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-Weber); see also the last two lectures of 204A, and also HW 9.

An unramified extension of a number field

$K = \mathbb{Q}(\sqrt{-5})$ $\qquad \mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$

$2\mathcal{O}_K = \mathfrak{p}^2$ $\qquad \mathfrak{p} = (2, 1+\sqrt{-5})$ nonprincipal

$Cl(K) \cong \mathbb{Z}/2\mathbb{Z}$

$\mathbb{Q}(\sqrt{-1}, \sqrt{-5}) = L$

$$\begin{tikzcd}[column sep=small] & L \arrow[dl, dash] \arrow[dr, dash] & \\ \mathbb{Q}(\sqrt{-1}) \arrow[dr, dash] & & \mathbb{Q}(\sqrt{-5}) = K \arrow[dl, dash] \\ & \mathbb{Q} & \end{tikzcd}$$

L/K is unramified over primes of K lying over odd primes of $\mathbb{Q}$

and over $\mathfrak{p}$

$L = K(\alpha)$ $\qquad \alpha = \frac{1+\sqrt{5}}{2}$ has min poly $x^2 - x - 1$ over $\mathbb{Q}$ and K

has distinct roots mod $\mathfrak{p}$

(i.e. $L = K(\sqrt{5})$ w/ $\mathbb{Q}(\sqrt{5})/\mathbb{Q}$ doesn't ramify at 2.)

Jargon watch: "places"

A place of a number field K is an equivalence class of nontrivial absolute values on K.

nonarchimedean

Each of these is either a finite place; class of

nonzero

$|\ |_{\mathfrak{p}}$ for some prime $\mathfrak{p}$ of $\mathcal{O}_K$;

archimedean

or an infinite place; class of some extension of $|\ |_\infty$ on $\mathbb{Q}$.

real abs value

Theorem-definition: the Hilbert class field

Let L/K be maximal extension of K which is abelian and everywhere unramified even at infinite places (i.e. real places of K extend to real places of L rather than cmplx places)

Then L/K is finite, and...

L is called the Hilbert class field of K.

e.g. the Hilbert class field of $\mathbb{Q}(\sqrt{-5})$ ~~contains~~ is equal to $\mathbb{Q}(\sqrt{-5}, \sqrt{-1})$

e.g. Hilbert class field of $\mathbb{Q}$ is $\mathbb{Q}$ (Minkowski!)

The Galois group of the Hilbert class field

... $\mathrm{Gal}(L/K)$ is isomorphic to $Cl(K)$ (in a specific way given by Artin reciprocity)

ex. $K = \mathbb{Q}(\sqrt{-5})$, then $L = \mathbb{Q}(\sqrt{-5}, \sqrt{-1})$.

Example: genus theory for quadratic fields

$K/\mathbb{Q}$ imaginary quadratic. if K is real, must be more careful

Gauss: $Cl(K)/2Cl(K)$ has order 2^{t-1}

$t := \#$ finite places of $\mathbb{Q}$ that ramify in K.

Via theorem, this means that K has an unramified extension which is Galois with Galois group $(\mathbb{Z}/2\mathbb{Z})^{t-1}$

This can be seen explicitly (exercise)

Unramified extensions can be nonabelian

e.g. if $P(x) \in \mathbb{Z}[x]$ has square free discriminant D & irreducible with Galois group S_n, $n = \deg(P)$

$K = \mathbb{Q}(\sqrt{D})$. Then K has an unramified extension with Galois group A_n.

$$\begin{tikzcd}[column sep=small]
 & L \arrow[dl, dash] \arrow[dr, dash, "{A_n,\ \text{unramified}}"] & \\
\mathbb{Q}(\alpha) \arrow[dr, dash] & & \mathbb{Q}(\sqrt{D}) \arrow[dl, dash] \\
 & \mathbb{Q} &
\end{tikzcd}$$

where $P(\alpha) = 0$

<u>Class field tower</u>:

K_{n+1} = Hilbert class field of K_n

$$\begin{array}{c} \vdots \\ | \\ K_2 \\ | \\ K_1 \\ | \\ K = K_0 \end{array}$$

<u>Thm</u> (Golod–Shafarevich): $\exists$ explicit examples of K for which the class field tower is infinite.

Now, back to Kummer theory

Thm (Kummer): K field containing ζ_n (primitive n-th root of unity)

Then $\mathbb{Z}/n\mathbb{Z}$-extensions of K are of form $K(a^{1/n})$ where $a \in K^*$ represents an element of $K^*/(K^*)^n$ of order n.

Pf let L/K be an $\mathbb{Z}/n\mathbb{Z}$-extension. let $g \in Gal(L/K)$ generator.

Define $f : Gal(L/K) \to L^*$ sending g^r to ζ_n^r.

This defines an element of $H^1(Gal(L/K), L^*)$, i.e. f satisfies

$$f(hg) = h(f(g))\, f(h) \quad \forall g, h \in Gal(L/K).$$

(crossed homomorphism)

Hilbert: any crossed homomorphism has form $f(h) = h(t)/t$ for some $t \in L^*$. $\Rightarrow t = \alpha^{1/n}$ for some $\alpha \in K^*$.

Kummer theory and local Kronecker-Weber

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

To do this, first look at $\mathbb{Q}_p(\zeta_p)$ $\quad \pi = \zeta_p - 1$

$$\mathbb{Q}_p(\zeta_p)^* = \pi^{\mathbb{Z}} \times \mathbb{Z}_p[\zeta_p]^*$$

$$= \pi^{\mathbb{Z}} \times \langle \zeta_{p-1} \rangle \times U_1 \quad x \equiv 1 \bmod \pi$$

$$(\mathbb{Q}_p(\zeta_p)^*)^p = \pi^{p\mathbb{Z}} \times \langle \zeta_{p-1} \rangle \times U_1^p = U_{p+1}$$

$x \equiv 1 \bmod \pi^{p+1}$ (HW)