sec:lect1

## 1. Lecture 1, Brian Shin, 6/1

Goal of this seminar is to introduce the "Langlands philosophy". What is this? The idea is to understand the number field extensions of $K$ in terms of the arithemtic of $K$. What does vague statement mean? Note that we are largely following garbanati [Gar81] for the first few lectures.

First, we interpret the arithmetic of a number field $K$ to mean the study of primes of $\mathcal{O}_K$, the ring of integers of $K$ (the integral closure of $\mathbb{Z}$ in $K$).

*Example* 1. The arithmetic of $K$ is determined by the group

$$\begin{aligned} \mathrm{Div}(K) &= \text{“group of divisors of K”} \\ &= \text{"Free abelian group generated by primes of K"}. \end{aligned}$$

There exists an exact sequence describing $\mathrm{Div}(K)$:

$$0 \to \mathcal{O}_K^* \to K^* \to \mathrm{Div}(K) \to \mathrm{Cl}(K) \to 0.$$

It is a classical fact in algebraic number theory that the Galois extensions $L/K$ are determined by the set

$$\mathrm{Spl}(L/K) = \left\{ \mathfrak{p} \subset \mathcal{O}_K | \mathfrak{p} \text{ splits completely over L} \right\}.$$

Where by $\mathrm{Spl}(L/K)$ we mean the following: Given $L/K$ an extension of number fields, and $\mathfrak{p} \subset \mathcal{O}_K$ a prime ideal, then $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \dots \mathfrak{P}_r^{e_r}$ is a unique factorization into prime ideals of $\mathcal{O}_L$ (since $\mathcal{O}_L$ is a Dedekind domain) with $f_i = [\mathcal{O}_L/\mathfrak{P}_i : \mathcal{O}_K/\mathfrak{p}]$. We say $\mathfrak{p}$ splits completely if all the $e_1 = \dots = e_r = f_1 = \dots = f_r = 1$.

We now offer a proof sketch of this fact. Let $L, L'$ be two Galois extensionf of $K$. These two extensions fit into a diagrams

$$\begin{tikzcd} & LL' \arrow[dl, dash] \arrow[dr, dash] & \\ L \arrow[dr, dash] & & L' \arrow[dl, dash] \\ & K & \end{tikzcd}$$

We also have the containments $\mathrm{Spl}(L/K) \supseteq \mathrm{Spl}(LL'/K)$, $\mathrm{Spl}(L'/K) \supseteq \mathrm{Spl}(LL'/K)$, and their intersection equaling $\mathrm{Spl}(LL'/K)$.

By a theorem of Frobenius, if $L/K$ is Galois, then $\mathrm{Spl}(L/K)$ has density $1/[L : K]$ in the set of all primes of $K$ (where it's up to you to interpret what we mean by density). So $\mathrm{Spl}(L/K) = \mathrm{Spl}(L'/K)$ implies $[L : K] = [LL' : K] = [L' : K]$ and hence $L = L'$

Remark: The use of densities implies that it sufficies to know $\mathrm{Spl}(L/K)$ up to a finite set.

We can refine our goal slightly

(1) Classify finite Galois extensions of $K$ in terms of the arithmetic of $K$.
(2) For a given Galois extension $L/K$ describe $\mathrm{Gal}(L/K)$ in terms of the arithmetic of $K$.

Recall: Let $L/K$ be a finite extension, $\mathfrak{p} \subset \mathcal{O}_K$ a prime ideal which factors in $\mathcal{O}_L$ as

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \dots \mathfrak{P}_1^{e_r}.$$

If $L/K$ is Galois, then let $\sigma \in \mathrm{Gal}(L/K)$ be an element of the Galois group. The group acts on prime ideals of $L$ by $\sigma\mathfrak{P} = \{\sigma(x) | x \in \mathfrak{P}\}$, and permutes the primes lying over $\mathfrak{p}$. This defines a transitive group action of $\mathrm{Gal}(L/K)$ on the set of the $\mathfrak{P}_i$ over $\mathfrak{p}$. In particular, this implies that $e_1 = \ldots e_r = e$ and $f_1 = \ldots = f_r = f$. For each of these $\mathfrak{P}_i$ we have a canonical surjection

$$\mathrm{Fix}(\mathfrak{P}_i) \to \mathrm{Gal}(\kappa(\mathfrak{P}_i)/\kappa(\mathfrak{p})) = \mathbb{Z}/f\mathbb{Z}$$

Fact, if $e = 1$ this is an isomorphism. So for any prime living above $\mathfrak{p}$ there is a canonical generator of the group fixing the prime $\mathfrak{P}_i$. Call this canonical element $\mathrm{Frob}_{\mathfrak{P}_i} \in \mathrm{Gal}(L/K)$.

