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**

**Theorem (Furtwängler)** (Principal Ideal Theorem) (Cotitation theorem)

Let $K$ be a field. Let $L$ be the Hilbert class field of $K$. Then any fractional ideal of $K$ extends to a principal fractional ideal of $L$. That is, the map $\text{Cl}(K) \rightarrow \text{Cl}(L)$ is zero.

**Example**

$K = \mathbb{Q}(\sqrt{-5})$  
$L = \mathbb{Q}(\sqrt{-5}, \sqrt{-1})$  
$\mathcal{O}_L = (1 + \sqrt{-5})$.
The role of Artin reciprocity

\[ \mathcal{O}_K = \mathcal{O}_L \text{ for } K \leq M \leq L \]

By Artin reciprocity,

\[ \mathcal{O}_K \rightarrow \mathcal{O}_L, \quad \mathcal{O}_M \rightarrow \mathcal{O}_L \]

What is the dashed arrow? Can I characterize it in a more graphical way?
More group theory of the situation

\[ C \]

\[ C \subseteq \text{Gal}(L/K) \]

\[ \text{Gal}(L/K) \]

\[ \text{Gal}(M/K) \]

\[ C \]

\[ \text{Gal}(M/L) \]

\[ C \]

\[ \text{Gal}(M/L) \]

\[ C \]

\[ \text{Gal}(M/L) \]

\[ C \]

\[ \text{Gal}(M/L) \]

\[ C \]

\[ \text{Gal}(M/L) \]

\[ C \]

\[ \text{Gal}(M/L) \]

\[ C \]

\[ \text{Gal}(M/L) \]

\[ C \]

\[ \text{Gal}(M/L) \]

\[ C \]

\[ \text{Gal}(M/L) \]

\[ C \]

\[ \text{Gal}(M/L) \]

\[ C \]

\[ \text{Gal}(M/L) \]

\[ C \]

\[ \text{Gal}(M/L) \]

\[ C \]

\[ \text{Gal}(M/L) \]

\[ C \]

\[ \text{Gal}(M/L) \]

\[ C \]

\[ \text{Gal}(M/L) \]

\[ C \]

\[ \text{Gal}(M/L) \]

\[ C \]

\[ \text{Gal}(M/L) \]

\[ C \]

\[ \text{Gal}(M/L) \]

\[ C \]

\[ \text{Gal}(M/L) \]

\[ C \]

\[ \text{Gal}(M/L) \]

\[ C \]

\[ \text{Gal}(M/L) \]

\[ C \]

\[ \text{Gal}(M/L) \]

\[ C \]

\[ \text{Gal}(M/L) \]

\[ C \]

\[ \text{Gal}(M/L) \]

\[ C \]

\[ \text{Gal}(M/L) \]

\[ C \]

\[ \text{Gal}(M/L) \]

\[ C \]

\[ \text{Gal}(M/L) \]

\[ C \]

\[ \text{Gal}(M/L) \]

\[ C \]

\[ \text{Gal}(M/L) \]

\[ C \]

\[ \text{Gal}(M/L) \]

\[ C \]

\[ \text{Gal}(M/L) \]

\[ C \]

\[ \text{Gal}(M/L) \]

\[ C \]

\[ \text{Gal}(M/L) \]

\[ C \]

\[ \text{Gal}(M/L) \]
A candidate map: the transfer

\[ \mathcal{H} \leq G \Rightarrow \mathcal{H} \leq \mathcal{H} \]

let \( s, \ldots, s_n \) be left coset reps of \( H \leq G \)

so \( G = g_iH \cup \ldots \cup g_nH \) for \( g_i \notin H \),

write \( \phi(g) = g_i \) where \( g \in g_iH \) for \( H \)

\[ V(g) = \prod_{i=1}^{n} \phi(g) \bigg|_{g \in H} \]

\( \phi(g) \) : \( V : G \to \mathcal{H} \)
A candidate map: the transfer

\[ V(g) = \prod_{i=1}^{n} \phi^{-1}(g g_i) g g_i \]

The map \( V: G \rightarrow H \) induces a homomorphism \( V: G \rightarrow \prod_{i=1}^{n} H = H / (N, H) \).

- It does not depend on choice of \( g_i \).

- This map maps through \( \text{transfer homomorphism} \).

\( V: G \to H \) \( \rightarrow H_{ab} \) (Verlag ers)
The transfer in the number field setting

\[
\text{Cl}(K) \cong \text{Cl}(L/K) = \text{Cl}(M/K) \quad \checkmark
\]

\[
\text{Cl}(L) \cong \text{Cl}(M/L) = \text{Cl}(M/K) \quad \checkmark
\]

The dashed move \( \leq 15 \text{V} \): \( C \rightarrow \mathbb{C} \)

\( y = M \triangleq \text{Cl}(M/L) \triangleq \text{Cl}(M/K) \)

If \( \mathbb{F} \) runs on a single prime \( \mathfrak{p} \) of \( K \)

let \( \sigma, \tau, \ldots, \) be parts at \( L \) above \( \mathfrak{p} \) in \( \mathbb{F} \)

\( \mathfrak{p} \mathbb{F} = \mathfrak{p} \mathbb{F} \lhd \). Pick a prime \( \mathfrak{p} \) of \( M \) above \( \mathfrak{p} \),

\( \sigma + \mathfrak{p} \mathbb{F} \subset C \) algebraic; denote \( \sigma = \bigcup \mathfrak{p} \mathbb{F} \triangleleft H \).
The transfer in the number field setting

Let \( \mathcal{O} \) be a discrete valuation ring and \( G \) a connected reductive group over \( \mathbb{C} \).

Let \( G = L \times H \) with \( L \) a split torus and \( H \) a split reductive group.

Given a set of \( \Gamma \) in \( L \), we have to compute \( \mathbf{V} \).

Lemma: \( \text{Fr}_L^{\mathbb{Q}_L}(\mathbf{g}) = \prod_{(i,j)} \phi_{L_{ij}}(\mathbf{g}_{ij}) \)

where \( \mathbf{g} = \text{Fr}_L(\mathbf{g}) \)

\( \mathbf{V} \) completes the diagram.
A theorem of pure group theory

Let $G = \text{Aut}(M/K)$ and $H = \text{Aut}(L/L)$. Let $a, b, c \in G$ be such that $a b \in H$. Let $H$ be a normal subgroup of $G$. Then $G / H \cong G / a b$. Thus $G / H$ is a group.

Let $G = C^6$ and $H = C_6$. Then $G / H$ is a group.
Et cetera

\[ K = \mathcal{H} \text{ field} \]

The class field tower of \( K \) is the sequence

\[ K = K_0 \subseteq K_1 \subseteq K_2 \subseteq \ldots \]

where \( K_n \) is HCF of \( K_n \). These are all Galois extensions of \( K \).

Everywhere unramified.

Then (Goldfeld-Schatarevich) examples where

\[ K_n + K_{n+1} \text{ for } n \text{ even} \]

(\( K = \mathbb{Q}(\sqrt{d}) \) with \( d \) a prime or \( d \) a product of at least six distinct primes.)
Analogous construction for the linear fields (finite extensions of $\mathbb{F}_q(t)$) can be used to find curves over $\mathbb{F}_q$ of low genus, where

\[
\text{Immerse rational points} > 0 \quad (\text{some})
\]

relevant for algebraic coding theory.