The principal ideal theorem

Schedule adjustment: no lecture or office hours on Friday, January 15. Instead, that day's lecture will be given (and recorded) Thursday, January 14 at 4pm, and followed by 30 minutes of office hours.

Additional reminder: no lecture or office hours on Monday, January 18 (university holiday).

Statement of the theorem, and an example

Thm (Furtwängler) (Principal ideal theorem)
(Capitulation theorem)

Let K be a # field. Let L be the Hilbert class field of K.
Then every fractional ideal of K extends to a principal fractional ideal of L; that is, the map

$$Cl(K) \longrightarrow Cl(L)$$
$$[\mathfrak{a}] \to [\mathfrak{a}\mathcal{O}_L]$$

is zero. $\mathfrak{p}=(2, 1+\sqrt{-5})$

$Cl(K) \cong \mathbb{Z}/2\mathbb{Z}$
$=\{1 \cup [\mathfrak{p}]\}$

Example $K=\mathbb{Q}(\sqrt{-5})$
$L=\mathbb{Q}(\sqrt{-5}, \sqrt{-1})$ $\mathfrak{p}\mathcal{O}_L=(1+\sqrt{-1})$.

The role of Artin reciprocity

$M/L/K$ $\quad L = $ HCF of K, $M = $ HCF of L

M is Galois over K but not abelian unless $M = L$.

$\Leftrightarrow |Cl(L)| = 1$

By Artin reciprocity

$$\begin{tikzcd} Cl(K) \arrow[r, "\sim"] \arrow[d] & Gal(L/K) \arrow[d, dashed, "?"] \\ Cl(L) \arrow[r, "\sim"] & Gal(M/L) \end{tikzcd}$$

Q What is the dashed arrow? Can I characterize it in a purely group-theoretic way?

More group theory of the situation

$M/L/K$

Galois M/L

$$\begin{tikzcd}
Cl(K) \arrow[r] \arrow[d] & Gal(L/K) \cong \overbrace{Gal(M/K)}^{G}{}^{ab} \arrow[d] \\
Cl(L) \arrow[r] & \overbrace{Gal(M/L)}^{=H} \cong Gal(M/L)^{ab}
\end{tikzcd}$$

H normal subgroup of G

i.e. Working w/ a map $G^{ab} \to H^{ab}$

A candidate map: the transfer

$H \leq G$ finite groups

Let $g_1, \ldots, g_n$ be left coset reps of H in G

so $G = g_1 H \sqcup \cdots \sqcup g_n H$. For $g \in G$,

write $\phi(g) = g_i$ where $g \in g_i H$ & then

$$V(g) = \prod_{i=1}^{n} \underbrace{\phi(g g_i)^{-1} g g_i}_{\in H} \quad ; \quad V : G \to H$$

A candidate map: the transfer

$$V(g) = \prod_{i=1}^{n} \phi(gg_i)^{-1} gg_i$$

<u>Thm</u> - The map $V : G \to H$, induces a <u>homomorphism</u>

$V : G \to H^{ab} = H/[H,H]$

- it does not depend on choice of g_i's

— this map factors through

$\to V : G^{ab} \to H^{ab}$ (Verlagerung)

the transfer homomorphism

The transfer in the number field setting

$$\begin{array}{ccc} Cl(K) & \xrightarrow{\sim} & \mathrm{Gal}(L/K) = \mathrm{Gal}(M/K)^{ab} \\ \downarrow \ \mathfrak{p} \mapsto \mathfrak{q}_1 \cdots \mathfrak{q}_r & & \downarrow \ \checkmark \\ Cl(L) & \xrightarrow{\sim} & \mathrm{Gal}(M/L) = \mathrm{Gal}(M/L)^{ab} \end{array}$$

$$\begin{array}{c} M \\ | \\ L \\ | \\ K \end{array}$$

<u>Lemma</u> The dashed arrow is $V: G^{ab} \to H^{ab}$ for $H = \mathrm{Gal}(M/L) \subseteq \mathrm{Gal}(M/K)$

<u>Pf</u> reduces to a single prime $\mathfrak{p}$ of K.
Let $\mathfrak{q}_1, \ldots, \mathfrak{q}_r$ be primes of L above $\mathfrak{p}$, i.e. $\mathfrak{p}\mathcal{O}_L = \mathfrak{q}_1 \cdots \mathfrak{q}_r$. Pick a prime $\underline{\mathfrak{r}_i}$ of M above $\mathfrak{q}_i$; let $G_{\mathfrak{r}} \subseteq G$ decomp grps; decompose $G = \bigsqcup_i G_{\mathfrak{r}} \tau_i H$.

The transfer in the number field setting

Correspondence of q_i to double cosets $G_{\underline{r}}\tau_i H$

$$\underline{r}^{\tau_i} \cap L \longleftarrow\!\shortmid \; G_{\underline{r}}\tau_i H$$

$$G_{\underline{r}}\tau_i H = \bigsqcup_{j=0}^{m-1} \underbrace{\mathrm{Frob}^j \tau_i H}_{g_{ij}}.$$ Gives coset reps for H in G,

use these to compute V.

Lemma $\mathrm{Frob}_{M/L}(q_i) = \prod_{j=0}^{m-1} \phi(g g_{ij})^{-1} g g_{ij}$

for $q_i = \underline{r}^{\tau_i} \cap L$ where $g = \mathrm{Frob}_{M/K}(\underline{r})$.

$\Longrightarrow$ V completes the diagram.

A theorem of pure group theory

$G = \mathrm{Gal}(M/K)$
$H = \mathrm{Gal}(M/L)$

Thm Let G be a finite group. Let H be its commutator subgroup, so $G/H \cong G^{ab}$.

Then $V : G^{ab} \longrightarrow H^{ab}$ is zero.

Pf pure group theory.

Et cetera

K = \# field.

The <u>class field tower</u> of K is the sequence

$K = K_0 \subseteq K_1 \subseteq K_2 \cdots$

where K_{n+1} is HCF of K_n. These are all Galois extensions of K, & everywhere unramified.

<u>Thm</u> (Golod-Shafarevich) $\exists$ examples where $K_n \neq K_{n+1}$ $\forall n$, i.e. towers infinite.

(e.g. $K = \mathbb{Q}(\sqrt{-D})$, $D > 0$, with at least six ramified primes.)

Analogous construction for function fields (finite extensions of $\mathbb{F}_p(t)$) can be used to find curves over $\mathbb{F}_q$ of large genus g, where

$$\liminf_{g \to \infty} \frac{\#\text{rational points}}{g} > 0$$

(Serre etc.)

relevant for algebraic coding theory