Note: This condition that $e = 1$ is necessary, but no so bad. There are only going to be a finite number of ramified primes. So again, with respect to densities we should be alright making this assumption.

All of the $\mathrm{Frob}_{\mathfrak{P}_i}$ are conugate in $\mathrm{Gal}(L/K)$, and hence $\mathfrak{p} \subset \mathcal{O}_K$ determines a canonical conjugacy class $\mathrm{Frob}_{\mathfrak{p}} \subset \mathrm{Gal}(L/K)$. Another example of the arithmetic of $K$ determining the structure of the extension $L/K$ is the following proposition:

**Proposition 1.** *An unramified prime $\mathfrak{p} \subseteq \mathcal{O}_K$ splits completely in $L$ if and only if* $\mathrm{Frob}_{\mathfrak{p}} = \{\mathrm{Id}\}$.

*Example* 2. Consider the field extension $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$ with $d$ a square free integer. Let

$$\Delta = \begin{cases} d & \text{if } d \equiv 1 \mod 4 \\ 4d & \text{else} \end{cases}$$

Note: In this case, $\Delta$ is the discriminant of this field extension.
Fact: $\mathrm{Frob}_p = \left(\frac{\Delta}{p}\right)$, the usual Legendre symbol.
Fact: $p$ is unramified in $\mathbb{Q}(\sqrt{d})$ if and only if $p \nmid \Delta$

It can be shown that the association of Frobenius map in this case factors through $(\mathbb{Z}/\Delta\mathbb{Z})^\times$.

$$\begin{tikzcd}
\{p \text{ unramified }\} \arrow[r, "\mathrm{Frob}_p"] \arrow[dr] & \mathrm{Gal}(\mathbb{Q}(\sqrt{d})/\mathbb{Q}) \\
 & (\mathbb{Z}/\Delta\mathbb{Z})^\times \arrow[u]
\end{tikzcd}$$

With a little more work, this factorization is shown to be equivalent to the classical statement of quadratic reciprocity.

We now want to accomplish the two goals laid out earlier for all field extensions. This is still an open question in general, but some work has already been done in special cases. In particular, class field theory accomplishes this goal for finite abelian extensions of $L/K$ of number fields. One of the aspects of the Langlands program is to extend this analysis to non-abelian extensions.

sec:lect2

## 2. Lecture 2, Brian Shin, 6/8

The goal for this lecture is to discuss class field theory over $\mathbb{Q}$. Lets remember the goals:

Start with a number field $K$.

(1) Classify the Galois extensions of $K$ in terms of the arithmetic of $K$.
(2) Given a Galois extension $L/K$, realize $\mathrm{Gal}(L/K)$ in terms of the artihmetic of $K$.

(3) Given a Galois extension $L/K$, study the decomposition of primes of $K$ in terms of the arithmetic of $K$.

We'll tackle these questions for the specific case of *abelian* extensions of $\mathbb{Q}$ in this lecture.

**Definition 1.** The $m$th cyclotomic field $\mathbb{Q}_m$ (notation from Garbanati) is the extension $\mathbb{Q}(e^{2\pi i/m})$.

A couple facts about the Galois theory of $\mathbb{Q}_m$:

(1) $\mathbb{Q}_m$ is the *splitting field* of $x^m - 1$.
(2) $\mathrm{Gal}(\mathbb{Q}_m/\mathbb{Q}) = (\mathbb{Z}/m\mathbb{Z})^\times = C_m$, where the equality is taking the residue $\bar{n}$ to the automorphism taking $\zeta \mapsto \zeta^n$.

The arithmetic of $\mathbb{Q}_m = \mathbb{Z}[\zeta]$.

For any prime $p$, let $f_p$ be the smallest $f \in \mathbb{N}$ such that $p^f \equiv 1 \mod m/p^{\nu_p(m)}$ (if $p \nmid m$ then this is easier to describe). Then $p$ factors over $\mathbb{Q}_m$ as

$$p = (\mathfrak{P}_1 \dots \mathfrak{P}_g)^{\nu_p(m)}$$

and each $\mathfrak{P}_i$ has inertial degree $f_p$.

