The Hilbert class field

HW 9 to be posted later today, due next Thursday. (The numbering is continued from 204A.)

For those new to 204B, there is a CoCalc project associated to this course. For access to it, see the thread "Announcements/CoCalc" on Zulip. (If you don't know what CoCalc is, watch Thomas Grubb's video from 204A.)

The corresponding section of the CFT notes (2.1) is short enough that I don't expect to spend the full lecture time on it. I will fill in the rest of the time with more details from Chapter 1 (Kummer theory and local Kronecker-Webber); see also the last two lectures of 204A, and also HW 9.
An unramified extension of a number field

\[ K = \mathbb{Q}(\sqrt{-5}) \]
\[ 2 \mathfrak{O}_K = \mathfrak{p}^2 \]
\[ \mathfrak{O}_K(\sqrt{-5}) = \mathfrak{p} \]
\[ \mathfrak{O}_K(\sqrt{-1}, \sqrt{-5}) = \mathfrak{p} \]
\[ C(\mathfrak{p}) = \mathbb{Z}/2\mathbb{Z} \]
\[ L/K \text{ is unramified over primes of } \mathfrak{p} \]
\[ \text{if } \mathfrak{p} \text{ is odd powers of } \mathfrak{p} \]
\[ \text{and even over } \mathfrak{p} \]
\[ L = K(\sqrt{d}) \]
\[ d = 1 + \sqrt{5} \]
\[ x^2 - x - 1 \text{ has no roots } \mathfrak{p} \text{ over } \mathfrak{O}_K \text{ and } K \]
\[ \text{has distinct roots modulo } \mathfrak{p} \]
\[ \text{i.e., } L = K(\sqrt{5}) \]
Jargon watch: "places"

A place of a number field $K$ is an equivalence class of nontrivial absolute values on $K$. Each of these is either a finite place, class of nonarchimedean values on $K$ or of $1/|p|$ for some prime $p$ at $\mathbb{Q}$; class of some extension of $\mathbb{R}$ or of $1/|p|$ on $\mathbb{Q}_p$. real abs value
Theorem-definition: the Hilbert class field

Let $L/K$ be a maximal extension of $K$ which is abelian and everywhere unramified except at infinite places (i.e., real places of $K$ extend to real places of $L$) rather than (say) $p$-places. Then $L/K$ is finite, and...

$L$ is called the Hilbert class field of $K$.

E.g., the Hilbert class field of $\mathbb{Q}(\sqrt{-5})$ is equal to $\mathbb{Q}(\sqrt{-5}, \sqrt{7})$.

E.g. Hilbert class field of $\mathbb{Q}$ is $\mathbb{Q}$.
The Galois group of the Hilbert class field

... $G_1(K_1|\mathbb{Q})$ is isomorphic to $\text{Cl}^1(K)$

(in a specific way given by Artin reciprocity)

E.g. $K = \mathbb{Q}(\sqrt{5})$, then $L = \mathbb{Q}(\sqrt{5}, \sqrt{-1})$. 
Example: genus theory for quadratic fields

Given a quadratic field $K$ over $\mathbb{Q}$, the genus of $K$ is defined as

$$\text{Genus: } \frac{1}{2} \chi_2(\mathcal{O}_K)$$

where $\chi_2$ is the 2-adic valuation of the ideal class group of $K$. The genus of $K$ is a measure of the number of equivalence classes of ideals in $\mathcal{O}_K$.

Via the generalized Dedekind–Hasse theorem, this means that $K$ has an unramified extension which is Galois with Galois group $(\mathbb{Z}/2\mathbb{Z})^{t-1}$, where $t$ is the number of real places of $K$.

This can be seen explicitly (exercise).
Unramified extensions can be nonabelian.

If \( P(x) \in \mathbb{Q}(x) \) has some degree, it must be irreducible with Galois group \( S_n \) or \( A_n \).

\[ K = \mathbb{Q}(\sqrt{D}) \text{ and } K_n = \mathbb{Q}(\sqrt{-D}) \text{ are unramified where } \mathbb{Q}(x) \rightarrow \mathbb{Q}(\sqrt{D}). \]

\[ \text{Hilbert class field of } K_n = \mathbb{Q}(\sqrt{-D}) \]

\[ K_\infty = \bigcup K_n \text{ is the class field tower of } K \]

\[ K = K_0 \]
Now, back to Kummer theory

Theorem: Let $K$ be a field containing $\mathbb{Q}_p$ (where $p$ is prime). Let $G = (\mathbb{Z}/n)^\times$ be a cyclic group of order $n$. Consider the field $L = K^{(\sqrt[n]{a})}$ where $a \in K$ such that $a^n - 1 \in K^\times$.

For any $h \in G$, define $f(h) : L \to L$ by $f(h)(x) = x^h$. This defines a homomorphism $f : G \to \text{Aut}(L)$. The kernel of $f$ is $\text{Ker}(f) = \{g \in G : f(g) = 1\} = \{g \in G : g^n = 1\}$, which is a subgroup of $G$.

For any $g \in G$, define $f(g) : L \to L$ by $f(g)(x) = x^g$ for all $x \in L$. This defines a homomorphism $f : G \to \text{Aut}(L)$. The kernel of $f$ is $\text{Ker}(f) = \{g \in G : f(g) = 1\} = \{g \in G : g^n = 1\}$, which is a subgroup of $G$.

Let $L/K$ be a cyclic extension. Let $\sigma \in \text{Gal}(L/K)$. The homomorphism $f(\sigma)$ satisfies $f(\sigma)(x) = x^\sigma$ for all $x \in L$. This defines a homomorphism $f : \text{Gal}(L/K) \to \text{Aut}(L)$.

The crossed homomorphism $f$ is given by $f(h) = h(b)/b$ for some $b \in L^\times$. Thus, $f(h) = h(b)/b$ for some $b \in L^\times$. The kernel of $f$ is $\text{Ker}(f) = \{g \in G : f(g) = 1\} = \{g \in G : g^n = 1\}$.
Kummer theory and local Kronecker-Weber

Recall that to prove local KW we need to classify $\mathbb{Q}_p$-extensions of $\mathbb{Q}_p$. $p > 2$

But to do this, first look at $(\mathbb{Q}_p, (\mathbb{Q}_p))$ $n = s_0 - 1$

$$(\mathbb{Q}_p, (\mathbb{Q}_p))^{*} = \mathbb{Z} \times \mathbb{Z}_p (\mathbb{Q}_p)^{*}$$

$$= \mathbb{Z} \times <\gamma_{p-1}> \times U_{1}$$

$x \equiv 1 \mod \pi_{p}^{n}$

$$(\mathbb{Q}_p, (\mathbb{Q}_p))^{*} = \mathbb{Z} \times <\gamma_{p-1}> \times U_{1}^{\infty}$$

$x \equiv 1 \mod \pi_{p}^{n+1}$