Generalized ideal class groups and Artin reciprocity

HW 9 has been posted, due Thursday, January 14. Again, please let me know in advance of the deadline if you need an extension.

As with Math 204A, non-UCSD students can take this course for credit via concurrent enrollment (for a fee which I do not control). Please let me know via PM on Zulip if you are planning to do this.

Land acknowledgment: UC San Diego's main campus is located near the Pacific Ocean on approximately 1,200 acres of coastal woodland in La Jolla, California. The campus sits on the ancestral homelands of the Kumeyaay Nation. Kumeyaay people continue to have an important and thriving presence in the region. [Additional note: the name "La Jolla" is of Kumeyaay origin.]

Reminder: example of a Hilbert class field

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

L/K is an everywhere unramified abelian extension

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

Thm A ~~prime~~ unramified prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ splits in L iff it is principal. (in other words, $Frob_{\mathfrak{q}}$ for $\mathfrak{q}$ above $\mathfrak{p}$ "is" class of $\mathfrak{p}$ in $Cl(K)$.)

Splitting of primes in this example

$\mathcal{O}_K = \mathbb{Z}(\sqrt{-5})$

- If $\mathfrak{p} = (p)$ where $p \neq 2, 5$ is a rational prime, which is inert in K

$\Rightarrow \left(\frac{-5}{p}\right) = -1 \Rightarrow$ either $\left(\frac{-1}{p}\right) = 1$ or $\left(\frac{5}{p}\right) = 1$

Since $L = K(\sqrt{-1}) = K(\sqrt{5})$, $\mathfrak{p}$ splits in L

- If $\mathfrak{p}$ ~~$\mathfrak{p}$~~ $= (p)$ where $p \neq 2, 5$ splits in K
  - if $\mathfrak{p} = (\beta)$, $\beta = x + y\sqrt{-5}$, $x, y \in \mathbb{Z}$ $\Rightarrow x^2 + 5y^2 = p$
    $\Rightarrow p \equiv 1 \mod 4$
    $\Rightarrow$ ~~$\mathfrak{p}$~~ splits in L
  - if $\mathfrak{p} = \alpha(2, 1+\sqrt{-5})$, Taking norms $\Rightarrow p = 2(x^2 + 5y^2)$, $x, y \in \mathbb{Q}$
    $\Rightarrow p \equiv 3 \mod 4$
    $\Rightarrow \mathfrak{p}$ does not split in L.

(etc.)

Compare this with Kronecker-Weber

$K/\mathbb{Q}$ abelian (but typically ramified)

by K-W $K \subseteq \mathbb{Q}(\zeta_n)$ for some n

primitive n-th root of 1

p prime $\Rightarrow$ splitting of (p) in $\mathbb{Q}(\zeta_n)$ is determined by p mod n.

(relates to $\mathbb{F}_p(\zeta_n) / \mathbb{F}_p$ — $\#\mathbb{F}_p(\zeta_n) = p^a$

where a is least integer s.t. $p^a \equiv 1 \bmod n$).

Generalized ideal class groups

K = # field

$\underline{m}$ = formal product of places of K

"modulus" = nonzero ideal of $\mathcal{O}_K$ × formal product of infinite places

$I_K^{\underline{m}}$ = { fractional ideals of K coprime to $\underline{m}$ }

$P_K^{\underline{m}}$ = { fractional ideals of K of form (α) with: for $\mathfrak{p}^e | \underline{m}$ finite, $\alpha \equiv 1 \bmod \mathfrak{p}^e$; for a real place τ in $\underline{m}$, $\tau(\alpha) > 0$ }

The quotient $I_K^{\underline{m}} / P_K^{\underline{m}} = Cl^{\underline{m}}(K)$ is the <u>generalized ideal class group</u> of K of modulus $\underline{m}$.

The Artin map

L/K finite abelian extension of # fields

Let $\mathfrak{p}$ be a prime of $\mathcal{O}_K$ unramified in L.

Let $\mathfrak{q}$ be a prime of L above $\mathfrak{p}$. Decomposition group

$G_{\mathfrak{q}}$ is cyclic generated by $\mathrm{Frob}_{\mathfrak{q}}$ (generator $\mathrm{Gal}\left(\frac{\mathcal{O}_L}{\mathfrak{q}} / \frac{\mathcal{O}_K}{\mathfrak{p}}\right)$

$x \to x^q$ $\quad q = \# \frac{\mathcal{O}_K}{\mathfrak{p}}$

because L/K abelian

$G_{\mathfrak{q}}$ depends only on $\mathfrak{p}$, as does $\mathrm{Frob}_{\mathfrak{q}} = \mathrm{Frob}_{\mathfrak{p}} \in \mathrm{Gal}(L/K)$

By multiplicativity, get $I_K^{\underline{m}} \longrightarrow \mathrm{Gal}(L/K)$ for some modulus $\underline{m}$

because $\mathfrak{p}$ doesn't ramify in L

e.g. $K = \mathbb{Q}$,

$\underline{m} = n\infty$ $\quad Cl^{m}(K) = (\mathbb{Z}/n\mathbb{Z})^*$

$\underline{m} = n$ $\quad Cl^{m}(K) = \frac{(\mathbb{Z}/n\mathbb{Z})^*}{\pm 1}$

Artin reciprocity

L/K finite abelian extension

Thm For some modulus $\mathfrak{m}$, this map $I_K^{\mathfrak{m}} \to \mathrm{Gal}(L/K)$ factors through $Cl_K^{\mathfrak{m}} \longrightarrow \mathrm{Gal}(L/K)$

(Artin map)

Def The conductor of L/K is the smallest $\mathfrak{m}$ for which this inclusion holds.

Ray class fields

For $\mathfrak{m}$ a modulus of K

A ray class field for $\mathfrak{m}$ is an abelian extension L/K s.t. Artin map $Cl^{\mathfrak{m}}(K) \to Gal(L/K)$ exists and is an isomorphism.

e.g. $\mathfrak{m} = 1$, this is the Hilbert class field.

$K = \mathbb{Q}$, $\mathfrak{m} = n\infty$ ray class field $\mathbb{Q}(\zeta_n)$

$K = \mathbb{Q}$, $\mathfrak{m} = n$ ray class field $\mathbb{Q}(\zeta_n)^+ = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$

Note: Artin reciprocity implies uniqueness of ray class field.

The existence theorem

Thm For $\mathfrak{m}$ a modulus of # field K, there exists a ray class field L/K of $\mathfrak{m}$.

Meanwhile Artin reciprocity $\Rightarrow$ every finite abelian extension of K is contained in some ray class field.

TO union of all abelian extensions of K = union of all ray class fields.

Inexplicitness of the existence theorem

For most K the existence theorem is

<u>not constructive</u>!

$K = \mathbb{Q}$ Kronecker-Weber (torsion of $\mathbb{G}_m$)

$K = \mathbb{Q}(\sqrt{-D})$ CM elliptic curves complex multiplication

function fields Drinfeld modules

K = finite extension of $\mathbb{Q}_p$ — Lubin-Tate (formal groups)

* (Shimura)

: ?? (Bertolini-Darmon)

Bonus observation: the principal ideal theorem

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

Note: $(2, 1+\sqrt{-5})\mathcal{O}_L = (1+\sqrt{-1})\mathcal{O}_L$.

$\Rightarrow$ Every ideal of $\mathcal{O}_K$

becomes principal in $\mathcal{O}_L$!