**Theorem 1.** *Fore any finite abelian extension $L/\mathbb{Q}$, there is a positive integer $m$ and an embedding $L \subset \mathbb{Q}_m$.*

This theorem is by no means obvious (really hard, Kronecker-Weber theorem). This will allow us to resolve our goal of solving the above 3 problems.

**Definition 2.** $L/\mathbb{Q}$ abelian. If $L \subseteq \mathbb{Q}_m$, we say $m$ is a *defining modulus* of $L$. The smallest defining modulus is called the *conductor* $\mathfrak{f}_L$ of $L$.

Observe $\mathbb{Q}_m \cap \mathbb{Q}_n = \mathbb{Q}_{\gcd(m,n)}$. In particular, any $L/\mathbb{Q}$ abelian can be realized as the fixed field as the fixed field $\mathbb{Q}_m^{I_{L,m}}$ for some modulus $m$.

Note that this actually resolves our questions...

$C_m = (\mathbb{Z}/m\mathbb{Z})^\times$ is part of *arithmetic* of $\mathbb{Q}$. This is particularly trivial in this case, because any prime number is an element of $C_m$ by considering its modulus mod $m$. So what are the resolutions?

Classify abelian extensions of $\mathbb{Q}$: start with $m$ a modulus, and take $I_{L,m} \subseteq C_m$.

Given the abelian extension $L/\mathbb{Q}$ realize $\mathrm{Gal}(L/\mathbb{Q})$:

If $L/\mathbb{Q}$ corresponds to $I_{L,m} \subseteq C_m$. then we have the short exact sequence:

$$1 \to I_{L,m} \to C_m \to \mathrm{Gal}(L/\mathbb{Q}) \to 1$$

Some people call this "reciprocity", and the last map is denote in this case to be $(L/\mathbb{Q}/-)$, the Artin symbol. Note about why $(\mathbb{Z}/m\mathbb{Z})^\times$ is arithmetic because we can think of the map:

$$\begin{aligned} \mathbb{Z}\left\{p : p \nmid m \text{ primes}\right\} &\to (\mathbb{Z}/m\mathbb{Z})^\times \\ p &\mapsto \bar{p} \end{aligned}$$

Ramification: Let $L/\mathbb{Q}$ Abelian with defining modulus $m$. If $p \nmid m$, then $p$ is *unramified* in $L$. In fact we have the Conductor-Ramification theorem

**Theorem 2.** *Let $L/Q$ be Abelian. A prime number $p$ ramifies in $L$ if and only if $p | \mathfrak{f}_L$.*

Another number with this property is the discriminant. There's a theorem that says these two things are related. (they have the same prime factors)

Decomposition of primes:

$$C_m \longrightarrow \mathrm{Gal}(L/\mathbb{Q})$$

**Theorem 3.** *Let $L/\mathbb{Q}$ be an Abelian extension with modulus $m$. For $p$ a prime number, and $p \nmid m$ then the* order *of $\left(L/\mathbb{Q}, p\right) \in \mathrm{Gal}(L/\mathbb{Q})$ is the inertia degree of $p$.*

In particular, if $p \nmid m$ then $p$ splits completely in $L$ if and only if $\left(L/\mathbb{Q}, p\right) = 1$ if and only if $\left(L/\mathbb{Q}, p\right) \in I_{L,m}$.

*Example* 3. Quadratic reciprocity says:

$$\left(\frac{p^*}{q}\right) = \left(\frac{p}{q}\right)$$

where $p, q$ are distinct primes such that $p^* = (-1)^{\frac{p-1}{2}} p$. Fact: $\mathbb{Q}(\sqrt{p}) \subset \mathbb{Q}_p$, and it's the fixed field of $\left((\mathbb{Z}/p\mathbb{Z})^\times\right)^2 \subseteq (\mathbb{Z}/p\mathbb{Z})^\times$

$$\left(\frac{p^*}{q}\right) = 1 \iff q \text{ splits completel in } \mathbb{Q}_p \iff$$

$$\iff q \in \left((\mathbb{Z}/p\mathbb{Z})^\times\right)^2$$

*Remark* 1. Using the moduli is *annoying* because this is a non-canonical choice. We can define the defining one, but when comparing different abelian extensions we need to start using non-canonical moduli and this stuff goes terribly.

