\mathfrak{m}}$, so

$$\begin{array}{ccc} \dfrac{J_{\mathfrak{m}}}{W_{\mathfrak{m}}} & \simeq & I(\mathfrak{m}). \\ \cup\!\!\mid & & \cup\!\!\mid \\ \dfrac{K_{\mathfrak{m}} W_{\mathfrak{m}}}{W_{\mathfrak{m}}} & \simeq & P_{\mathfrak{m}} \end{array} \quad + \text{3rd iso thm}$$

We want to get, on the RHS, $\dfrac{I(\mathfrak{m})}{P_{\mathfrak{m}}\mathfrak{N}(\mathfrak{m})}$ - we need to figure out what to do in the LHS.

From Chap III, recall (4.9) Prop: $L_w/K_v$ ext. of local fields, then $N_{L_w/K_v}(L_w^\times) = \begin{cases} \mathbb{R}_{>0}^\times & L_w=\mathbb{C}, K_v=\mathbb{R} \\ \supseteq 1+\hat{\mathfrak{p}}_v^k \text{ some } k\geq 1 & \text{if non-~~arch~~} \\ \supseteq \mathcal{O}_v^\times & \text{if } L_w/K_v \text{ is \underline{unramified}.} \end{cases}$

<u>Corollary</u>: if $L/K$ is a finite ext. of number fields.

Then $\exists\, \mathfrak{m}$ modulus of $K$ s.t. $N_{L/K}(J_L) \supseteq W_{\mathfrak{m}}$

~~Pf~~ We want first $\mathfrak{m}$ to contain the ramified primes. //

Def The modulus $\mathfrak{m}$ is <u>admissible</u> for $L/K$ Galois if $N_{L/K}(J_L) \supseteq W_{\mathfrak{m}}$.

<u>(4.10) Theorem</u>: Let $L/K$ Galois, $\mathfrak{m}$ admissible. Then $J_K / K^\times N_{L/K}(J_L) \cong \dfrac{I(\mathfrak{m})}{P_{\mathfrak{m}}\mathfrak{N}(\mathfrak{m})}$

(where $\mathfrak{N}(\mathfrak{m}) = N_{L/K}(I_L(\mathfrak{m}))$).

<u>Remark</u>: We say a modulus $\mathfrak{m}'$ is <u>smaller</u> than $\mathfrak{m}$ if $\mathfrak{m}' \mid \mathfrak{m}$.

Then given $L/K$, $\exists$ <u>smallest</u> admissible modulus $\mathfrak{f}$ (called <u>conductor</u>).

<u>Pf of 4.10</u>: First, define $J_{L,\mathfrak{m}} := \{ b \in J_L : b \equiv 1 \bmod^* \hat{\mathfrak{m}} \}$, where

$\hat{\mathfrak{m}} = (\mathfrak{m}_0 \mathcal{O}_L) \cdot \hat{\mathfrak{m}}_\infty$, where a ~~real~~ prime $w$ of $L$ divides $\hat{\mathfrak{m}}_\infty$ iff $w \mid$ real $v$ of $\mathfrak{m}_\infty$.

Can show that $N(J_{L,\mathfrak{m}}) \subset J_{\mathfrak{m}}$.

(cont pf):

2 steps:

$$\begin{array}{ccc} J_m/W_m & \cong & I(m) \\ \rotatebox{90}{$\subseteq$} & & \rotatebox{90}{$\subseteq$} \\ \dfrac{K_m W_m N(J_{L,m})}{W_m} & \cong & P_m N(m) \\ \rotatebox{90}{$\subseteq$} & & \rotatebox{90}{$\subseteq$} \\ \dfrac{K_m W_m}{W_m} & \cong & P_m \end{array}$$

used

$$\begin{tikzcd} J_L \arrow[r, "id"] \arrow[d, "Nm"'] \arrow[dr, phantom, "\circlearrowright"] & I_L \arrow[d, "Nm"] \\ J_K \arrow[r, "id"] & I_K \end{tikzcd}$$

So get by 3rd isom, $\dfrac{J_m}{K_m W_m N(J_{L,m})} \cong \dfrac{I(m)}{P_m N(m)}$

Second step: Show that $\dfrac{J_m}{K_m W_m N(J_{L,m})} \cong \dfrac{J_K}{K^\times N_{L/K}(J_L)}$ if m admissible.

$$\frac{J_m}{K_m} \cong J/K^\times \quad (4.8(a)) \implies \frac{J_m}{K_m W_m} \simeq \frac{J}{K^\times W_m}$$

$$\begin{array}{ccc} \dfrac{J_m}{K_m W_m} & & \dfrac{J}{K^\times W_m} \\ \rotatebox{90}{$\subseteq$} & & \rotatebox{90}{$\subseteq$} \\ \dfrac{K_m W_m N(J_{L,m})}{K_m W_m} & \underset{\uparrow (*)}{\cong} ~~\dfrac{J}{K^\times W_m N(J_L)}~~ & \underset{\substack{\uparrow \\ \text{if } W_m \subseteq N(J_L)}}{\dfrac{K^\times N(J_L)}{K^\times W_m}} \end{array}$$

(*) uses that $J_{L,m} \cdot L^\times = J_L$ (cor. to 4.8(a) applied to $L$).

So $N(J_L) = N(J_{L,m}) \cdot N(L^\times) \subseteq N(J_{L,m}) \cdot K^\times$.

Thus $N(J_{L,m}) \twoheadrightarrow \dfrac{K^\times N(J_L)}{K^\times W_m}$.

Finally, just apply 3rd iso thm ~~t~~ get the theorem.

we will later prove $$\frac{I(m)}{P_m N(m)} \cong \underbrace{Gal(L/K) \cong \frac{J_K}{K^\times N J_L}}_{\sim}$$ ^ just proven!

What's the map $J_K \twoheadrightarrow Gal(L/K)$ ?

Example: $K = \mathbb{Q}$, $L = \mathbb{Q}(\zeta_p)$, $p$ prime. $Gal(L/\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^\times$.

$m = (p)\cdot\infty$ is admissible.

$$\begin{tikzcd} J_m \subseteq J_{\mathbb{Q}} \arrow[r, two heads, "\phi"] & Gal(L/\mathbb{Q}) \end{tikzcd}$$

Write $J_{\mathbb{Q}} = \{ a = (a_\infty, a_2, a_3, a_5, \dots),\ a_\infty \in \mathbb{R}^\times,\ a_\ell \in \mathbb{Q}_\ell^\times \}$.

$J_m = \{ a \in J_{\mathbb{Q}} : a_\infty > 0,\ a_p \equiv 1 \bmod p, (\text{i.e } v_p(a_p - 1) \geq v_p(m_0) = 1) \}$.

1) If $a \in J_m$, then $\phi(a) = (id(a), L/\mathbb{Q})$ ← Artin symbol.

as $id(a) = (n)$, $n = \prod_{\ell \text{ prime}} \ell^{v_\ell(a_\ell)}$. So $\phi(a)\zeta = \zeta^n$

2) $a = (-1, 1, 1, 1, \dots) \notin J_m$.

Multiply $a$ by the ppal idele $1-p = (1-p, 1-p, \dots)$ and recall $\phi(\mathbb{Q}^\times) = 1$.

Get $b = (p-1, 1-p, 1-p, \dots) \in J_m$ . So $\phi(a) = \phi(b) =$
$\qquad\qquad\qquad$ ↑ position $p$.

$id(b) = (1-p)$ . So $\phi(a) = (\underset{(p-1)}{\overset{}{(1-p)}}, L/\mathbb{Q}) = \zeta^{p-1} = \zeta^{-1}$ (take the positive generator of the ideal)

3) $a = (1, 1, \dots, \underset{\uparrow \text{position } p.}{p}, 1, 1, \dots) \notin J_m$

Let $b = \frac{1}{p} \cdot a = (p^{-1}, p^{-1}, \dots, \overset{\swarrow \text{pos } p.}{1}, p^{-1}, \dots) \in J_m$.

$id(b) = \mathbb{Z}$ because $a_\ell$ is an $\ell$-adic unit $\forall$ primes $\ell$.

Therefore $\phi(a) = 1$.

4) $a = (1, 1, \dots, \overset{\swarrow \text{pos } p}{u}, 1, \dots)$ , $u \in \mathbb{Z}_p^\times$. Let $u^*$ pos. integer s.t $u^* u \equiv 1 \bmod p$.

Then $\phi(a) = \phi(u^* a) = (id(u^*, u^*, \dots 1, u^*, \dots), L/\mathbb{Q}) = (u^*\mathbb{Z}, L/\mathbb{Q}) = \zeta^{u^*}$. //

Now let $L/K$ be a Galois extension. $G = \mathrm{Gal}(L/K)$.

Then $G$ acts on $J_L$ - we want that $(J_L)^G = J_K$ (as $L^G = K$).

So, how does $G$ act on $J_L$ ?..

Fix a prime $v$ of $K$. Then $G$ acts on $\prod_{w|v} L_w$ by: (recall $\sum_{w|v}[L_w : K_v] = [L/K]$)

- $[L/K] = [L_w/K_w]$ : Then $G = \mathrm{Gal}(L/K) =$ decomp gp $D_w \cong \mathrm{Gal}(L_w/K_v)$.
  So extend $G$ by continuity to $L_w$.
- Case $v$ splits completely in $L$: Then $\forall w|v$, $L_w = K_v$.
  Then $G$ permutes the copies of $K_v$

extreme cases

A little more motivation:

$$\begin{tikzcd} L \arrow[d, dash] & \mathfrak{P} \arrow[d, dash] & \sigma\mathfrak{P} \arrow[dl, dash] & \text{primes} \\ K & \mathfrak{P}_v & & \end{tikzcd}$$

Suppose $\mathfrak{P} = (\pi_\mathfrak{P})$, $\pi_\mathfrak{P} \in \mathcal{O}_L$.
Then $\sigma\mathfrak{P} = (\sigma\pi_\mathfrak{P})$, and $|\sigma\pi_\mathfrak{P}|_{\sigma\mathfrak{P}} = |\pi_\mathfrak{P}|_\mathfrak{P}$.

Fix a prime $v$ of $K$. Then $G$ acts on $\{w : w|v\}$ by $|\sigma\alpha|_{\sigma w} = |\alpha|_w$ $\alpha \in L$.

Quote from Tate's article in Cassel - Frohlich: "A cauchy sequence (from $L$) for $|\cdot|_w$ acted on by $\sigma \in \mathrm{Gal}(L/K)$ gives a c.s for $|\cdot|_{\sigma w}$, and conversely. So $\sigma$ induces by continuity an isomorphism $L_w \to L_{\sigma w}$"

Let $B = (b_w) \in \prod_{w|v} L_w$.

Def: $\sigma B$ has component $\sigma b_w$ in the $\sigma w$-position.

For $b \in J_L$, $(\sigma b)_{\sigma w} := \sigma b_w$. $\sigma$ acting on $L_w \to L_{\sigma w}$.

Remark: the group ring $K_v[D_w] \subseteq K_v[G]$. Then $\prod_{w|v} L_w \cong K_v[G] \otimes_{K_v[D_w]} L_w$

(induced representation).

(4.11) Prop: $L/K$ Galois, $G = \mathrm{Gal}(L/K)$. Then $(J_L)^G = J_K$.

Pf/ Suffices to prove $\left(\prod_{w|v} L_w\right)^G = K_v$

$\supseteq$] obvious.

$\subseteq$] Fix $w$, let $\sigma \in D_w$. Then know $L_w^{D_w} = K_v$,

So $\sigma w = w$ - component of $\sigma B$ is $\sigma b_w = b_w$ as $\sigma$ fixes $L_w$.

Repeat for each $w$, to conclude that $B \in \prod_{w|v} K_v^\times$

Now, use the transitive action of $G$ on $\{w : w|v\}$ to conclude that all components of $B$ are equal.

Let $A$ be a $G$-module, so $G$ acts on $A$, $G \times A \to A$.
(i.e. a $\mathbb{Z}[G]$-module)

If, $A, B$ are $G$-modules, then $f : A \to B$ is a hom of $G$-modules if it's a gp hom + $f(\sigma a) = \sigma f(a)$. (say $f$ is $G$-linear)

Define $A^G = \{a \in A : \sigma a = a \ \forall \sigma \in G\} \leq A$.

Given a s.e.s of $G$-modules $0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$

Apply the functor of fixed points $(\cdot)^G$:

$$0 \to A^G \to B^G \to C^G \xrightarrow{\delta} H^1(G,A) \to H^1(G,B) \to H^1(G,C) \xrightarrow{\delta} H^2(G,A) \to \cdots$$

is a long-exact sequence of abelian gps.

$$H^1(G,A) = \frac{Z^1(G,A)}{B^1(G,A)}$$

1-cocycles $Z^1(G,A) := \{$ functions $\varphi : G \to A$ s.t. $\varphi(\sigma\tau) = \varphi(\sigma) + \sigma\varphi(\tau)$, $\sigma, \tau \in G \}$.
(gp under addition)

1-coboundaries $B^1(G,A) := \{$ functions $\varphi : G \to A$ s.t. $\exists\, a \in A$ s.t. $\varphi(\sigma) = \sigma a - a \ \forall \sigma \in G \}$.

Note: if $A^G = A$, then $H^1(G,A) = \mathrm{Hom}(G,A) = \mathrm{Hom}(G_{ab}, A)$.

Ref: Serre "Corps Locaux"; Cassels-Fröhlich, ...

• Hilbert's Theorem 90: $L/K$ galois, $G = \mathrm{Gal}(L/K)$. Then $H^1(G, L^\times) = 0$.

(Hilbert did it for cyclic extensions, easy to prove in general).

Application:

(4.12) Recall that the idele class gp is $C_L := J_L/L^\times$, $C_K = J_K/K^\times$.

Then $G$ acts on $C_L$, and $C_L^G = C_K$.

Pf

$$1 \to L^\times \to J_L \to C_L \to 1$$ s.e.s. of $G$-modules.

Take $(\cdot)^G$: Note $(L^\times)^G = K^\times$, $(J_L)^G = J_K$.

$$\begin{tikzcd} 1 \arrow[r] & K^\times \arrow[r] & J_K \arrow[r] & (C_L)^G \arrow[r] & H^1(G, L^\times) \arrow[r] \arrow[d, equal, "\leftarrow H90"] & \cdots \\ & & & & 0 & \end{tikzcd}$$

Thus $C_K \simeq C_L^G$.

Corollary:
$$\frac{C_L^G}{N_{L/K} C_L} \cong \frac{J_K}{K^\times N_{L/K} J_L}.$$

Pf
$$\left.\begin{aligned} & C_L^G = C_K = J_K/K^\times. \\ & N_{L/K} C_L = N\left(J_L/L^\times\right) = N J_L . K^\times / K^\times \end{aligned}\right\} \Rightarrow \checkmark.$$

... Lang Chapter IX ...

We had the universal norm inequality, for $L/K$ finite galois:

$$(J_K : K^\times N J_L) \leq [L:K]$$

we did it by using analysis to show, for $\mathfrak{m}$ any modulus,

that $(I(\mathfrak{m}) : P_{\mathfrak{m}} \mathfrak{N}(\mathfrak{m})) \leq [L:K]$.

and then show that if $\mathfrak{m}$ is admissible, the LHS ~~are~~ equal.

Now we will show that, if $L/K$ is cyclic, we have equality.

We develop what Lang calls the Q-machine.

Let $G = \langle \sigma \rangle$, cyclic of order $n < \infty$.

Let $A$ be a $G$-module.

Define • $D : A \to A$, $D(a) := a - \sigma a = \overset{\mathbb{Z}[G]}{(1-\sigma)} \cdot a$ $(\forall a)$

• $N : A \to A$, $N(a) := a + \sigma \cdot a + \dots + \sigma^{n-1} \cdot a = \overset{\mathbb{Z}[G]}{\overbrace{(1+\sigma+\dots+\sigma^{n-1})}} \cdot a$

Note that $D \circ N = N \circ D = 0$

Thus $\operatorname{im} N \subseteq \operatorname{Ker} D$, $\operatorname{im} D \subseteq \ker N$.

Define then $H^0(G,A) := \dfrac{\operatorname{Ker} D}{\operatorname{Im} N} = \dfrac{A^G}{N(A)}$

$H^{-1}(G,A) := \dfrac{\operatorname{Ker} N}{\operatorname{Im} D} \left( \cong H^1(G,A) \right)$.

For $G$ cyclic, one proves that $\overset{\text{defined before}}{H^q(G,A)} = \begin{cases} H^0(G,A) & q \geq 2,\ q \text{ even} \\ H^{-1}(G,A) & q \geq 1,\ q \text{ odd}. \end{cases}$

Note that $\dfrac{C_L^G}{NC_L} \cong H^0(G, C_L)$

(5.1) Prop: $G$ cyclic, finite of order $n$. Given $0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$ exact of $G$-modules

Then we have an exact hexagon:

$$\begin{tikzcd}
 & H^0(G,A) \arrow[r, "f_0"] & H^0(G,B) \arrow[dr, "g_0"] & \\
H^1(G,C) \arrow[ur, "\delta"] & & & H^0(G,C) \arrow[dl, "\delta"] \\
 & H^1(G,B) \arrow[ul, "g_{-1}"] & H^{-1}(G,A) \arrow[l, "f_{-1}"'] &
\end{tikzcd}$$

Pf Use snake lemma for appropriate diagrams (see Lang).

Define: Herbrand quotient: Suppose $H^0(G,A)$, $H^{-1}(G,A)$ are finite

Let $Q(A) := \dfrac{|H^0(G,A)|}{|H^{-1}(G,A)|} \in \mathbb{Q}^\times$ ← note $Q(A)$ depends also on $G$!!

(5.2a) Theorem: $G$ cyclic of order $n$. Given ses $0 \to A \to B \to C \to 0$ of $G$-modules. Suppose that 2 out of 3 of $Q(A)$, $Q(B)$, $Q(C)$ are defined. Then the third is defined, and $Q(B) = Q(A) \cdot Q(C)$

Pf From (5.1) + Isomorphism theorems. //

Example: $A = \mathbb{Z}$, trivial $G$-action, $|G| = n$

In this case, $Q(\mathbb{Z}) = n$!

$$H^0(G,\mathbb{Z}) = \frac{\mathbb{Z}^G}{N(\mathbb{Z})} = \frac{\mathbb{Z}}{n\mathbb{Z}}, \quad H^{-1}(G,\mathbb{Z}) = \frac{\ker N}{\operatorname{Im} D} = \frac{\{0\}}{\{0\}} = \{0\}.$$

So $Q(\mathbb{Z}) = n$.

(5.2)(b): If C is finite, then $Q(C) = 1$.

Generalization of $H^0, H^1$ to any finite group $G$

Let $G$ be any finite gp, $A$ a $G$-module.

$$0 \to I_G \to \mathbb{Z}G \xrightarrow{f} \mathbb{Z} \to 0 \qquad f \text{ the augmentation map.}$$

$$\sum n_\sigma \sigma \mapsto \sum n_\sigma$$

Then $I_G$ is called the augmentation ideal, spanned as a $\mathbb{Z}$-module by all the $\sigma - 1$, $\sigma \in G$.

Define then $N := \sum \sigma \in \mathbb{Z}G$. So:

$$H^0(G,A) := A^G / N(A), \quad H^{-1}(G,A) = \frac{\ker(N)}{I_G(A)} \left( = \frac{\ker N}{\operatorname{Im}(\sigma_0 - 1)} \text{ if } G = \langle \sigma_0 \rangle \text{ cyclic} \right).$$

Rk: Theorem (5.2) applies only to $G$ cyclic!

(8.2) Prop (Restatement): $G$ a finite cyclic group.

(a) Suppose $0 \to A \to B \to C \to 0$ s.e.s of $G$-modules.

Then if 2 out of 3 of $Q(A), Q(B), Q(C)$ are defined, then so is the third, and $Q(B) = Q(A)\,Q(C)$.

(b) If $A$ is finite, then $Q(A) = 1$, for any $G$ module $A$.

Pf (b):

$$0 \to \ker D \to A \to \operatorname{im} D \to 0$$

$$0 \to \ker N \to A \to \operatorname{im} N \to 0$$

By 1st iso thm, $|A| = |\ker D| \cdot |\operatorname{im} D| = |\ker N|\,|\operatorname{im} N|$

$$\therefore \left|\frac{\ker D}{\operatorname{im} N}\right| = \left|\frac{\ker N}{\operatorname{im} D}\right| \quad //$$

(a) ommited. Uses the exact hexagon. //

• Outline of Chapter IX of Lang (pg 193):

$L/K$ cyclic. Know that $(J_K : K^\times N J_L) \overset{(*)}{\leq} [L:K]$. Want to show equality.

We know $J_K/K^\times N J_L \cong \underset{\overset{\parallel}{H^0(G, C_L)}}{\dfrac{C_K}{N(C_L)}}$, $C_K = J_K/K^\times$

because $C_L^G = C_K$.

To get equality in $(*)$, suffices to show that $Q(C_L) = [L:K]$, as

$$Q(C_L) = \frac{|C_K/NC_L| \leftarrow \leq [L:K] = N}{|H^{-1}(G, C_L)| \geq 1}$$

Note that $Q$ is multiplicative, but not $H^i$ $\left(H^i(G,B) \overset{\overset{\text{in general}}{\downarrow}}{\neq} H^i(G,A) \oplus H^i(G,C)\right)$

We might try $Q(C_L) = Q(J_L/L^\times) = Q(J_L)/Q(L^\times)$ but this is not ok, as $Q(L^\times)$ (and $Q(J_L)$) are infinite! $\left( H^0(G, L^\times) = \frac{K^\times}{NL^\times} \right)$

Clever detour: Choose a set $S$ of primes of $L$ so large that $J_L = L^\times J_S$;

$$J_S = \prod_{w \in S} L_w^\times \times \prod_{w \notin S} \mathcal{O}_w^\times$$

and $S$ $G$-stable, $S \supset S_\infty$, $S \supset$ ramified primes.

Then, $$\frac{J_L}{L^\times} = \frac{L^\times J_S}{L^\times} \underset{\text{iso thm}}{\cong} \frac{J_S}{J_S \cap L^\times} = \frac{J_S}{L_S}$$ where $L_S =$ $S$-units of $L$ $= \{\alpha \in L : |\alpha|_w = 1 \ \forall w \notin S\}$.

$\left[ \mathcal{O}_L^\times \subseteq L_S, \ \mathbb{Z}\text{-rank of } L_S = |S| - 1 \leftarrow \text{generalizes D. Unit thm} \right]$.

Fact: $Q(J_S)$, $Q(L_S)$ are defined!

Then we will compute that, if:

$S_K :=$ primes of $K$ below primes $S$ of $L$,

1) $Q(J_S) = \prod_{v \in S_K} [L_w : K_v]$ (select one $w$ above each $v$) (Local Calculation)

2) $Q(L_S) = \prod_{v \in S_K} [L_w : K_v] \Big/ [L:K]$

$\therefore Q(J_S)/Q(L_S) = [L:K] = Q(C_L) \Rightarrow$ ✓

In the following, we will prove (1) + (2).

Recall: $L/K$ Galois, prime $v$ of $K$, ~~have~~ a $K_v$-algebra $A := \prod_{w|v} L_w$, and $G$ acts on $A$. Then $A$ is called a semilocal representation of $G$.

If $H = D_w$ is decomp. gp, $G = \bigcup_{i=1}^{s} \sigma_i H$, coset reps, $\sigma_1 = 1$.

Then as a $\mathbb{Z}$-module, $\mathbb{Z}[G] = \bigoplus_{i=1}^{s} \sigma_i \mathbb{Z}H$.

Will generalize this:

## Semilocal Representations

Let $G$ be a finite group, $A$ a $G$-module s.t $\exists$ sgp $H \subseteq G$, and $\exists B \subseteq A$, $B$ an $H$-module s.t $A = \bigoplus_{i=1}^{s} \sigma_i B$ where $G = \bigcup \sigma_i H$

(Then $A \simeq \mathbb{Z}[G] \otimes_{\mathbb{Z}[H]} B$, $A$ is the induced representation)

Ex 1: $A = \prod_{w|v} L_w^\times$, fix $w = w_0$, $B := L_{w_0}^\times$, $G = Gal(L/K)$, $H = Gal(L_{w_0}/K_v)$.

This is the example just done before.

Ex 2: Normal Basis thm: $L/K$ finite Galois, then $\exists \alpha \in L$ s.t $\{\sigma\alpha : \sigma \in G\}$ are a $K$-basis of $L$. ($L$ is a free $K[G]$ module of rank 1)

Take $H = \{1\}$, $G = Gal(L/K)$, $B = \alpha K$, $A = L$.

Then $A = \bigoplus \sigma_i B$ just says $L = \bigoplus_{\sigma \in G} (\sigma\alpha) K$.

(5.3) Shapiro's Lemma: $G$ a finite group. Suppose $A, B, G, H$ as above. (i.e $A = \bigoplus \sigma_i B$).

Then: $H^i(G, A) \cong H^i(H, B)$ for $i = 0, -1$.

$\uparrow$ i.e. given $A, G$, suppose $\exists H, B$ as above.

(or start with $B$ an $H$-module, and form $A := \mathbb{Z}G \otimes_{\mathbb{Z}H} B$.)

In ex 1, Shapiro's lemma says: if $A = \prod_{w|v} L_w^\times$,

$H^i(G, \prod L_w^\times) \simeq H^i(D_{w_0}, L_{w_0}^\times)$ where $D_{w_0} = Gal(L_w/K_v)$, $i=0,-1$.

Then $H^{-1} = H^1(D_{w_0}, L_{w_0}^\times) \underset{\nwarrow \atop H90}{=} 0$.

Proof of Shapiro's lemma:

We'll do the case $i=0$. See Berg for $i=1$, or see Milne for a more high-fancy proof.

Have the projection $\pi : A \longrightarrow B$ by $\pi(\sum \sigma_i b_i) = b_1$ (project on 1st factor),

recall that $A \simeq \oplus \sigma_i B_i$ with $\sigma_1 = 1 \in G$.

Claim: $A^G = \{ \sum_{i=1}^{s} \sigma_i b_1 : b_1 \in B^H \}$

pf

$\supseteq]$ Let $a = \sum \sigma_i b_1$, To show $\sigma a = a$:

If $\sigma\sigma_i \in \sigma_j H$, then $\sigma\sigma_i = \sigma_j \tau$, $\tau \in H$. Then the $j^{th}$ component of $\sigma a$ is $\sigma_j \tau b_1 = \sigma_j b_1$ since $b_1 \in B^H$. The $a^{th}$ component of $a$ is also $\sigma_j b_1$, so //.

$\subseteq]$ Let $a = \sum \sigma_i b_i \in A^G$. To show: $a = \sum \sigma_i b_1$, $b_1 \in B^H$.

Let $\sigma := \sigma_j^{-1}$. Then the 1st component of $\sigma a$ is $\sigma_j^{-1}\sigma_j b_j = b_j$,

So $b_j = b_1$ $\forall j$. Now as $H \subseteq G$ and $\sigma a = a$ $\forall \sigma \in H$, then $b_1 \in B^H$. //

So $\pi : A^G \xrightarrow{\sim} B^H$ is an isomorphism.

In $G$, $N_G = \sum_{\sigma \in G} \sigma$, $N_H = \sum_{\sigma \in H} \sigma$. Have also $\overset{\text{in } \mathbb{Z}G}{N_G} = N_G \cdot \sigma = \sigma N_G$

and $N_G = \sum_{i=1}^{s} \sigma_i N_H$. So $N_G(\sigma_j a) = N_G(a) = \sum_{i=1}^{s} \sigma_i N_H(a)$ $\forall a \in A$.

Taking $a = \sum \sigma_i b_i$, get $N_G(A) = \bigoplus_i \sigma_i N_H(B)$, and so taking $\pi$,

$\pi(N_G(A)) \simeq N_H(B)$.

Now consider

$$\begin{tikzcd} L_w \arrow[d, dash, "G"] \\ K_v \arrow[d, dash] \\ \mathbb{Q}_p \end{tikzcd}$$

$L_w/K_v$ Galois, cyclic with unit gp $\mathcal{O}_w^\times$.

want to show $Q(\mathcal{O}_w^\times) = 1$, and that $|H^i(G, \mathcal{O}_w^\times)| = e(L_w/K_v)$

So we'll show $\exists$ $G$-submodule $M \subset \mathcal{O}_w^\times$, of finite index, which is free,

$\cong \mathcal{O}_v[G]$ where $\mathcal{O}_v$ is the valuation ring of $K_v$.

Then use the $Q$-machine, as $G$ is cyclic:

$$1 \longrightarrow M \longrightarrow \mathcal{O}_w^\times \longrightarrow \mathcal{O}_w^\times/M \longrightarrow 1.$$

$$Q(\mathcal{O}_w^\times) = Q(M) \cdot Q(\text{finite}) = 1 \cdot 1 = 1.$$

<u>p-adic logarithm</u> (use to convert $\times \longmapsto +$).

Let $x \in K_v$ $\setminus_{\mathbb{Q}_p}$. Then $\log(1+x) = \sum_{n=1}^{\infty} (-1)^{n+1} \frac{x^n}{n}$ converges if $|x|_v < 1$

That is, $x \in \hat{\mathfrak{p}}_v$.

<u>Examples</u>: will apply $(1 + p\mathbb{Z}_p, \cdot) \overset{\log}{\cong} (p\mathbb{Z}_p, +)$. ($p$ odd), and $1 + 4\mathbb{Z}_2 \cong 4\mathbb{Z}_2$

<u>Notation</u>: for $K_v$, $p\mathcal{O}_v = \pi^e \mathcal{O}_v$, and $v(u\pi^n) = n \in \mathbb{Z}$, $(u \in \mathcal{O}_v^\times)$.

<u>Prop</u> (5.4)

(a) The series $\sum (-1)^{n+1} \frac{x^n}{n}$ converges for $v(x) \geq 1$ $(|x| < 1)$.

(b) Assume $v(x) > \frac{e}{p-1}$. Then $v\left(\frac{x^n}{n}\right) > v(x)$ for $n \geq 2$, hence $v(x) = v(\log(1+x))$.

<u>Pf later</u>:

**Exponential:**

$1+\hat{\mathfrak{p}}^r \underset{\exp}{\overset{\log}{\rightleftarrows}} \hat{\mathfrak{p}}^r$ want for $r$ large enough, that log, exp are inverse.

$$\exp(x) := \sum_{n\geq 0} \frac{x^n}{n!}$$

(5.5) Prop: $\exp(x)$ converges for $v(x) > \frac{e}{p-1}$. In that case, $v\left(\frac{x^n}{n!}\right) > v(x)$ for $n \geq 2$,

hence $v(x) = v(\exp(x)-1)$.

Pf later.

After proving that the series converge, we deduce that $\begin{cases} \log((1+x)(1+y)) = \log(1+x)+\log(1+y) \\ e^{x+y} = e^x e^y. \end{cases}$

To prove (5.4) & (5.5), use that

$$p^t \| n! \Rightarrow t = \sum_{k=1}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor = \frac{n-s_n}{p-1}$$ where if $n = a_0 + a_1 p + \dots + a_r p^r$ $0\leq a_i < p$ then $s_n = \sum a_i$.

Proof (5.4) & (5.5):

∘(5.4):

a) $\log(1+x) = \sum_{n\geq 1}^{\infty} \frac{x^n}{n}(-1)^{n+1}$ converges $\Leftrightarrow \left|\frac{x^n}{n}\right| \to 0$

Note that if $|x| \geq 1$, then $\left|\frac{x^n}{n}\right| \not\to 0$.