Also note that all abelian extensions of $\mathbb{Q}$ arise via special values of $f(z) = e^{2\pi i z}$.

Next time: Class field theory over a general number field.

## 3. Lecture 3, Brian Shin, 6/15

sec:lect3

Recall the goals of class field theory: Let $K$ be a number field, we want to

(1) Classify the abelian extensions of $K$ in terms of the arithmetic of $K$.
(2) Given an abelian extension $L/K$, we want to realize the Galois group $\mathrm{Gal}(L/K)$ in terms of the arithmetic of $K$.
(3) Given an Abelian extension $L/K$, we want to study the decomposition of primes of $K$ in terms of the arithmetic of $K$.

We achieved this solution over $\mathbb{Q}$ by leveraging the Kronecker-Weber theorem that any abelian extension is contained in a cyclotomic field extension $\mathbb{Q}_m = \mathbb{Q}(\zeta_m)$. Now we will find suitable replacements for all the various constructions seen before in the new setting when the base of our extensions of a general numberfield $K$ instead of $\mathbb{Q}$.

Let $K$ be a number fields

**Definition 3.** A *prime* of $K$ is an equivalence class of *valuations* on $K$.

*Example* 4. For $\mathfrak{p}$ a prime ideal and an element $a$, the functions

$$\|a\| = |\mathcal{O}_K/\mathfrak{p}|^{\nu_{\mathfrak{p}}(a)}$$

Defines a prime. These are called *finite* primes (i.e. $\mathfrak{p} \nmid \infty$).

*Example* 5. For a complex embedding $\sigma : K \to \mathbb{C}$, the function $\|a\| = |\sigma a|$ defines a prime $\mathfrak{p}_\sigma$. These are *infinite* primes (i.e. $\mathfrak{p}_\sigma | \infty$). If $\sigma(K) \subset \mathbb{R}$, we say $\mathfrak{p}_\sigma$ is *real.*

Fact: All primes of $K$ are of this form. This is a fairly standard fact from a first course in algebraic number theory.

**Definition 4.** A *modulus* of $K$ is a formal product

$$\mathfrak{m} = \mathfrak{m}_0 \cdot \mathfrak{m}_\infty$$

where $\mathfrak{m}_0$ is an *ideal* of $\mathcal{O}_K$ and $\mathfrak{m}_\infty$ is a collection of *infinite real primes* of $K$.

Remark: This will play the role of $m$ from before.

**Definition 5.** For $\mathfrak{m}$ let

$$S(\mathfrak{m}) = \left\{ \text{ primes that divide } \mathfrak{m} \right\}$$

$$I_K^{S(\mathfrak{m})} = \text{ free abelian group generated by finite primes } \mathfrak{p} \notin S(\mathfrak{m})$$

$$R_K^{S(\mathfrak{m})} = \text{ subgroup generated by } \frac{a}{b} \text{ with } a \equiv b \mod \mathfrak{m}_0, \text{ and } \sigma\left(\frac{a}{b}\right) > 0 \text{ if } \mathfrak{p}_\sigma \mid \mathfrak{m}_\infty$$

$$C_\mathfrak{m} = I_K^{S(\mathfrak{m})} / R_K^{S(\mathfrak{m})}$$

*Example* 6. For $K = \mathbb{Q}$ and $\mathfrak{m} = m \cdot \infty$ where $m$ is a positive integer, and $\infty$ corresponds to the usual inclusion $\mathbb{Q} \hookrightarrow \mathbb{R}$.

$$S(\mathfrak{m}) = \{\text{prime divisors of } m\} \cup \{\infty\}$$

$$I_\mathbb{Q}^{S(\mathfrak{m})} = \left\{ \frac{a}{b} \in \mathbb{Q}^\times \mid \; a, b \text{ positive}, \gcd(a, m) = \gcd(b, m) = 1 \right\}$$

$$R_\mathbb{Q}^{S(\mathfrak{m})} = \left\{ \frac{a}{b} \in I_\mathbb{Q}^{S(\mathfrak{m})} \mid \; a \equiv b \mod m \right\}$$

$$C_\mathfrak{m} = (\mathbb{Z}/m\mathbb{Z})^\times$$

In the case of general number field, $C_\mathfrak{m}$ will play the role of $(\mathbb{Z}/m\mathbb{Z})^\times$.