Conversely, $v\left(\frac{x^n}{n}\right) = n\,v(x) - v(n) \geq n - \overset{\text{usual log.}}{\log_p}(n) \longrightarrow \infty$ as $n \to \infty$.

b) if $v(x) > \frac{e}{p-1}$, then if $p^r \leq n < p^{r+1}$, $p^s \| n$, (~~so~~ $s \leq r$) $(n \geq 2)$

Hence $v(n) = e\cdot s$. Then $v\left(\frac{x^n}{n}\right) - v(x) = n\,v(x) - v(x) - v(n) = (n-1)\,v(x) - e s >$

$> \frac{(n-1)e}{p-1} - es = e\left(\frac{n-1}{p-1} - s\right) \geq e\left(\frac{n-1}{p-1} - r\right) \geq 0$ check.

Remarks: 1) if $x, y \in 1+\hat{\mathfrak{p}}_w$, then define $\log(x) := \log(1+(x-1))$, so $|x-1|<1$.

2) $\log(x\cdot y) = \log(x) + \log(y)$ (formal power series identity + convergente series).

More remarks:

- Suppose $\zeta^{p^k} = 1$. Then $\log \zeta = 0$ : Let $L_w = \mathbb{Q}_p(\zeta)$.

  Note $|\zeta - 1| < 1$, so $\log(\zeta)$ is defined.

  And $\underset{\underset{0}{\shortparallel}}{\log}(\zeta^{p^k}) = p^k \log(\zeta) \Rightarrow \log(\zeta) = 0$.

- Suppose $\sigma$ is an aut. of $L_w$. Then $\log(\sigma x) = \sigma \log(x)$ by continuity of $\sigma$.

Pf of (5.5):

$$\exp(x) = \sum_{n \geq 0} \frac{x^n}{n!}, \quad x \in L_w.$$

$$v\left(\frac{x^n}{n!}\right) = n v(x) - v(n!) = n v(x) - \frac{(n - s_n) e}{p-1} = \frac{n(p-1) v(x) - (n - s_n) e}{p-1} \quad \ldots \text{(exercise)}.$$

//

(5.6) Theorem: in $L_w$, let $a > \frac{e}{p-1}$. Then

$$(1 + \hat{\mathfrak{p}}_w^a, \cdot) \overset{\ell}{\cong} (\hat{\mathfrak{p}}_w^a, +) \quad \text{and if } \sigma \in \mathrm{Aut}(L_w), \text{ then } \ell(\sigma x) = \sigma \ell(x).$$

Pf Just done; //

Local norm index:

(5.7): $L_w/K_v$ cyclic, $G = \mathrm{Gal}(L_w/K_v)$.

1) $Q(G, L_w^\times) = (K_v^\times : N L_w^\times) = [L_w : K_v]$.

2) $Q(G, \mathcal{O}_w^\times) = 1$, and $(\mathcal{O}_v^\times : N\mathcal{O}_w^\times) = e(L_w/K_v)$.

Rk: if $L_w/K_v$ is unramified, then we know (2) already!

Pf of (5.7)

H90 $\Rightarrow$ $H^{-1}(G, L_w^\times) = 0$. So $\overset{Q(G,L_w^\times)}{\overset{\shortparallel}{Q}}(L_w^\times) = \# H^0(G, L_w^\times) = (K_v^\times : N L_w^\times)$.

Consider now the ses of G modules: $1 \to \mathcal{O}_w^\times \to L_w^\times \xrightarrow{v} \mathbb{Z} \to 0$ ← trivial G-action

$\pi^n u \longmapsto n$

$\therefore Q(L_w^\times) = Q(\mathcal{O}_w^\times) \cdot Q(\mathbb{Z}) = Q(\mathcal{O}_w^\times) \cdot [L_w : K_v]$

← $Q(\mathbb{Z}) = \# G$.

↓

Cassels- Fröhlich

5.14a

*Proof.* Suppose for example that $h(A)$ is defined. From the exact sequences

$$0 \to \mathrm{Ker}(f) \to A \to f(A) \to 0$$
$$0 \to f(A) \to B \to \mathrm{Coker}(f) \to 0$$

it follows from Prop. 10 and 11 that $h(f(A))$ is defined and equal to $h(A)$, then that $h(B)$ is defined and equal to $h(f(A))$.

PROPOSITION 12. *Let $E$ be a finite-dimensional real representation space of $G$, and let $L$, $L'$ be two lattices of $E$ which span $E$ and are invariant under $G$. Then if either of $h(L)$, $h(L')$ is defined, so is the other, and they are equal.*

For the proof of Prop. 12 we need the following lemma:

LEMMA. *Let $G$ be a finite group and let $M$, $M'$ be two finite-dimensional $\mathbf{Q}[G]$-modules such that $M_{\mathbf{R}} = M \otimes_{\mathbf{Q}} \mathbf{R}$ and $M'_{\mathbf{R}} = M' \otimes_{\mathbf{Q}} \mathbf{R}$ are isomorphic as $\mathbf{R}[G]$-modules. Then $M$, $M'$ are isomorphic as $\mathbf{Q}[G]$-modules.*

*Proof.* Let $K$ be any field, $L$ any extension field of $K$, $A$ a $K$-algebra. If $V$ is any $K$-vector space let $V_L$ denote the $L$-vector space $V \otimes_K L$. Let $M$, $M'$ be $A$-modules which are finite-dimensional as $K$-vector spaces. An $A$-homomorphism $\varphi: M \to M'$ induces an $A_L$-homomorphism $\varphi \otimes 1: M_L \to M'_L$, and $\varphi \mapsto \varphi \otimes 1$ gives rise to an isomorphism (of vector spaces over $L$)

$$(\mathrm{Hom}_A(M, M'))_L \cong \mathrm{Hom}_{A_L}(M_L, M'_L). \qquad (8.3)$$

In the case in point, take $K = \mathbf{Q}$, $L = \mathbf{R}$, $A = \mathbf{Q}[G]$, so that $A_L = \mathbf{R}[G]$. The hypotheses of the lemma imply that $M$ and $M'$ have the same dimension over $\mathbf{Q}$, hence by choosing bases of $M$ and $M'$ we can speak of the *determinant* of an element of $\mathrm{Hom}_{\mathbf{Q}[G]}(M, M')$, or of $\mathrm{Hom}_{\mathbf{R}[G]}(M_{\mathbf{R}}, M'_{\mathbf{R}})$. (It will of course depend on the bases chosen.)

From (8.3) it follows that if $\xi_i$ are a $\mathbf{Q}$-basis of $\mathrm{Hom}_{\mathbf{Q}[G]}(M, M')$, they are also an $\mathbf{R}$-basis of $\mathrm{Hom}_{\mathbf{R}[G]}(M_{\mathbf{R}}, M'_{\mathbf{R}})$. Since $M_{\mathbf{R}}$, $M'_{\mathbf{R}}$ are $\mathbf{R}[G]$-isomorphic, there exist $a_i \in \mathbf{R}$ such that $\det(\sum a_i \xi_i) \neq 0$. Hence the polynomial

$$F(t) = \det(\textstyle\sum t_i \xi_i) \in \mathbf{Q}[t_1, \ldots, t_m],$$

where $t_i$ are independent indeterminates over $\mathbf{Q}$, is not identically zero, since $F(a) \neq 0$. Since $\mathbf{Q}$ is infinite, there exist $b_i \in \mathbf{Q}$ such that $F(b) \neq 0$, and then $\sum b_i \xi_i$ is a $\mathbf{Q}[G]$-isomorphism of $M$ onto $M'$.

For the proof of Prop. 12, let $M = L \otimes \mathbf{Q}$, $M' = L' \otimes \mathbf{Q}$. Then $M_{\mathbf{R}}$ and $M'_{\mathbf{R}}$ are both $\mathbf{R}[G]$-isomorphic to $E$. Hence by the lemma there is a $\mathbf{Q}[G]$-isomorphism $\varphi: L \otimes \mathbf{Q} \to L' \otimes \mathbf{Q}$. $L$ is mapped injectively by $\varphi$ to a lattice contained in $(1/N)L'$ for some positive integer $N$. Hence $f = N . \varphi$ maps $L$ injectively into $L'$; since $L, L'$ are both free abelian groups of the same (finite) rank, $\mathrm{Coker}(f)$ is finite. The result now follows from the Corollary to Prop. 11.

Note that $Q(\mathcal{O}_w^\times)$ is defined, since both $Q(\mathcal{U})$ and $Q(L_w^\times)$ are.

So to see (1) it's enough to see that $Q(\mathcal{O}_w^\times)=1$.

By (5.6), for suff large $a$, $1+\hat{\mathfrak{p}}_w^a \cong \hat{\mathfrak{p}}_w^a$ as $G$-modules.

So $\mathcal{O}_w^\times / 1+\hat{\mathfrak{p}}_w^a$ is finite $\Rightarrow Q(\mathcal{O}_w^\times) = Q(1+\hat{\mathfrak{p}}_w^a) \overset{\Downarrow}{=} Q(\hat{\mathfrak{p}}_w^a)$.

There $\exists\, \alpha \in L_w$ s.t. $\{\sigma\alpha : \sigma \in G\}$ are a $K_v$-basis for $L_w$ (Normal Basis thm)

Let $M = \sum_{\sigma \in G} \mathcal{O}_v(\sigma\alpha)$ ($\mathcal{O}_v$ = val ring of $K_v$).

So $K_v M = L_w$. By multiplying $\alpha$ by a suitable power of $p$, we may assume that $M \subseteq \hat{\mathfrak{p}}_w^a$ (as $p \in K_v$, then $\sigma$ acts trivially on it).

But $\hat{\mathfrak{p}}_w^a / M$ is finite, so $Q(\hat{\mathfrak{p}}_w^a) = Q(M) = 1$, because $H^i(G,M)=0$ $i=0,-1$ (as $M \cong \mathcal{O}_v[G]$).

It only remains to see that $(\mathcal{O}_v^\times : N\mathcal{O}_w^\times) = e(L_w/K_v)$.

Since $Q(\mathcal{O}_v^\times)=1$, it suffices to show that $\#H^{-1}(G, \mathcal{O}_w^\times) = e$

Say $G = \langle\sigma\rangle$. $H^{-1}(G,\mathcal{O}_w^\times) = \dfrac{\ker(N : \mathcal{O}_w^\times \to \mathcal{O}_v^\times)}{(\mathcal{O}_w^\times)^{1-\sigma}}$.

$N(u)=1 \overset{H90}{\Leftrightarrow} \exists\, x \in L_w^\times$ st $u = \dfrac{x^\sigma}{x}$ (and conversely).

So $\ker N = (L_w^\times)^{1-\sigma}$ $\left(= \left\{ \dfrac{x}{x^\sigma} \,\Big|\, x \in L_w^\times \right\}\right)$. (note $\dfrac{x}{x^\sigma} \in \mathcal{O}_w^\times$, because if $\pi$ is a prime of $L_w$ so is $\sigma\pi$.)

Hence we need to compute $\dfrac{(L_w^\times)^{1-\sigma}}{(\mathcal{O}_w^\times)^{1-\sigma}}$

Note $L_w^\times \twoheadrightarrow L_w^{\times\, 1-\sigma}$ and $\mathcal{O}_w^\times \twoheadrightarrow \mathcal{O}_w^{\times\, 1-\sigma}$, so $L_w^\times / \mathcal{O}_w^\times \xrightarrow{D} \dfrac{(L_w^\times)^{1-\sigma}}{(\mathcal{O}_w^\times)^{1-\sigma}}$

Also, $K_v^\times \subseteq \ker D$.

Claim: $\dfrac{L_w^\times}{\mathcal{O}_w^\times K_v^\times} \underset{D}{\xrightarrow{\sim}} \dfrac{L_w^{\times\, 1-\sigma}}{\mathcal{O}_w^{\times\, 1-\sigma}}$

Pf Suppose $x^{1-\sigma} = u^{1-\sigma}$ for $x \in L_w^\times$, $u \in \mathcal{O}_w^\times$. So $\dfrac{x}{u} = \left(\dfrac{x}{u}\right)^\sigma$. As $G=\langle\sigma\rangle$, $\dfrac{x}{u} \in K_v^\times$. So $x \in K_v^\times \cdot \mathcal{O}_w^\times$. //

Finally, we compute $\#\left(\frac{L_w^\times}{\mathcal{O}_w^\times K_v^\times}\right)$.

Note that $\pi_K = \pi_L^{e(L/K)}\cdot u$, $u \in \mathcal{O}_w^\times$. So this group is cyclic of order $e(L_w/K_v)$ //

Remarks:

(1) Local CFT will show that (local) $L^\times/_{NL^\times} \cong Gal(L/K)$ for finite abelian exts.

(2) (5.7) $\Rightarrow$ $\left.\begin{array}{l}(K^\times : NL^\times) \text{ divides } [L:K] \\ (\mathcal{O}_K^\times : N\mathcal{O}_L^\times) \text{ divides } e(L/K)\end{array}\right\}$ L/K abelian.

Pf/ Suppose first

$$\begin{tikzcd} L_2 \arrow[d, dash, "\text{cyclic of deg } n_2"] \\ L_1 \arrow[d, dash, "\text{cyclic of deg } n_1"] \\ K \end{tikzcd}$$

We know $(L_1^\times : NL_2^\times) = n_2$, $(K^\times : NL_1^\times) = n_1$

Apply $\underbrace{N_{L_1/K}}_{=:N_1}$ to the first to get $(N_1 L_1^\times : N_1 NL_2^\times)$ divides $n_2$.

So $(K^\times : NL_2^\times)$ divides $n_1 n_2$.

Similarly for units. //

Back to Global Fields: Let $L/K/\mathbb{Q}$ exts of # fields, $G = Gal(L/K)$ cyclic.

Want to show that $Q(J_{L,S}) = \prod_{v\in S_K} [L_w : K_v]$ $(*)$

where $S$ = finite set of primes of L containing $S_\infty$ and ramified primes in $L/K$, and $S$ G-stable.

(Write $S_K$ = primes of K "under" S)

Proof of $(*)$:

write $J_S = \left(\prod_{v\in S_K} \prod_{w|v} L_w^\times\right) \times \left(\prod_{v\notin S_K} \prod_{w|v} \mathcal{O}_w^\times\right)$ (thanks to S being G-stable)

↓

(Cont pf)

Then $$H^i(G, J_S) = \prod_{v \in S_\infty} \left( H^i\left(G, \prod_{w|v} L_w^\times\right)\right) \times \prod_{v \notin S_\infty} \left( H^i\left(G, \prod_{w|v} \mathcal{O}_w^\times\right)\right)$$

Now, use Shapiro's lemma: each $\begin{cases} H^i\left(G, \prod_{w|v} L_w^\times\right) \simeq H^i(G_w, L_w^\times). \text{ (for any } w|v) \\ H^i\left(G, \prod_{w|v} \mathcal{O}_w^\times\right) \simeq H^i(G_w, \mathcal{O}_w^\times) \text{ (for any } w|v) \end{cases}$

$(G_w = \mathrm{Gal}(L_w/K_v))$

Now $H^i(G_w, \mathcal{O}_w^\times) = 0$ $\forall i=0,-1)$ since $w$ is unramified over $K_v$.

So $$H^i(G, J_S) \simeq \prod_{v \in S_\infty} H^i(G_w, L_w^\times) = \begin{cases} 0 \text{ (by H90) if } i=-1 \\ \prod_{v \in S_\infty} \underset{\substack{\uparrow \\ (\text{by } 5.7)}}{[L_w : K_v]} \text{ if } i=0. \end{cases}$$

**Remarks:** The proof shows that $H^{-1}(G, J_S) = 0$.

As $J_L = \varinjlim_{S \text{ finite}} J_S$ and then $H^{-1}(G, J_L) = \varinjlim H^{-1}(G, J_S) = \varinjlim 0 = 0$.

So: $H^1(G, J_L) = 0$ for $L/K$ cyclic. (H90 for ideles).

• S-units of $L/\mathbb{Q}$:

If $S$ is a finite set of primes of $L$ containing $S_\infty$, then:

Def The group of S-units $L_S = \{\alpha \in L^\times : |\alpha|_w = 1 \ \forall w \notin S\}$

(So if $S = S_\infty$, $L_S = \mathcal{O}_L^\times$).

Example: $L = \mathbb{Q}$; $S = \{\infty, 3, 7\}$. Then $L_S = \langle -1, 3, 7 \rangle \subseteq \mathbb{Q}^\times$. $(L_S \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z})$.

Example: $L = \mathbb{Q}(\sqrt{-5})$. $(2) = \mathfrak{p}_2^2$, $\mathfrak{p}_2$ not principal. $S = \{\infty, \mathfrak{p}_2\}$.

Then $L_S = \langle -1, 2 \rangle \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}$.

Theorem: $L_S \cong (\text{roots of unity in } L) \times \mathbb{Z}^{|S|-1}$. ($S = S_\infty$ is the unit theorem).

Proof (From Fröhlich-Taylor):

Let $S - S_\infty = \{\mathfrak{p}_1, \dots, \mathfrak{p}_m\}$, $m \geqslant 0$.

Define homomorphism $L_S \xrightarrow{f} \mathbb{Z}^m$ by $f(\alpha) := (v_{\mathfrak{p}_1}(\alpha), \dots, v_{\mathfrak{p}_m}(\alpha))$.

Let $h$ = class number of $L$. So $\mathfrak{p}_i^h = (\beta_i)$, $\beta_i \in \mathcal{O}_L$.

Then $f(\beta_i) = (0, \dots 0\, \overset{\swarrow \text{pos. } i\text{th}}{h}, 0 - 0)$

So im $f$ has finite index in $\mathbb{Z}^m$.

By algebra, then im $f \cong \mathbb{Z}^m$ ($f$ is <u>not</u> onto, though).

$\alpha \in \ker f \Leftrightarrow$ $\alpha \in \mathcal{O}_L^\times$.

$$1 \longrightarrow \mathcal{O}_L^\times \longrightarrow L_S \longrightarrow \mathbb{Z}^m \longrightarrow 0$$

As $\mathbb{Z}^m$ is projective, this splits $\Rightarrow$ $L_S \simeq \mathcal{O}_L^\times \times \mathbb{Z}^m$.

Hence $L_S \simeq \mu_L \times \mathbb{Z}^{r_1+r_2-1} \times \mathbb{Z}^m = \mu_L \times \mathbb{Z}^{|S|-1}$

(5.10) Theorem: Suppose $L/K$ cyclic, $G = \mathrm{Gal}(L/K)$. Let $S$ be a finite set of primes of $L$, containing $S_\infty$ and $G$-stable.

Then: $Q(G, L_S) = \prod_{v \in S_K} [L_w : K_v] \Big/ [L:K]$ ($S_K$ = primes of $K$ below $S$).

$\uparrow$ select one $w|v$ for each $v$.

(5.11) Lemma: Let $G$ be a cyclic group, $V$ a fin. dim. $\mathbb{R}[G]$ module.

Let $M, N$ be lattices in $V$ that span $V$ and are $G$-modules.

Then if either $Q(M)$, $Q(N)$ is defined, so is the other and they are equal.

Pf Handout

Pf of 5.10:

Form $V :=$ $\mathbb{R}$-vectorspace with basis the primes $w \in S$. Then $G$ acts on $S$, hence acts on $V$, making $V$ an $\mathbb{R}[G]$-module.

Example: $K=\mathbb{Q}$, $L=\mathbb{Q}(i)$, $S=\{\infty, p_2, p_5, p_5'\} = \{w_\infty, w_2, w_5, w_5'\}$.

A typical elt of $V$ will be $x = a w_\infty + b w_2 + c w_5 + d w_5'$, $a,b,c,d \in \mathbb{R}$.

$\sigma \in Gal(K/\mathbb{Q})$ is cpx conjugation, and $\sigma x = a w_\infty + b w_2 + \underbrace{d w_5 + c w_5'}_{\text{switches } w_5, w_5'}$.

As $G$-modules, $V \cong \mathbb{R}^2 \times \mathbb{R}[G]$.

Define a $G$-homomorphism

$$\log : L_S \longrightarrow V$$
$$u \longmapsto \sum_{w \in S} \overbrace{(\log |u|_w)}^{\mathbb{R}} \cdot w$$

where $|\cdot|_w$ is normalized so that the product formula holds.

Clearly it's gp hom. $G$ linear: $\log(\sigma u) = \sum_S (\log |\sigma u|_w) \cdot w$

As $w \mapsto \sigma w$ is a permutation of $S$, we get

$$= \sum_S (\log |\sigma u|_{\sigma w}) \cdot \sigma w \overset{|\sigma x|_{\sigma w} = |x|_w}{=} \sum_S (\log |u|_w) \cdot \sigma w = \sigma(\log u) \,//$$

Since $u \in L_S$, $|u|_w = 1$ for $w \notin S$.

The product formula says $1 = \prod_{\text{all } w} |u|_w = \prod_{w \in S} |u|_w \Rightarrow \sum_S \log |u|_w = 0$.

Hence $\text{im} \log \subseteq$ hyperplane $\{\sum_S x_w w : \sum x_w = 0, x_w \in \mathbb{R}\}. = H$.

Let $M^\circ = \log(L_S)$. By the proof of strong unit thm, $M^\circ$ is a lattice $\subseteq H$. and it spans it.

The $\text{Ker}(\log) = \mu_L$. So

$$1 \to \mu_L \to L_S \to M^\circ \to 0 \Rightarrow Q(L_S) = \overset{1}{\overset{\shortparallel}{Q(\mu_L)}} \cdot Q(M^\circ)$$

Let $\tilde{w} := \sum_{w\in S} w \in V$, and let $M = M^0 \oplus \mathbb{Z}\cdot\tilde{w}$. (Note $M^0 \cap \mathbb{Z}\tilde{w} = 0$)

Then $M$ is a lattice in $V$ spanning it.

We look for a second lattice $N$ in $V$.

Just define $N := \bigoplus_{w\in S}\mathbb{Z}w$. Then $N$ is a $\mathbb{Z}[G]$-module and it's easy to find its cohomology.

Write $\underset{\underset{S \text{ is } G \text{ stable}}{\uparrow}}{N} = \bigoplus_{v\in S_K}\left(\bigoplus_{w|v}\mathbb{Z}w\right)$. By Shapiro's lemma,

$$H^i(G,N) = \bigoplus_{v\in S_K} H^i\Big(G, \bigoplus_{w|v}\mathbb{Z}w\Big) = \bigoplus_{v\in S_K} H^i(\overset{\text{decomp. sgp.}}{G_w}, \underset{\text{trivial } G_w\text{-action}}{\mathbb{Z}w})$$

We know $H^0(G_w, \mathbb{Z}) = \mathbb{Z}/n_w\mathbb{Z}$, $n_w = [L_w:K_v]$, $H^1(G_w,\mathbb{Z}) = 0$.

Therefore, $Q(N) = \prod_{v\in S_K}[L_w:K_v]$.

~~By the 5 lemma~~, $Q(N) = Q(M)$ (by 5.11).

Now, $M = M^0 \oplus \mathbb{Z}\tilde{w} \Rightarrow Q(M) = Q(M^0)\,Q(\mathbb{Z}) = Q(M^0)\cdot[L:K]$.

Hence $Q(L_S) = Q(M^0) = \prod \frac{[L_w:K_v]}{[L:K]}$ //

**(5.12) Theorem** (Global cyclic norm index):

$L/K$ cyclic.

1) $H^0(G, C_L)$ has order $[L:K]$.

2) $H^{-1}(G, C_L) = 0$

Pf Let $S$ be a finite set of primes of $L$, $G$ stable & containing ram. primes $\cup\ S_\infty$.

Need $J_{L,S}\cdot L^\times = J_L$. Then $Q(J_L/L^\times) = Q(J_{L,S}/L_S) = \frac{Q(J_{L,S})}{Q(L_S)}$

$$= \frac{\prod[L_w:K_v]}{\prod[L_w:K_v]/[L:K]}$$

. Then, just recall universal norm inequality, $\Rightarrow$ order of $H^0(G,C_L) \leq [L:K]$. //

Pf of 5.12 Again:

Consider $Q(C_L) = Q(G, C_L)$ where $S$ = finite set of primes of $L$ containing $S_\infty$, ramified primes and being $G$-stable

$$\overset{\shortparallel}{Q}(J_L/L^\times) = Q\left(J_S L^\times / L^\times\right) = Q\left(J_S / J_S \cap L^\times\right) = Q\left(J_S / L_S\right) =$$

$$= Q(J_S) / Q(L_S) = \frac{\prod_{v \in S_K} [L_w : K_v]}{\prod_{v \in S_K} [L_w : K_v] / [L:K]} = [L:K].$$

Just need to see that $H^{-1}(G, C_L) = 0$.

Or we go by universal norm inequality $\Rightarrow |H^0(G, C_L)| \overset{(\leq)}{\text{(divides)}} [L:K] \Rightarrow (1), (2)$ follow

(5.8) Lemma: $L/K$ abelian, $\mathfrak{m} = \mathfrak{m}_0 \mathfrak{m}_\infty$ an admissible modulus for $L/K$.
Then: if a prime $v$ of $K$ ramifies in $L$, then $v$ divides $\mathfrak{m}$.

Pf Recall $\mathfrak{m}$ admissible for $L/K$ means that $N_{L/K} J_L \supseteq W_\mathfrak{m} = \prod_{v | \mathfrak{m}} W_\mathfrak{m}(v) \times \prod_{v \nmid \mathfrak{m}} \mathcal{O}_v^\times$
where $W_\mathfrak{m}(v) \subsetneq \mathcal{O}_v^\times$.

From 5.7.(ii), if $w$ is ramified over $v$, then the norm $\mathcal{O}_w^\times \to \mathcal{O}_v^\times$ is not onto.
(the coker has order $e(w/v)$).

Chapter X of Lang

Rks: $L/K$ abelian extension. Let $\mathfrak{m}$ be a modulus of $K$, containing the ramified primes.
There's the Artin map $\omega_{L/K} : I_K(\mathfrak{m}) \longrightarrow Gal(L/K)$ (gp hom).
We showed (2.13) that $\omega_{L/K}$ is onto.
We also know that, if $\mathfrak{m}$ is admissible, $I_K(\mathfrak{m}) / P_\mathfrak{m} \mathfrak{N}(\mathfrak{m}) \simeq J_K / K^\times N(J_L)$ has the right order for cyclic ext. $([L:K])$

What's left: show that $\exists\, \mathfrak{m}$ s.t. $\omega_{L/K}(P_\mathfrak{m}) = 1$. !

(existence of a conductor). It was one of E Artin's main contributions (1927).

Claim: this is a type of reciprocity!

Why: $L = \mathbb{Q}(\sqrt{d})$, $K = \mathbb{Q}$, $d$ = discriminant.

Let $p$ be an odd prime. $p$ splits $\Leftrightarrow \left(\frac{d}{p}\right) = +1$.

$\left(\frac{\alpha}{p}\right)$ is periodic mod $p$ : trivial.

Quad. reciprocity says $\left(\frac{d}{p}\right)$ depends on $p$ mod $(4)d$.

Thus $4d$ (or $d$) is the conductor (the smallest $\mathfrak{m}$).

Exercise: finish it!

Formal properties of Artin Symbol:

$L/K$ Galois, $\mathfrak{P}$ a prime of $L$, unramified over $K$, $\mathfrak{p} := \mathfrak{P} \cap K$.

Let $f := [\mathcal{O}_L/\mathfrak{P} : \mathcal{O}_K : \mathfrak{p}]$ (so $N\mathfrak{P} = \mathfrak{p}^f$).

Recall that the Frobenius $F_{\mathfrak{P}} := (\mathfrak{P}, L/K)$ is the unique lift of $\alpha \mapsto \alpha^q$ mod $\mathfrak{P}$, $\alpha \in \mathcal{O}_L$ where $q = |\mathcal{O}_K : \mathfrak{p}|$, to an element of $\mathrm{Gal}(L/K)$.

Then $\alpha^{F_{\mathfrak{P}}} \equiv \alpha^q$ mod $\mathfrak{P}$.

if $L/K$ is abelian, we have that $\mathfrak{P}, \mathfrak{P}'$ divide $\mathfrak{p}$, then $F_{\mathfrak{P}} = F_{\mathfrak{P}'}$, so $F_{\mathfrak{P}}$ depends only on $\mathfrak{p}$, and write $(\mathfrak{p}, L/K) := (\mathfrak{P}, L/K)$.

↖ Artin symbol.

Then if $\mathfrak{a} = \prod \mathfrak{p}_i^{a_i}$, $\mathfrak{p}_i$ unramified, $(\mathfrak{a}, L/K) := \prod (\mathfrak{p}_i, L/K)^{a_i}$

Takagi had shown (before Artin) that $I_K(\mathfrak{m}) / P_{\mathfrak{m}} N(\mathfrak{m}) \cong \mathrm{Gal}(L/K)$ but without using the Artin map, which was introduced by Artin (later).

Properties. $L/K$ abelian. $\tau$ an (Aut) of $L$ (any, not fix $K$). Then

$$\begin{tikzcd}
L \arrow[r, dash] \arrow[d, dash] & \tau L \arrow[d, dash] \\
K \arrow[r, dash] & \tau K
\end{tikzcd}$$

Then (Math 800) $\mathrm{Gal}(\tau L/\tau K) = \tau\, \mathrm{Gal}(L/K)\, \tau^{-1}$

Also, check $(\tau\mathfrak{P}, \tau L/\tau K) = \tau(\mathfrak{P}, L/K)\tau^{-1}$

($\mathfrak{P}$ an unram. prime of $L$).

Then $\mathfrak{P}$ unramified of $L$, then

A1: $(\tau\mathfrak{a}, \tau L/\tau K) = \tau(\mathfrak{a}, L/K)\tau^{-1}$ ($\mathfrak{a}$ an ideal of $K$, if $\mathfrak{p}|\mathfrak{a}$, require that $\mathfrak{p}$ unram in $L/K$)

A2: $L' \,|\, L \,|\, K$ abelian. Then $\mathrm{res}_L((\mathfrak{a}, L'/K)) = (\mathfrak{a}, L/K)$.

(ie:
$$\begin{tikzcd}
I_K(m) \arrow[r, "\omega"] \arrow[d, equal] \arrow[dr, phantom, "\circlearrowleft"] & \mathrm{Gal}(L'/K) \arrow[d, "\mathrm{res}"] \\
I_K(m) \arrow[r, "\omega"] & \mathrm{Gal}(L/K)
\end{tikzcd}$$
)

A3: $L/K$ abelian, $F/K$ any extension. Then: $\mathrm{Gal}(LF/F) \xrightarrow[\mathrm{res}]{\simeq} \mathrm{Gal}(L/L\cap F)$

$$\begin{tikzcd}
& & LF \supseteq \mathfrak{q}' \arrow[dll, dash] \arrow[d, dash] \\
\mathfrak{q}'\cap L = \mathfrak{P} \supseteq L \arrow[d, dash] & & F \supseteq \mathfrak{q} = \mathfrak{q}'\cap F \arrow[dll, dash] \\
L\cap F \arrow[d, dash] & & \\
K \supseteq \mathfrak{p} = \mathfrak{q}'\cap K & &
\end{tikzcd}$$

Assume all primes are unramified.

Then: $\mathrm{res}_L(\mathfrak{q}, LF/F) = (\mathfrak{p}, L/K)^f$

where $f = [\mathcal{O}_F/\mathfrak{q} : \mathcal{O}_K/\mathfrak{p}]$

Proof (A3): Let the Frob of $(\mathfrak{q}', LF/F)$ be the unique lift of $\overset{\mathcal{O}_{LF}}{\beta} \mapsto \beta^{q^f} \bmod \mathfrak{q}'$

where $q = |\mathcal{O}_K/\mathfrak{p}|$, $q^f = |\mathcal{O}_F/\mathfrak{q}|$.

Restrict it to $L$, to get the $f$th power of the lift of $\overset{\mathcal{O}_L}{\alpha} \mapsto \alpha^q \bmod \mathfrak{P}'$

Thus $\mathrm{res}_L(\mathfrak{q}, LF/F) = (\mathfrak{p}, L/K)^f$.

Restate of A3:

Let $\mathfrak{m}$ contain all the ramified primes.

$$\begin{tikzcd} I_F(\mathfrak{m}) \arrow[r, "\omega_{LF/F}"] \arrow[d, "N_{F/K}"'] & Gal(LF/F) \arrow[d, "res_L"] \\ I_K(\mathfrak{m}) \arrow[r, "\omega_{L/K}"'] & Gal(L/K) \end{tikzcd}$$

Note: $N_{F/K}(\mathfrak{q}) = \mathfrak{p}^f$.

A4: $\mathfrak{a}$ ideal of $F$, such that if $\mathfrak{q} | \mathfrak{a}$, then $\mathfrak{q} \cap K$ is unramified in $L$.

Then $res_L(\mathfrak{a}, LF/F) = (N_{F/K}\mathfrak{a}, L/K)$.

Rk: Special case $K \subseteq F \subseteq L$ (so $LF = L$). Then $(\overset{\text{ideal of } F.}{\mathfrak{a}}, L/F) = (N_{F/K}\mathfrak{a}, L/K)$.

Recall: for $K = \mathbb{Q}$, $L = \mathbb{Q}(\zeta_m)$, $\zeta_m^m = 1$; $\mathfrak{m} = (m)\infty$, $\beta \in \mathbb{Q}^\times$.

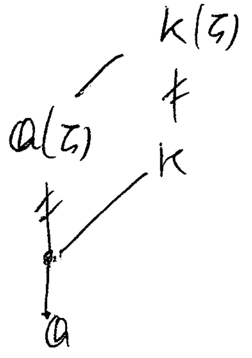
Then if $\beta \equiv 1 \bmod^* \mathfrak{m}$, then $\omega_{L/\mathbb{Q}}(\beta) = 1$.

(basically, this is saying if $k \equiv 1 \bmod m$, $k \in \mathbb{Z}$, then $\zeta \mapsto \zeta^k$ is the identity).

(6.2) Theorem: $L/K$ abelian and suppose ~~$\exists \mathfrak{m}$~~ s.t. $\exists\, m$ s.t. $L \subset K(\zeta_m)$.

Then $\exists$ a modulus $\mathfrak{m}$ of $K$, divisible only by $\mathfrak{p} | m$ and archimedean primes, such that $\alpha \equiv 1 \bmod^* \mathfrak{m} \Rightarrow \omega_{L/K}((\alpha)) = 1$.

Pf By consistency (A2), we may assume $L = K(\zeta)$.



By A4, $res_{\mathbb{Q}(\zeta)}(\mathfrak{a}, L/K) = (N_{K/\mathbb{Q}}(\mathfrak{a}), \mathbb{Q}(\zeta)/\mathbb{Q})$

If $\mathfrak{a} = (\alpha)$, $\alpha \in K^\times$, Then $res_{\mathbb{Q}(\zeta)}((\alpha), L/K) = ((N_{K/\mathbb{Q}}(\alpha)), \mathbb{Q}(\zeta)/\mathbb{Q})$

Call now $\beta := N_{K/\mathbb{Q}}(\alpha)$.

(cont pf)

if $\beta \in \mathbb{Q}^\times$ satisfies $\beta \equiv 1 \bmod^* m\infty$, then $((\beta), \mathbb{Q}(\zeta)/\mathbb{Q}) = 1$, as we have noted.

Appeal now to the continuity of local norms & to global norm = product of local norms to deduce that $\exists$ modulus $\mathfrak{m}$ of $K$ s.t. $\alpha \equiv 1 \bmod^* \mathfrak{m} \Rightarrow N_{K/\mathbb{Q}}(\alpha) \equiv 1 \bmod^* m\infty$

($\mathfrak{m}$ divisible only by primes dividing $m$ and $\infty$).

In the general case, we will try to reduce to this case of (6.2):

Sketch of Proof

Let $L/K$ cyclic. Suppose $\omega_{L/K}(\mathfrak{p}) = 1$.

$$\begin{tikzcd}[column sep=small]
 & L(\zeta) \arrow[d, dash] & \\
 & LE \arrow[dl, dash] \arrow[d, dash] & \\
L \arrow[d, dash] & E \arrow[dl] & \\
K & &
\end{tikzcd}$$

Artin's Lemma: $\exists$ integer $m$ and a subfield $E \subseteq L(\zeta_m)$

s.t. • $E \cap L = K$
- $E(\zeta) = L(\zeta)$
- $L \cap K(\zeta) = K$
- $\mathfrak{p}$ splits completely in $E$.

Suppose now $\mathfrak{P}$ of $E$ divides $\mathfrak{p}$ of $K$. By (A3), $\mathrm{res}_L(LE/E, \mathfrak{P}) = (N_{E/K}\mathfrak{P}, L/K)$
$= (\mathfrak{p}, L/K)$

Thus $(\mathfrak{p}, L/K)$ is "controlled" by $(\mathfrak{P}, LE/E)$, and $LE \subset E(\zeta)$, so we can apply there (6.2).

Then replace in general $\mathfrak{p}$ by $\prod \mathfrak{p}_i^{a_i}$, and $E$ by $E_i$ ...

· 3 lemmas :

(6.3) Lemma: Given integers $a, r$ each $\geq 2$, and a prime $q$, then $\exists\, p$ prime s.t the multiplicative order of $a$ mod $p$ is $q^r$.

Pf Idea: consider $p$ dividing $T = \dfrac{a^{q^r}-1}{a^{q^{r-1}}-1} \in \mathbb{Z}$

If $a^{q^r} \equiv 1$ mod $p$ and $a^{q^{r-1}} \not\equiv 1$ mod $p$, we're done.

Example: $q=2,\ a=3$.

$3-1=2$

$3^2-1=2^3$

$3^4-1=2^4 \cdot \boxed{5}$

$3^8-1=2^5 \cdot 5 \cdot \boxed{41}$

$3^{16}-1=2^6 \cdot 5 \cdot 41 \cdot \boxed{17}\,\boxed{193}$

$3^{32}-1=2^7 \cdot 5 \cdot 41 \cdot 17 \cdot 193 \cdot \boxed{21523361}$

Note that we always get new prime divisors.

~~(and only q divides to power > 1)~~

(and increments only by 1)

Suppose first $p \mid T$.

Case 1: $p \nmid a^{q^{r-1}}-1$ ✓.

Case 2: $p \mid a^{q^{r-1}}-1$ (bad primes)

Write $T = \dfrac{(X+1)^q-1}{X} = \left(a^{q^{r-1}}-1\right)^{q-1} + q\left(a^{q^{r-1}}-1\right)^{q-2} + \dots + q \quad (*)$

Then from $(*)$, if $p \mid T$, then need also that $p \mid q$, hence $p=q$.

circled ones in example

"new"

(2a) $q$ odd $\Rightarrow q-1 \geq 2$. From $(*)$, $q \,\|\, T$. But $T > q$, so $\exists$ prime dividing $T$, not dividing $a^{q^{r-1}}-1$

(2b) $q=2$. Then $T = a^{q^{r-1}}+1$. So $q=2$ divides $T \Rightarrow a$ odd.

$r-1 \geq 1 \Rightarrow T \equiv 1+1$ mod $4 \Rightarrow 2 \,\|\, T$, ~~but~~ as $T > 2$, $\exists$ new prime..

$$(\mathbb{Z}/m\mathbb{Z})^\times$$
$$\|$$

**Def** $\sigma, \tau \in$ group $G$ are independent if $\langle\sigma\rangle \cap \langle\tau\rangle =$ identity.

[6.4] Lemma 2 Given integers $a \geq 2$ and $n = q_1^{r_1} \cdots q_s^{r_s}$, $r_i \geq 1$.
$\exists$ integer $m = p_1 \cdots p_s\, p_1' \cdots p_s'$ with distinct primes $p_i > p_i'$
such that

$n \mid$ order of $a$ mod $m$.

And $\exists$ $b$ indep of $a$ in $(\mathbb{Z}/m\mathbb{Z})^\times$ s.t. $n \mid$ order of $b$ mod $m$.
Further the primes $p_i, p_i'$ may be chosen arbitrarily large.

Proof From Cor, $\exists$ arb. large primes $p$ s.t. $a$ mod $p$ has order div by a fixed power of $q$.

So $\exists$ primes $p_1, \ldots, p_s$ s.t. order of $a$ mod $p_i$ is $q_i^{r_i^*}$, $r_i^* > r_i$
($r_i^* \geq 2$).

and $\exists$ distinct primes $p_1', \ldots, p_s'$ s.t. order of $a$ mod $p_i'$ is $q_i^{r_i'}$, $r_i' \geq r_i^*$.

Thus $n \mid$ order of $a$ mod $m$.

Define $b$ by CRT $b \equiv \begin{cases} a \text{ mod } p_1 \cdots p_s \\ 1 \text{ mod } p_1' \cdots p_s'. \end{cases}$

Of course, $n \mid$ order of $b$ mod $m$.

Independence of $a, b$ mod $m$:

Suppose $a^u b^v \equiv 1$ mod $m$

$1 \equiv a^u b^v \equiv a^u$ mod $p_1' \cdots p_s'$

order of $a$ mod $p_i'$ is $q_i^{r_i'}$, $r_i' \geq r_i^* > r_i$

$\Rightarrow q_i^{r_i'} \mid u \Rightarrow a^u \equiv 1$ mod $p_1 \cdots p_s$

$\therefore a^u \equiv 1$ mod $p_1 \cdots p_s\, p_1' \cdots p_s'$

so $a^u \equiv b^v \equiv 1$ mod $m$.

QED

Remark

1) $6.3 \to 6.4$
replace $a$ mod $p$ has order $q^r$

$a$ mod $\prod p_i$ has order $\prod q_i^{r_i}$.

2) Given $a \geq 2$, $n$ : $\exists m$ s.t. $n \mid$ order of $\left((a), \mathbb{Q}(\zeta_m)/\mathbb{Q}\right)$.

Corollary: $a, q, r$ as above. Then $\exists\ \infty$-many primes $p$ such that $q^r$ divides the order of $a$ mod $p$.

Pf/ In above proof, replace $T$ by $\dfrac{a^{q^k}-1}{a^{q^{k-1}}-1}$, $k \geqslant r$, and let $k \to \infty$. //

Def $\sigma, \tau \in G$ $\left(=\left(\mathbb{Z}/m\mathbb{Z}\right)^\times \text{ in our case}\right)$. We say that $\sigma, \tau$ are independent if $\langle\sigma\rangle \cap \langle\tau\rangle = \{1\}$.

(6.4) Lemma 2: Given integers $a \geqslant 2$, $n = \prod_{i=1}^{s} q_i^{r_i}$, $r_i \geqslant 1$, then

$\exists$ integer $m = p_1 \cdots p_s\, p_1' \cdots p_s'$ with distinct primes $p_i, p_i'$

$\nwarrow\nearrow$ can be chosen to be arbitrarily large

such that $n \mid$ order of $a$ mod $m$, and

$\exists\, b$ indep. of $a$ in $\left(\mathbb{Z}/m\mathbb{Z}\right)^\times$ s.t. $n \mid$ order of $b$ mod $m$.

Proof: Use CRT. to define $b \equiv \begin{cases} a \bmod p_1 \cdots p_s \\ 1 \bmod p_1' \cdots p_s' \end{cases}$
(See handout for a proof). //

(6.5) Lemma 3: Given $S$ a finite set of rat'l primes, an ext. $L/K$, $n = [L:K]$, and a prime ideal $\mathfrak{p}$ of $K$;

then $\exists\, m \in \mathbb{Z}$ ~~relatively~~ $(m, \mathfrak{p}) = 1$ and $m$ relat. prime to primes in $S$, s.t.

1) $n \mid \operatorname{ord} \sigma = \left(\mathfrak{p}, K(\zeta_m)/K\right)$

2) $L \cap K(\zeta_m) = K$

3) $\exists\, \tau \in \operatorname{Gal}\left(K(\zeta_m)/K\right)$ independent of $\sigma$, with order divisible by $n$.

Pf of 6.5:

$$\begin{tikzcd} & K(\zeta_m) \arrow[d, dash] \\ K \arrow[ur, dash, "\times"] \arrow[d, dash] & \mathbb{Q}(\zeta_m) \\ \mathbb{Q} \arrow[ur, dash, "\times\times"] & \end{tikzcd}$$

Choose $m$ such that (and given by Lemma 2) $\left\{ \begin{array}{l} K \cap \mathbb{Q}(\zeta_m) = \mathbb{Q} \\ L \cap K(\zeta_m) = K \end{array} \right.$

Then $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \cong \mathrm{Gal}(K(\zeta_m)/K)$

Let $(a) = N_{K/\mathbb{Q}}\mathfrak{p}$, $a>0$, and take $b$ as in Lemma 2.

Then $\tau :=$ Aut. taking $\zeta_m \mapsto \zeta_m^b$

//

Artin's Lemma: Given $L/K$ cyclic of degree $n$; and $S$ a finite set of rat. primes. and $\mathfrak{p}$ a prime of $K$ unramified in $L$.

Then: $\exists$ integer $m$, prime to $\mathfrak{p}$ and $S$, & a finite extension $E/K$, such that $(\zeta = \zeta_m)$

(i) $L \cap K(\zeta) = K$

(ii) $\mathfrak{p}$ splits completely in $E$.

(iii) $E(\zeta) = L(\zeta)$.

(iv) $L \cap E = K$.

(i.e. Given $\begin{array}{c} L \\ | \\ K \end{array}$ cyclic can find $\begin{array}{c} LE \\ | \\ E \end{array}$ cyclotomic (of some degree))

$\uparrow$ i.e. inside a cyclotomic extension of $E$

Pf Choose $m$ as in lemma 3, so (i) holds.

Therefore, $\mathrm{Gal}(L(\zeta)/K) \simeq \underbrace{\mathrm{Gal}(L/K)}_{G,\ \text{cyclic } \langle\gamma\rangle,\ \gamma^n=1} \times \mathrm{Gal}(K(\zeta)/K)$.

Let $\sigma := (\mathfrak{p}, K(\zeta)/K)$ and have $\tau$ independent (from Lemma 3).

Define a sgp $H = \langle (\mathfrak{p}, L(\zeta)/K),\ \underset{\overset{\wedge}{\mathrm{Gal}(L(\zeta)/K)}}{\gamma\times\tau} \rangle \subseteq \mathrm{Gal}(L(\zeta)/K)$.

It is easy to see that $(\mathfrak{p}, L(\zeta)/K) = (\mathfrak{p}, L/K) \times (\mathfrak{p}, K(\zeta)/K) = \overset{\text{some } 0\le r<n}{\overset{\downarrow}{\gamma^r}} \times \sigma$

Define $E := L(\zeta)^H$.

$\downarrow$

(cont pf)

Remains to check (ii)(iii),(iv).

- $\mathfrak{p}$ splits completely in $E$ since $H$ contains Frobenius of $\mathfrak{p}$. $(= \gamma^r \times \sigma)$
- $E(\zeta) = E \cdot K(\zeta)$, which is the fixed field of $H \cap (G \times \{1\})$

Let $\theta \in H \cap (G \times \{1\})$. $\theta \in H \Rightarrow \theta = (\gamma^r \times \sigma)^u (\gamma \times \tau)^v$

Also $\theta \in G \times \{1\} \Rightarrow \sigma^u \tau^v = 1$. As $\sigma, \tau$ are independent, $\sigma^u = \tau^v = 1$

Moreover, $n \mid$ order $\sigma, \tau$ and $|G \times \{1\}| = n \Rightarrow \theta = 1$. //

- To see $E \cap L = K$, note that by def. of $E$, $L \cap E$ is the subfield of $L$ fixed by $H$.

As $H$ contains $\gamma \times \tau$ and $\mathrm{res}_L (\gamma \times \tau) = \gamma$, then $L^{\langle \gamma \rangle} = K \Rightarrow$ ✓.

Upgrade: Replace $\mathfrak{p}$ by a finite set $\{\mathfrak{p}_1, \dots, \mathfrak{p}_s\}$ primes of $K$ unramified in $L$. For each $i$, $1 \leq i \leq s$, choose $m_i$ as in Artin's Lemma. and construct $E_i$. Then define $E := E_1 \cdots E_s$.

(6.7) $E$ Claim: also satisfies $L \cap E = K$, so $\mathrm{Gal}(LE/E) \simeq \mathrm{Gal}(L/K)$.

$$\begin{tikzcd}
 & & LE \\
 & LE_i \arrow[ur, dash] & \\
L \arrow[ur, dash] & & E \arrow[uu, dash] \\
 & E_i \arrow[uu, dash] \arrow[ur, dash, dotted] & \\
K \arrow[uu, dash] \arrow[ur, dash] & &
\end{tikzcd}$$

$\mathfrak{p}_i$ splits completely in $E_i/K$.

(6.8) Theorem: $L/K$ cyclic of degree $n$, and let $\mathfrak{m}$ be admissible for $L/K$.

Then the kernel of $\omega_{L/K} : I_K(\mathfrak{m}) \twoheadrightarrow Gal(L/K)$ is $P_{\mathfrak{m}} \underbrace{\mathfrak{N}(\mathfrak{m})}_{\text{norms from } L/K.}$

Pf Strategy: want to show

$$\overbrace{\mathrm{Ker}\, \omega_{L/K} \subseteq P_{\mathfrak{m}} \mathfrak{N}(\mathfrak{m}) \underbrace{\subseteq I_K(\mathfrak{m})}_{[L:K] \text{ by } (5.12)}}^{[L:K]}$$

and then we will be done by the index of each.

Apply Artin's Lemma: First, suppose $\omega(\prod \mathfrak{p}_i^{a_i}) = 1$. (to show: $\prod \mathfrak{p}_i^{a_i} \in P_{\mathfrak{m}}\mathfrak{N}(\mathfrak{m})$)

$$\begin{tikzcd}[column sep=small, row sep=small]
 & E_i(\zeta_{m_i}) \arrow[d, dash] \\
 & E_iL \arrow[dd, dash, "\nmid"] \\
L \arrow[ur, dash] \arrow[dd, dash, "\nmid"'] & \\
 & E_i \\
K \arrow[ur, dash] &
\end{tikzcd}$$

$E_i$, $1 \leq i \leq r$ s.t. $\mathfrak{p}_i$ splits completely in $E_i$.

$\exists$ integer $m_i$, s.t. $LE_i \subset E_i(\zeta_{m_i})$

Let $E = E_1 \cdots E_r$. So have

$$\begin{tikzcd}[column sep=small, row sep=small]
E_i(\zeta_{m_i}) \arrow[d, dash] & \\
LE_i \arrow[r, dash] \arrow[d, dash, "\nmid"'] & LE \arrow[d, dash, "\nmid"] \\
E_i \arrow[r, dash] & E
\end{tikzcd}$$

Note that we don't know that $\omega(\mathfrak{p}_i^{a_i}) = 1$!

Let $\langle \gamma \rangle = Gal(L/K)$. So $(\mathfrak{p}_i^{a_i}, L/K) = \gamma^{d_i}$ and $\underline{hyp} \Rightarrow \sum_{i=1}^{r} d_i = n \cdot d$ (some $d$)

Take an ideal $\mathfrak{B}_E$ of $E$, prime to $\mathfrak{m}$ and all the $m_i$,

such that $(\mathfrak{B}_E, LE/E) = \gamma$, and let $\mathfrak{B}_K := N_{E/K}\mathfrak{B}_E$.

By property A4, $(\mathfrak{B}_K, L/K) = (N_{E/K}\mathfrak{B}_E, L/K) \overset{A4}{=} (\mathfrak{B}_E, LE/E) = \gamma$

So (1) $(\mathfrak{p}_i^{a_i}\mathfrak{B}_K^{-d_i}, L/K) = 1$

As $\mathfrak{p}_i$ splits completely in $E_i/K$ ($\Rightarrow$ it's a norm), and $\mathfrak{B}_K$ is a norm from $E \supset E_i$,

then $\exists$ ideal $\mathfrak{a}$ of $E_i$, prime to $\mathfrak{m}$ and all the $m_i$, such that

$N_{E_i/K}(\mathfrak{a}_i) = \mathfrak{p}_i^{a_i}\mathfrak{B}_K^{-d_i}$. So again by A4 and (1), $(\mathfrak{a}_i, LE_i/E_i) = 1$ (2)

↓

Then as $E_i \subset LE_i \subset E_i(\zeta_{m_i})$ (cyclotomic), then the conductor exists for $LE_i/E_i$, with modulus $\mathfrak{m}_i'$, divisible by $(m_i)\infty$.

Further, require $\mathfrak{m} \mid \mathfrak{m}_i'$.

Thus $\mathfrak{a}_i = (\beta_i) N_{LE_i/E_i}(\mathfrak{B}_i)$ where $\begin{cases} \beta_i \equiv 1 \bmod^* \mathfrak{m}_i', \ \beta_i \in E_i \\ \mathfrak{B}_i \text{ is an ideal prime to } \mathfrak{m}_i' \end{cases}$

(cyclotomic result). (6.1, 6.2)

Taking norms, $(N_{E_i/K})$

(3) $\beta_i^{a_i} \mathfrak{B}_K^{-d_i} = N_{E_i/K}(\beta_i) \cdot N_{LE_i/K}(\mathfrak{B}_i)$

As $\mathfrak{m} \mid \mathfrak{m}_i'$, then $N_{E_i/K}(\beta_i) \equiv 1 \bmod^* \mathfrak{m}$

Take now the product over all $i$:

$$\left(\prod \beta_i^{a_i}\right) \mathfrak{B}_K^{-nd} = \prod N_{E_i/K}(\beta_i) \cdot \prod N_{LE_i/K}(\mathfrak{B}_i) \in P_{\mathfrak{m}} \cdot \mathfrak{N}(\mathfrak{m})$$

Finally, $\mathfrak{B}_K^{-nd} =$ is an $n$th power of an ideal, so it's a norm:

$(\mathfrak{B}_K^{-nd} = N_{L/K}(\mathfrak{B}_K^{-d}).)$

Upgrade from cyclic to abelian:

(6.9) Main Theorem: $L/K$ abelian, $\mathfrak{m}$ admissible for $L/K$. Then $\omega_{L/K} : I_K(\mathfrak{m}) \to Gal(L/K)$ is onto with kernel $P_{\mathfrak{m}} \mathfrak{N}(\mathfrak{m})$.

Corollary:

$$C_K / N_{L/K} C_L \cong \frac{J_K}{K^\times N_{L/K} J_L} \cong \frac{I_K(\mathfrak{m})}{P_{\mathfrak{m}} \mathfrak{N}(\mathfrak{m})} \overset{\omega}{\cong} Gal(L/K)$$

Pf of Thm: Write $\mathrm{Gal}(L/K) = G_1 \times \cdots \times G_t$, $G_i$ cyclic.

Define $L_i := L^{\prod_{j \neq i} G_j}$ (check $\mathrm{Gal}(L_i/K) \simeq G_i$)

(and $L = L_1 L_2 \cdots L_t$). We know the result for each $L_i/K$.

Say $\mathfrak{m}_i$ is admissible for $L_i/K$, and choose $\mathfrak{m}'$ admissible for $L/K$ and divisible by all $\mathfrak{m}_i$.

So $P_{\mathfrak{m}} \subseteq P_{\mathfrak{m}_i}$.

$$\begin{tikzcd}
I_K(\mathfrak{m}) \arrow[r, "\omega_i"] \arrow[dr, "\omega_{L/K}"'] & \mathrm{Gal}(L_i/K) \\
& \mathrm{Gal}(L/K) \arrow[u, "\mathrm{res}_{L_i}\ (A1)"']
\end{tikzcd}$$

By (6.8), $P_{\mathfrak{m}_i} \subseteq \mathrm{Ker}\,\omega_i$.

$\therefore \bigcap P_{\mathfrak{m}_i} \subseteq \bigcap \mathrm{Ker}\,\omega_i = \mathrm{Ker}\,\omega_{L/K} \Rightarrow P_{\mathfrak{m}'} \subseteq \mathrm{Ker}\,\omega_{L/K}$.

$\rotatebox{90}{$\subseteq$}$

$P_{\mathfrak{m}'}$

$$\therefore P_{\mathfrak{m}'}\mathfrak{N}(\mathfrak{m}') \overbrace{\subseteq \underbrace{\mathrm{Ker}\,\omega_{L/K} \subseteq I_K}_{[L:K]}}^{\leq [L:K] \text{ (universal norm inequality) (2.14)}}(\mathfrak{m}') \Rightarrow \checkmark$$

So $P_{\mathfrak{m}'}\mathfrak{N}(\mathfrak{m}') = \mathrm{Ker}\,\omega_{L/K}$.

Finally, from (4.8), if $\mathfrak{f}$ is the smallest admissible modulus for $L/K$, then $I_K(\mathfrak{f})/P_{\mathfrak{f}}\mathfrak{N}(\mathfrak{f}) \simeq I_K(\mathfrak{m}'')/P_{\mathfrak{m}''}\mathfrak{N}(\mathfrak{m}'')$ for all admissible $\mathfrak{m}''$ (apply it to $\mathfrak{m}'' = \mathfrak{m}$ or $\mathfrak{m}'$)

We are close to the proof of Kronecker-Weber:

$L/\mathbb{Q}$ abelian, By $\exists$ of conductor $\mathfrak{m} = (m)\infty$, then $\operatorname{Ker} \omega_{L/\mathbb{Q}} = P_{\mathfrak{m}}\mathfrak{N}(\mathfrak{m})$.

To show: $L \subseteq \mathbb{Q}(\zeta_m)$.

Let $L' = \mathbb{Q}(\zeta_m)$. Then we know $\operatorname{Ker} \omega_{L'/\mathbb{Q}} = P_{\mathfrak{m}}$

The missing step is: if $\operatorname{Ker} \omega_{L/\mathbb{Q}} \supseteq \operatorname{Ker} \omega_{L'/\mathbb{Q}}$, then $L \subseteq L'$.

(note that the converse of this statement is trivial).

In <u>idele language</u>: $L', L$ abelian $/K$. If $K^\times N J_L \supseteq K^\times N J_{L'}$, then $L \subseteq L'$.

<u>Recall</u>: $$J_K \big/ K^\times N_{L/K} J_L \overset{f}{\cong} I(\mathfrak{m}) \big/ P_{\mathfrak{m}}\mathfrak{N}(\mathfrak{m})$$

Recall that $J_{\mathfrak{m}} = \{ a \in J_K : a \equiv 1 \bmod^* \mathfrak{m} \}$, $J_{\mathfrak{m}} \hookrightarrow J_K$.

Showed that $J_{\mathfrak{m}}/K_{\mathfrak{m}} \simeq J_K/K^\times$ (by weak approximation, given $a \in J_K$ $\exists \alpha \in K^\times$ s.t. $\alpha a \equiv 1 \bmod^* \mathfrak{m}$.)

So have
$$\begin{tikzcd} J_K/K^\times \arrow[r, phantom, "\simeq"] \arrow[rr, bend right, "\text{“}f\text{”}"'] & J_{\mathfrak{m}}/K_{\mathfrak{m}} \arrow[r, "\overset{\text{ideal map}}{\downarrow}\,\mathrm{id}"] & I(\mathfrak{m})/P_{\mathfrak{m}} \end{tikzcd}$$
+ mod-out the norms.

Define now $(a, L/K) := (\mathrm{id}(a\alpha), L/K) \leftarrow$ Artin symbol.

We have an injection
$$K_v^\times \xrightarrow{i_v} J_K$$
$$a_v \longmapsto (1,\dots,1, \overset{\overset{v}{\downarrow}}{a_v}, 1, \dots)$$

Let $S$ be a finite set of primes of $K$ containing $S_\infty$, the ramified primes in $L/K$ and the $v$'s such that $a_v$ is not a unit.

So if $v \notin S$, then $a_v \in N_{L_w/K_v}(\mathcal{O}_w^\times)$, $w \mid v$.

Thus $((a_v), L/K) = 1$. So $(a, L/K) = \prod_{v \in S} (i_v a_v, L/K)$

(6.10) $L/K$ abelian, then:

a) $J_K / K^\times N_{L/K} J_L \cong \mathrm{Gal}(L/K)$. and $(a, L/K) = \prod_{\text{all } v} (i_v a_v, L/K)$

b) $\mathfrak{p}_v$ unramified (in $L_w$) prime of $K_v$, ~~unramified~~ $\mathfrak{p}_v = \pi_v \mathcal{O}_v$ (note $i_v \pi_v \equiv 1 \bmod^* \mathfrak{m}$ so $\alpha = 1$)

$(i_v \pi_v, L/K) =$ Artin symbol $(\mathfrak{p}, L/K)$ where $\mathfrak{p} \subseteq \mathcal{O}_K$ corresponds to $\mathfrak{p}_v$.

c) If an infinite prime $v$ of $K$ is unramified in $L$, then $(i_v a_v, L/K) = 1$.

Comment: an alternative approach is to use $(a, L/K) = \prod_{\substack{v \in S \\ \uparrow \\ \text{or all } v}} (i_v a_v, L/K)$ as the definition of $(a, L/K)$.

Then can deduce global CFT from local CFT.

Properties A1-A3 for ideles: (not immediate, but easy).

A1: $L/K$ abelian, $\tau$ an iso.

$$\begin{tikzcd} L \arrow[r] \arrow[d] & \tau L \arrow[d] \\ K \arrow[r] & \tau K \end{tikzcd}$$

$\mathrm{Gal}(\tau L/\tau K) = \tau\, \mathrm{Gal}(L/K)\, \tau^{-1}$

$$\boxed{(\tau a, \tau L/\tau K) = \tau (a, L/K) \tau^{-1}, \ a \in J_K.}$$

A2 (consistency):

$$\begin{tikzcd} L' \arrow[d, dash] \\ L \arrow[d, dash] \\ K \end{tikzcd}$$

$L'/K$ abelian.

Then $$\boxed{\mathrm{res}_L (a, L'/K) = (a, L/K), \ a \in J_K.}$$

A3:

$$\begin{tikzcd} & & LF \arrow[d, dash, "\#" description] \\ L \arrow[urr, dash] \arrow[d, dash, "\#" description] & & F \\ L\cap F \arrow[urr, dash] \arrow[d, dash] & & \\ K & & \end{tikzcd}$$

For $b \in J_F$,

$(N_{F/K} b, L\cancel{F}/K) = \mathrm{res}_L (b, LF/F)$ $\Rightarrow$

$$\begin{tikzcd} J_F \arrow[r, "\omega_{LF/F}"] \arrow[d, "N_{F/K}"] \arrow[dr, phantom, "\circlearrowright"] & \mathrm{Gal}(LF/F) \arrow[d, "\mathrm{res}_L"] \\ J_K \arrow[r, "\omega_{L/K}"] & \mathrm{Gal}(L/K) \end{tikzcd}$$

Remark 1: $N_{F/k} J_F$ and hence $K^{\times} N_{F/K} J_F$ are open subgroups of $J_K$.

Pf: Show that $N_{F/K} J_F$ contain $W_m^{\subset \text{open}}$ for some $m$ and if they contain an open, then $N_{F/K} J_F$ is a union of cosets, all of them will be open.

Remark 2: By definition of the quotient topology, the open subgroup of $C_K := J_K/K^{\times}$ correspond to open subgroups of $J_K$ containing $K^{\times}$.

Remark 3: In the number field case, any open subgroup of $J_K$ containing $K^{\times}$ has finite index in $J_K$.

Existence & Uniqueness Thm: For every open subgroup $H$ of $C_K$ (of finite index by rk 3) there exists a unique abelian extension $L/K$ such that $N_{L/K} C_L = H$.

(proof later).

In this case, $H$ is called normic, $L$ is called the Class Field belonging to $H$, and $H$ the Class Group belonging to $L$.

Review: Case $K = \mathbb{Q}$. Then $J_{\mathbb{Q}} = \mathbb{R}_{>0}^{\times} \times \mathbb{Q}^{\times} \times \prod_{p \text{ prime}} \mathbb{Z}_p^{\times}$

Then $C_{\mathbb{Q}} := J_{\mathbb{Q}}/\mathbb{Q}^{\times} = \mathbb{R}_{>0}^{\times} \times \prod_{p} \mathbb{Z}_p^{\times}$

$\uparrow$ connected component not well-understood

(6.11) Prop: $L, L'$ (finite) abelian ext. of $K$, and say $L$ belongs to $\overset{C_K}{\overset{\cup}{H}}$, $L'$ to $\overset{C_K}{\overset{\cup}{H'}}$.

a) $L \subset L' \Leftrightarrow H \supset H'$

b) $LL'$ belongs to $H \cap H'$

c) $L \cap L'$ belongs to $HH'$

Comment: a lattice is a partially ordered set w/ l.u.b., g.l.b.

So this says that the lattice of finite abelian extensions of $K$ is "equivalent" to the lattice of open subgroups of the idele class group $C_K$.

$$\gamma : \mathcal{L} \to \mathcal{L}'$$
$$L \mapsto N_{L/K} C_L$$

← we are showing that $\gamma$ is a bijection, and $\gamma, \gamma'$ are order-reversing.

We first deduce uniqueness (in the Main Thm.) (taken from Tate's article in Cassels-Fröhlich)

Suppose $L, L'$ ab. ext. of $K$, $N_{L/K} C_L = N_{L'/K} C_{L'}$. to show: $L = L'$.

Let $M := LL'$, an abelian extension of $K$.

$$\begin{tikzcd}
1 \arrow[d] & 1 \arrow[d] \\
\frac{N_{L/K}(C_L)}{N_{M/K}(C_M)} \arrow[r, "\omega_{M/K}", "\simeq"'] \arrow[d] & Gal(M/L) \arrow[d] \\
C_K/N_{M/K}(C_M) \arrow[r, "\omega_{M/K}", "\simeq"'] \arrow[d] & Gal(M/K) \arrow[d] \\
C_K/N_{L/K}(C_L) \arrow[r, "\simeq", "\omega_{L/K}"'] \arrow[d] & Gal(L/K) \arrow[d] \\
1 & 1
\end{tikzcd}$$

$L \subset M$ is determined ~~by~~ as the fixed field of $Gal(M/L)$

But $Gal(M/L) = \omega_{M/K}\left(\frac{N_{L/K} C_L}{N_{M/K} C_M}\right)$

Similarly, $L'$ is the fixed field of

$$\omega_{M/K}\left(\frac{N_{L'/K} C_{L'}}{M_{M/K} C_M}\right)$$

But by hypothesis, $N_{L/K} C_L = N_{L'/K} C_{L'}$, so $Gal(M/L) = Gal(M/L') \Rightarrow L = L'$.

We are now left with the existence theorem.

First we will get a Corollary from (6.11) (equivalence of lattices).

The results that follow actually assume the main existence Theorem, which we will prove later.

Recall that, given a modulus $\mathfrak{m}$ of $K$, we have a subgroup $W_\mathfrak{m} \leq J_K$:

$$W_\mathfrak{m} = \prod_{v \nmid \mathfrak{m}} \mathcal{O}_v^\times \times \prod_{v \mid \mathfrak{m}_\infty} \mathbb{R}_{>0}^\times \times \prod_{v \mid \mathfrak{m}_0} (1 + \mathfrak{p}_v^{r_v}) \qquad (\mathfrak{p}_v^{r_v} \,\|\, \mathfrak{m}_0).$$

Def The class field $L'$ belonging to the open subgroup $K^\times W_\mathfrak{m}$ of $J_K$ is called the ray class field mod $\mathfrak{m}$ of $K$.

(i.e. $N_{L'/K} J_{L'} = K^\times W_\mathfrak{m}$).

The existence theorem will prove that the ray class field exists.

Restate for ideals:

Claim: $I_K(\mathfrak{m})/P_\mathfrak{m} \overset{\text{Artin}}{\cong} \mathrm{Gal}(L'/K)$ if $L'$ is the r.c.f. (i.e. norms are already in $P_\mathfrak{m}$)

Proof $J_\mathfrak{m}/K_\mathfrak{m} \cong J_K/K^\times$ (moving lemma).

Then
$$\begin{tikzcd} J_\mathfrak{m}/K_\mathfrak{m} W_\mathfrak{m} \arrow[r, phantom, "\cong"] \arrow[d, "\wr", "\mathrm{id}"'] & J_K/K^\times W_\mathfrak{m} \\ I_K(\mathfrak{m})/P_\mathfrak{m} & \end{tikzcd}$$

← Lang, pg 147.

//

Corollary to 6.11(a)

$\mathfrak{m}$ admissible for an abelian extension $L/K$,

Then $L \subset L' :=$ ray class field mod $\mathfrak{m}$.

Pf By definition of admissible, $N_{L/K}(J_L) \supset W_\mathfrak{m}$. So $K^\times N_{L/K}(J_L) \supset K^\times W_\mathfrak{m} = K^\times N_{L'/K}(J_{L'})$

Therefore $L \subset L'$.

//

(6.12) (Kronecker-Weber): Let $L/\mathbb{Q}$ be an abelian extension. Then $\exists$ positive integer $m$ such that $L \subset \mathbb{Q}(\sqrt[m]{1})$.

Pf/ Take an admissible modulus $\mathfrak{m}$ for $L/\mathbb{Q}$.

Then $\mathfrak{m} = (m)\underset{\wedge}{\infty}$ not needed if $L$ is real.

We know that $\underset{\left(\mathbb{Z}/m\mathbb{Z}\right)^{\times}/\pm}{I_{\mathbb{Q}}(\mathfrak{m})/P_{\mathfrak{m}}} \cong Gal(\mathbb{Q}(\sqrt[m]{1})/\mathbb{Q})$ by the Artin map.

The point is that $\mathbb{Q}(\zeta_m)$ is the ray-class field mod $(m)\infty$.

Apply the previous corollary to get $L \subset \mathbb{Q}(\sqrt[m]{1})$.

Note: There are more direct proof of this theorem. This is really short and follows from the theory we've developed.

(6.13) Let $E/K$ be a finite extension. not necessarily abelian! Let $H := N_{E/K}(C_E)$. Let $M$ be the maximal abelian extension of $K$ in $E$. Then $H = N_{M/K}C_M$.

Hence $[E:K] = (C_K : N_{E/K}C_E) \iff E/K$ abelian.

Pf/ $H$ open subgroup of $C_K$. So $H = N_{L/K}C_L$, $L/K$ abelian (by existence).

$\forall b \in C_E$, $N_{E/K}b \in H$. So $1 = (N_{E/K}b, L/K) \overset{A3}{=} (b, LE/E)$

In other words, $\operatorname{Ker} \omega_{LE/E} = C_E$ ! Thus $LE = E$, So $\overset{KT}{} L \subseteq E$.

In fact, $L$ is the maximal abelian extension of $K$ in $E$:

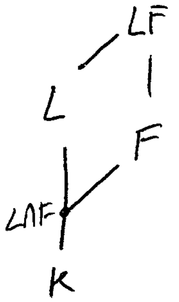
Let $L \subseteq M$: $L \subset M \subset E \Rightarrow N_{L/K}C_L \supset N_{M/K}C_M \supset N_{E/K}C_E$

equal!

So $N_{M/K}C_M = N_{L/K}C_L \underset{\text{uniqueness}}{\Rightarrow} L = M$

## (6.14) Translation theorem

Let $L/K$ an abelian extension, and $F/K$ any extension.



If $L/K$ belongs to an open subgroup $H \subseteq C_K$, then $LF/F$ belongs to $N_{F/K}^{-1}(H) \subseteq C_F$.

Pf/ By A3, have

$$\begin{tikzcd}
C_F \arrow[r, "\omega_{LF/F}"] \arrow[d, "N_{F/K}"'] \arrow[dr, phantom, "\circlearrowright"] & Gal(LF/F) \arrow[d, "res_L"] \\
C_K \arrow[r, "\omega_{L/K}"] & Gal(L/K)
\end{tikzcd}$$

We have that $LF/F$ belongs to $Ker\, \omega_{LF/F}$.

As $res_L$ is injective, $Ker\, \omega_{LF/F} = Ker\left(\omega_{L/K} \circ N_{F/K}\right) = N_{F/K}^{-1}\left(\overbrace{Ker\, \omega_{L/K}}^{H}\right)$ //

Example: $K = \mathbb{Q}$, $L = \mathbb{Q}(\zeta_m)$. Then $F(\zeta_m)/F$ belongs to $N_{F/\mathbb{Q}}^{-1}\left(\frac{\mathbb{Q}^\times W_{(m)\infty}}{\mathbb{Q}^\times}\right) \subseteq J_F/F^\times$.

## §7. Sketch of Kummer theory (Hungerford or Lang's Algebra).

Let $n > 1$, and assume $char\, K \nmid n$ or $char\, K = 0$.

Assume that $\mu_n \subset K^\times$.

Then if $\alpha \in K^\times$, $K(\sqrt[n]{\alpha})/K$ is the splitting field of $X^n - \alpha$, with Galois group cyclic of order dividing $n$. Conversely,

(7.1) Prop: $\mu_n \subset K^\times$ and $L/K$ is cyclic of degree $n$. Then $\exists \alpha \in K$ s.t $L = K(\sqrt[n]{\alpha})$.

Pf/ Suppose that $Gal(L/K) = \langle \sigma \rangle$. $L$ is a $K$-vectorspace of dimension $n$ and $\sigma : L \to L$ is a $K$-linear transformation. Write it as $T_\sigma$.

↓

(cont)

The char. polynomial of $T_\sigma$ is $X^n-1$, and it is also its minimal polynomial. (why?)

Thus $T_\sigma$ has $\xi_n$ (primitive $n$th root of $1$) as eigenvalue, with eigenvector $v \in L$. So $\sigma.v = \xi_n v$.

~~see next.~~ all roots of $X^n-1$ are distinct!

Note that $v^n \in K^\times$ because $\sigma(v^n) = (\sigma v)^n = (\xi_n v)^n = v^n$.

So $\sigma$ fixes $v^n \Rightarrow v^n \in K$. Let $\alpha := v^n$.

Then $K \subset K(\sqrt[n]{\alpha}) \subset L$, and we just checked that $(K(\sqrt[n]{\alpha}) : K) = n \Rightarrow$ V.

Proof (of $X^n-1$ is the minimal polynomial of $T_\sigma$:) don't need that!

$E := \{$eigenvalues of $T_\sigma\}$ form a group, since $L$ is a field.

Namely, ~~as L is a field,~~ $\left.\begin{array}{l} T_\sigma v = \xi v \\ T_\sigma v' = \xi' v' \end{array}\right\} \Rightarrow T_\sigma(vv') = (\xi\xi')(vv')$.

Thus $E$ is a finite cyclic group, and $\#E = n$ (if $\#E < n$, get a contradiction).

b) $K(\sqrt[n]{\alpha}) = K(\sqrt[n]{\beta})$, $\alpha, \beta \in K^\times \Leftrightarrow \beta = \alpha^r \gamma^n$, $\gamma \in K^\times$ and $(r,n)=1$

More generally, suppose that $L/K$ is Galois, abelian ~~and~~ the exponent of $Gal(L/K)$ divides $n$. Then $\exists\, \alpha_1, \dots, \alpha_t \in K^\times$ such that $L = K(\sqrt[n]{\alpha_1}, \dots, \sqrt[n]{\alpha_t})$.

Take a subgroup $D$ of $K^\times$, $K^\times \supset D \supset K^{\times n}$, with $D/_{K^{\times n}}$ finite.

Define $K_D := K(\sqrt[n]{D})$. Then $K_D/K$ is abelian of exponent dividing $n$.

Kummer Pairing: $D/_{K^{\times n}} \times Gal(K_D/K) \xrightarrow{B} \mu_n$

$$(\alpha \bmod K^{\times n}, \sigma) \longmapsto \sigma(\sqrt[n]{\alpha}) / \sqrt[n]{\alpha}$$

$B$ is bilinear. Also, $\left\{\begin{array}{l} B(\bar\alpha, \sigma) = 1\ \forall \bar\alpha \Rightarrow \sigma = 1 \\ B(\bar\alpha, \sigma) = 1\ \forall \sigma \Rightarrow \alpha \in K^{\times n} \end{array}\right.$ $(\bar\alpha := \alpha \bmod K^{\times n})$.

perfect pairing.

From the Kummer pairing, we get the duality:

$$D/K^{\times n} \cong \mathrm{Hom}\left(\mathrm{Gal}(K_D/K), \mu_n\right).$$

From this, $(D : K^{\times n}) = [K_D : K]$ (7.2).

Now, let $K$ be a number field.

(7.3) Prop. Assume $\mu_n \subset K$.

a) $\alpha \in \mathcal{O}_K$. Then $\mathfrak{p} \subset K$ is unramified in $K(\sqrt[n]{\alpha})/K$ if $\mathfrak{p} \nmid n\alpha$ (converse may not be true).

Pf $\mathcal{O}_K \supset \mathbb{Z}[\beta]$, $\beta^n = \alpha$

Let $f(x) = x^n - \alpha$. $f'(x) = nx^{n-1} \Rightarrow f'(\beta) = n\beta^{n-1}$.

Let $L := K(\sqrt[n]{\alpha})$. Know that $N_{L/K}(f'(\beta)) = \mathrm{disc}_K$ of $\mathbb{Z}[\beta]$, which is divisible by $\mathrm{disc}(L/K)$.

So if $\mathfrak{p} \nmid n\alpha$, $\mathfrak{p}$ is unramified. //

b) $\mathfrak{p}$ splits completely in $K(\sqrt[n]{\alpha})/K \Leftrightarrow \alpha \in (K_v^\times)^n$, where $K_v$ is the completion of $K$ at $\mathfrak{p}$.

Pf At $\mathfrak{p}$, we have $efg = (L:K)$. we want $ef = 1$. But $ef$ = local degree of $(K_v(\sqrt[n]{\alpha}) : K_v)$ //

Proof of the main theorem.

Let $K$ be a number field, $C_K = J_K/K^\times$. Let $H \subseteq C_K$ an open subgroup. We want to see that $H$ is norm, i.e. $\exists$ finite abelian ext $L/K$ s.t.

$$H = N_{L/K} C_L \quad (= \ker(\omega_{L/K} : C_K \to \mathrm{Gal}(L/K)))$$

we must construct many abelian extensions. We will use Kummer theory.

(7.4) Lemma:

a) Suppose $C_K \supset H \supset H_1$ where $H_1, H$ are subgroups, and $H_1$ is normic.
Then $H$ is normic.

b) Suppose given $H \subseteq C_K$ open subgroup, and $L/K$ a cyclic extension.
Define $H_L := N_{L/K}^{-1}(H) \subseteq C_L$.
Then if $H_L$ is normic, then $H$ is normic.

Proof

a) Suppose the abelian ext. $L_1/K$ belongs to $H_1$.

$$\begin{tikzcd}
H/H_1 \arrow[r, "\cong", "\omega_{L_1/K}"'] \arrow[d, hook] & Gal(L_1/L) \arrow[d, hook] \\
C_K/H_1 \arrow[r, "\cong", "\omega_{L_1/K}"'] & Gal(L_1/K)
\end{tikzcd}$$

Let $L \subseteq L_1$ be the fixed field of $\omega_{L_1/K}(H)$.

Taking projection + restriction ~~on co~~ we get

$$\begin{tikzcd}
H/H_1 \arrow[r, "\cong"] \arrow[d, hook] & Gal(L_1/L) \arrow[d, hook] \\
C_K/H_1 \arrow[r, "\cong"] \arrow[d, "proj."'] & Gal(L_1/K) \arrow[d, "res"] \\
C_K/H \arrow[r, "\cong", "\omega_{L/K}"'] & Gal(L/K)
\end{tikzcd}$$

$\omega_{L/K}$ by consistency (A2). ✓.

b) Suppose now that $M/L$ belongs to $H_L$. Idea: if we can show that $M/K$ is Galois and abelian, then $M/K$ belongs to $N_{M/K}C_M = N_{L/K}(\underbrace{N_{M/L}C_M}_{H_L}) =$
$= N_{L/K}(H_L) \subseteq H$. Hence $H$ contains a normic sgp $\overset{(a)}{\Rightarrow}$ ✓.

↓

(finishes proof of lemma)

So we just need to show $M/K$ is Galois and $M/k$ abelian.

$M/L$ belongs to $H_L \subseteq C_L$. Let $\tau$ be an isomorphism of $M$.

Then $\tau M/\tau L$ belongs to $\tau H_L \subseteq C_{\tau L}$ (Pf: use A1, $b \in C_L$. Then

$\omega(\tau b, \tau M/\tau L) = \tau \omega(b, M/L)\tau^{-1}$, so $\tau(\operatorname{Ker} \omega_{M/L}) (= \tau(H_L)) = \operatorname{Ker} \omega_{\tau M/\tau L}$)

Note that $\tau L = L$ since $L/K$ is Galois (cyclic!)

Recall that $H_L = N_{L/k}^{-1}(H)$. But $N_{L/k}(b) = N_{L/k}(\tau b) \leftarrow$ if $\tau$ fixes $k$.

So $\tau H_L = H_L$ $\forall \tau$ a $k$-isom.

Thus $M/L$ and $\tau M/L$ belong ~~to~~ the same group $H_L$, therefore $M = \tau M \Rightarrow M/k$ normal!

To show that $M/K$ is abelian:

$$\begin{tikzcd}
M \arrow[d, dash, "\text{abelian}"] \\
L \arrow[d, dash, "\text{cyclic}"] \\
k
\end{tikzcd}
\qquad
\begin{tikzcd}
 & & \operatorname{Gal}(M/k) \arrow[d] & \operatorname{Gal}(L/k) \text{ cyclic} \arrow[d, dash] & \\
1 \arrow[r] & A \arrow[r] & E \arrow[r] & G \arrow[r] & 1 \\
 & \operatorname{Gal}(M/L) \arrow[u] & & &
\end{tikzcd}$$

Then $E$ is abelian if $A \subseteq$ center of $E$ (elementary gp theory).

As $\omega_{M/L} : C_L \to A$ is onto, it suffices to prove that

$$\omega(\tau b, M/L) = \tau^{-1}\omega(b, M/L)\tau \overset{?}{=} \omega(b, M/L). \quad \forall \tau \in E.$$

So we want that $\omega\left(\frac{\tau b}{b}, M/L\right) = 1$, i.e. $\frac{\tau b}{b} \in \operatorname{Ker} \omega_{M/L} = H_L = N_{L/k}^{-1}(H)$

So want that $N_{L/k}\left(\frac{\tau b}{b}\right) \in H$ But $N_{L/k}\left(\frac{\tau b}{b}\right) = 1 \in H$, so this is trivial! //

This lemma allows us to increase the base field by a cyclic extension. Doing iteratively, we can increase it by any abelian extension.

- Application of 7.4:

Given an open subgroup $H \leq C_K$ s.t $C_K/H$ has exponent $n$.

Let $L = K(\zeta_n)$, $\zeta_n$ a primitive $n$th root of 1

Choose fields $K = L_0 < L_1 \subset \dots \subset L_t = L$ s.t. $L_i/L_{i-1}$ is cyclic.

Define $H_0 = H$; $H_i := N^{-1}_{L_i/K}(H) \subseteq C_{L_i}$. Apply (7.4) to the cyclic ext $L_i/L_{i-1}$

to conclude that, if $H_t$ is normic, then $H$ is also normic.

Hence it suffices to prove the existence theorem for open subgroups $H \subseteq C_K$, where $\mu_n \subseteq K$ (where $n$ = exponent of $C_K/H$).

(7.5) Lemma: (Lang, pg 47) Suppose $\mu_n \subseteq K_v^\times$. Then $(K_v^\times : K_v^{\times n}) = \frac{n^2}{\|n\|_v}$ where $\|\pi\|_v = \frac{1}{(\mathcal{O}:\mathfrak{P})}$

$\uparrow$ (and $\|\cdot\|_{\mathbb{R}}$ = usual, $\|a+ib\|_{\mathbb{C}} = a^2+b^2$).

Pf //

(7.6) Theorem: Assume $\mu_n \subseteq K$. Let $S$ be a finite set of primes containing $S_\infty$ and the divisors of $n$, and $S$ such that $J_K = K^\times J_S$ $\left(J_S = \prod_{v \in S} K_v^\times \times \prod_{v \notin S} \mathcal{O}_v^\times\right)$.

Let $B_S := \prod_{v \in S} K_v^{\times n} \times \prod_{v \notin S} \mathcal{O}_v^\times$, $L := K(\sqrt[n]{K_S})$

Then $L/K$ belongs to $K^\times B_S/K^\times \subseteq C_K$,

and $[L:K] = n^{\#S}$ and $K^\times \cap B_S = K_S^n$.

Rk: The existence thm follows from (7.6):

(7.7) Existence Thm(Pf) Given $H \subseteq C_K$ (of exponent $n$ for $C_K/H$), and $H$ open sgp in $J_K$.

Then $\exists$ finite $S$ s.t. $H \supseteq \mathcal{O}_v^\times$, $v \notin S$. Enlarge $S$ if necessary to get the hypothesis of (7.6); so $H \supseteq K^\times B_S \Rightarrow \checkmark$

//

We are now reduced to proving (7-6).

Pf (Show that $L/K$ belongs to $K^\times B_S/K^\times \subseteq C_K$, and $[L:K]=n^{\#S}$, $K^\times \cap B_S = K_S^n$)

Step 1: Let $s := \#S$

There exists an integer $d \geq 1$ s.t. $K_S \simeq \mu_{nd} \times \mathbb{Z}^{s-1}$ (Unit Theorem).

Then ~~B~~ $K_S^n \simeq \mu_d \times (n\mathbb{Z})^{s-1}$, and $K_S/K_S^n \simeq (\mathbb{Z}/n\mathbb{Z})^{s} \leftarrow$.

Let $D := K_S K^{\times n}$ $\quad (K^\times \supset D \supset K^{\times n})$.

Note that
$$D/K^{\times n} = \frac{K^{\times n} K_S}{K^{\times n}} \simeq \frac{K_S}{K_S \cap K^{\times n}} = \frac{K_S}{K_S^{\,n}}.$$

As $L = K(\sqrt[n]{D})$, by Kummer theory (7.2). $[L:K] = (D : K^{\times n}) = n^s$.

Recall that
$$B := B_S = \prod_{v \in S} K_v^{\times n} \times \prod_{v \notin S} \mathcal{O}_v^\times.$$

Step 2: Show that $K^\times B = K^\times N_{L/K} J_L$:

- Claim: $J_K \supset K^\times N_{L/K} J_L \underline{\supseteq} K^\times B$.

We prove it by looking at each component $v$.

$K_v^{\times n} \subseteq K^\times N_{L/K} J_L = \ker \omega_{L/K}$ because $\mathrm{Gal}(L/K)$ has exponent $n$.

So $\omega(n^{\text{th}} \text{ power}) = 1$ ✓. (for $v \in S$)

Now if $v \notin S$, then $v$ is unramified in $L/K$ (by Kummer theory, only divisors of ~~primes~~ $n$ and divisors of the $S$-unit, but an $S$-unit is unit outside $S$!).

In the unramified case, $\mathcal{O}_v^\times$ are local norms, thus $K^\times N J_L \supset K^\times B$ //

- Compute indices: as we know that $[L:K] = \# J_K / K^\times N J_L$, it suffices to prove that $\# J_K/K^\times B = n^s$ also. $\overset{n}{n^s}$

$$\# \frac{J_K}{K^\times B} = \# \left( \frac{K^\times J_S}{K^\times B} \right).$$

$\wr$

We use the elementary lemma:

Lemma: $X, Y, Z$ subgroups of an abelian group, $Y \supseteq Z$. Then we have an exact sequence:

$$0 \to \frac{Y\cap X}{Z \cap X} \to \frac{Y}{Z} \to \frac{XY}{XZ} \to 0$$

Pf: Use the modular law: $Y \cap (XZ) = (Y \cap X)\cdot Z$ $(\because Y \supseteq Z)$ //.

In our case:

$$1 \to \frac{J_S \cap K^\times}{B \cap K^\times} \to \frac{J_S}{B} \to \frac{K^\times J_S}{K^\times B} \to 1$$

Now, $\# \frac{J_S}{B} = \prod_{v\in S} [K_v^\times : K_v^{\times n}] \underset{\uparrow\ \text{Lang pg 47}}{=} \prod_{v\in S} \frac{n^2}{\|n\|_v} = n^{2s} \cdot \boxed{\prod_{v\in S} \frac{1}{\|n\|_v}} = n^{2s}.$

$\overset{\text{S has all divisors of } n.}{\downarrow}$ $\prod_{v\in S} = \prod_{\text{all } v}$ $\to$ $1 =$

It remains to show that $\# \frac{J_S \cap K^\times}{B \cap K^\times} = n^s$. (so that the quotient $\frac{n^{2s}}{n^s} = n^s$).

Note that $J_S \cap K^\times = K_S$. We want to show that $B \cap K^\times = K_S^n$.

$B \cap K^\times \supseteq K_S^n$ is trivial. So we need to show $B \cap K^\times \subseteq K_S^n$.

Let $\alpha \in B \cap K^\times$. As $\alpha \in K_S$, we just need that $\alpha \in K^{\times n}$.

We will show that $E := K(\sqrt[n]{\alpha}) = K$, by looking at norms.

Namely, we'll show that $K^\times N_{E/K} J_E = J_K$. (See that $N_{E/K} J_E \supset J_S$, and by multiplying by $K^\times$, done!)

If $v \notin S$, then $E_w/K_v$ is unramified. So $N_{E/K} J_E \supseteq \prod_{v\notin S} \mathcal{O}_v^\times$

If $v \in S$, then $\alpha \in B \Rightarrow \alpha \in K_v^{\times n} \Rightarrow K_v(\sqrt[n]{\alpha}) = K_v$, hence $\alpha$ is a local norm.

So $N_{E/K} J_E \supseteq \prod_{v\in S} K_v^{\times *}$. $\therefore N_{E/K} J_E \supseteq J_S$.

As by hypothesis, $K^\times J_S = J_K$, we get the result.

## The Hilbert Class Field. (Lang chap. XI, §3-5). ← will see in next page.

$C_K = J_K/K^\times$

$v$ a prime of $K$.

Have an injection $K_v^\times \xrightarrow{i_v} J_K$ $\quad$ $v$th position

$a_v \longmapsto (1,1,\ldots,1,a_v,1,1,\ldots)$

Note that still $K_v^\times \hookrightarrow J_K/K^\times$

Given an abelian extension $L/K$, belonging to $H \subseteq C_K$.

(means that $H = N_{L/K}(C_L)$, open subgroup).

(7.8) Theorem: $L/K$ abelian, belonging to $H$; $v$ a prime of $K$.

Then $v$ splits completely in $L/K \iff K_v^\times \subset H$.

## Local Class Field Theory

$L/K$ abelian. Fix $v$ a prime of $K$, $w \mid v$ a prime of $L$ above $v$.

So have $L_w/K_v$ (normal extension, $\mathrm{Gal}(L_w/K_v) \cong D_v$) ← decomposition subgroup of $w$ (depends only on $v$)

$$\begin{tikzcd}
J_K \arrow[r, two heads, "\omega_{L/K}"] & \mathrm{Gal}(L/K) \\
K_v^\times \arrow[u, hook, "i_v"] \arrow[r, dashed, "\omega_v"'] & D_v \arrow[u, hook]
\end{tikzcd}$$

Define $\omega_v := \omega_{L/K} \circ i_v$

(7.9) $\omega_v(K_v^\times) \subseteq D_v$. So get $\omega_v : K_v^\times \longrightarrow D_v$ making the diagram to commute.

Moreover, $\ker \omega_v = N_{L_w/K_v}(L_w^\times)$ and $\omega_v$ is onto $D_v$.

(so $K_v^\times / N(L_w^\times) \underset{\omega_v}{\cong} D_v = \mathrm{Gal}(L_w/K_v)$).

Also, $\mathcal{O}_v^\times / N(\mathcal{O}_w^\times) \cong I_v$ (= inertia subgroup).

(7.10) (Local existence theorem): ~~the extension~~ Given $K_v/\mathbb{Q}_p$, the finite abelian extensions of $K_v$ correspond 1-1 to open subgroups of finite index of $K_v^\times$ (see Lang, 2nd edition).

(7.11) $L/K$ abelian, belonging to $H$. Then:

A prime $v$ of $K$ is unramified in $L \Leftrightarrow \mathcal{O}_v^\times \subseteq H$

($\sim$ converse of "every local unit is a norm in an unramified extension")

Hilbert Class Field, $\hat{K}$ (of $K$).

$\hat{K}$ is the maximal abelian extension of $K$ that is unramified at all primes of $K$.

Q: To which subgroup $H$ does $\hat{K}$ belong?

By (7.11), $\forall v$, $H \supset \mathcal{O}_v^\times$ (in particular, if $v$ is infinite prime, then $H \supseteq \mathcal{O}_v^\times = K_v^\times$).

So $\hat{K}^\times$ belongs to $K^\times J_{S_\infty}/K^\times$, $\quad J_{S_\infty} = \prod_{v \in S_\infty} K_v^\times \times \prod_{v \notin S_\infty} \mathcal{O}_v^\times$

Thus, via the Artin map,

$$\boxed{J_K \big/ K^\times J_{S_\infty} \cong Gal(\hat{K}/K)}$$

Note also that, via the ideal map, $J_K \big/ K^\times J_{S_\infty} \simeq Cl(K)$.

So $$\boxed{\begin{matrix} Gal(\hat{K}/K) \simeq Cl(K) \\ (\mathfrak{p}, \hat{K}/K) \longleftrightarrow [\mathfrak{p}] \end{matrix}}$$

Consequence: A prime $\mathfrak{p}$ (of $K$) splits completely in $\hat{K} \Leftrightarrow$

$\Leftrightarrow [\mathfrak{p}, \hat{K}/K) = 1 \Leftrightarrow \mathfrak{p}$ is principal

Example: $K = \mathbb{Q}(\sqrt{10})$, $h_K = 2$.

We look for an unramified extension of $K$ (real primes remain real).

$$\begin{tikzcd}
 & L = \mathbb{Q}(\sqrt{10}, \sqrt{5}) \arrow[dl, dash] \arrow[d, dash, "K" near end] \arrow[dr, dash] & \\
\mathbb{Q}(\sqrt{2}) \arrow[dr, dash, "e_5=1"'] & \mathbb{Q}(\sqrt{10}) \arrow[d, dash, "e_5=2"'] & \mathbb{Q}(\sqrt{5}) \arrow[dl, dash] \\
 & \mathbb{Q} &
\end{tikzcd}$$

$\Rightarrow e_5(L/K) = 1$ and only divisors of $5$ could ramify in $L/K \Rightarrow L = \hat{K}$.

Class Tower Problem.

Let $K^{(1)} := \hat{K} = HCF$ of $K$.

For $i \geq 1$, let $K^{(i+1)} := H.C.F.$ of $K^{(i)}$.

Q: Does there exist $i$ st $K^{(i+1)} = K^{(i)}$ ? ($K$ fixed).

A: Not in general (1964, Golod + Shafarevic). (using gp theory)

One can look also at $K^{(i)}(p)$ ($p$-class field) = maximal abelian unramified $p$-extension of $K^{(i)}(p)$. Can consider the $p$-class-field-tower

Actually, Golod + Shafarevich showed that the $p$-class field tower can be infinite.

For example, $p = 2$, $K$ imaginary quadratic, $\infty$ 2-tower:

$$K := \mathbb{Q}\left(\sqrt{-2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13}\right)$$

If we want $K$ to be real quadratic, can take $K := \mathbb{Q}\left(\sqrt{2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19}\right)$.

(see P. Roquette in Cassels-Frohlich).

If $G$ is a finite $p$-group, $G$ has a lot of relations, if $d(G) = \#$ generators
$r(G) = \#$ relations

Golod + Shafarevich showed that $r(G) > \frac{d(G)^2}{4}$ if $G$ is finite.

Thus if the inequality fails, $G$ cannot be finite!

So Shafarevich + Golod just proved that inequality. $\left(G = \mathrm{Gal}\left(K^{(\infty)}/K\right)\right)$.

E.O.C