Let $L/K$ be a finite Abelian extension. Recall that if $\mathfrak{p}$ is a finite prime of $K$ unramified in $L$, then there is a unique element

$$\mathrm{Frob}_\mathfrak{p} \in \mathrm{Gal}(L/K)$$

such that

$$\mathrm{Frob}_\mathfrak{p}(x) \equiv x^{|\mathfrak{p}|} \mod \mathfrak{P}$$

for any $x \in \mathcal{O}_L$, $\mathfrak{P} \mid \mathfrak{p}$.

For any finite set $S$ of prime ideals of $K$ that includes the primes that ramify in $L$, we can define:

$$\begin{aligned} (L/K, -) : I_K^S &\longrightarrow \mathrm{Gal}(L/K) \\ \mathfrak{p} &\mapsto \mathrm{Frob}_\mathfrak{p}. \end{aligned}$$

We call this map the *Artin map.*

Observe that for $\mathfrak{P}$ a prime ideal of $L$ unramified over $\mathfrak{p}$ with inertia degree $f$ let

$$\mathrm{Nm}_{L/K}(\mathfrak{P}) = \mathfrak{p}^f$$

*Remark* 2. We have seen already how to define a norm map $\mathrm{Nm} : L \to K$, and it can be shown that the above definition matches with the norm calculated element-wise on the elements of $\mathfrak{P}$.

Then $(L/K, \mathrm{Nm}_{L/K}(\mathfrak{P})) = (L/K, \mathfrak{p})^f = \mathrm{Frob}_{\mathfrak{p}}^f = id$.

Thus $\mathrm{Nm}(I_K^S) \subseteq \ker((L/K, -))$.

Fact: The Artin map is always surjective. A consequence of this is that for a modulus $\mathfrak{m}$, there is a field $K(\mathfrak{m})/K$ such that $\ker((K(\mathfrak{m})/K, -)) = R_K^{\mathfrak{m}}$.

We would therefore know that $C_{\mathfrak{m}} \xrightarrow{\sim} \mathrm{Gal}(L/K)$. We would call this stand-in for $\mathbb{Q}_m$ the *Ray class field* of $\mathfrak{m}$.

Let $K$ be a number fields. The three main theorems of Class field theory are:

**Theorem 4** (Existence). *For any modulus $\mathfrak{m}$, there is a finite abelian extension $K(\mathfrak{m})/K$ that is unramified outside $S(\mathfrak{m})$ and such that the kernel of the Artin map $(K(\mathfrak{m})/K, -)$ is $R_K^{S(\mathfrak{m})}$.*

**Theorem 5** (Completeness). *For any finite abelian extension $L/K$ there is a modulus $\mathfrak{m}$ with $L \subset K(\mathfrak{m})$.*

**Theorem 6** (Reciprocity). *For any ffinite abelian extension $L/K$ of modulus $\mathfrak{m}$, the kernel of the Artin map*

$$(L/K, -) : I_K^{S(\mathfrak{m})} \longrightarrow \mathrm{Gal}(L/K)$$

*is the image of the norm map $\mathrm{Nm}_{L/K}(I_L^{S(\mathfrak{m})})$.*

Remarks:

- Modern formulation involved using idele groups
- Modern proofs proceed via local to global principals
- In the local case, can proceed via
  - Brauer groups and central simple algebras
  - Cohomology of Galois groups
  - Explicit constructions via Lubin-Tate formal groups
- In the global case, there is no explicit construction of $K(\mathfrak{m})$
- There is a formulation in terms of $L$-functions.

## 4. Lecture 4, Matej Penciak, 7/6

sec:lect4

The goal of the next few lectures is to understand some of the remarks that were made at the end of the last talk. In particular:

- A formulation of class field theory in terms of Adeles and Ideles
- A formulation of class field theory in terms of L-functions
- A local-to-global derivation of class field theory

With so many paths forward it's hard to decide which to tackle first (with the eventual goal of arriving at the Langlands program), so lets try to tackle the ideas as they appeared chronologically in history. To get an idea about the history of the subject, we follow [Con] (history_of_cft). Taking stock of all that we've done, we've essentially arrived at the formulation and results of class field theory known to Takagi. It's been a bit, so in order to state the results we know so far lets recap a few definitions:

*What followed was a recap of the last lecture, recalling $I_K^{S(\mathfrak{m})}$, $R_K^{S(\mathfrak{m})}$, $C_{\mathfrak{m}}$.*

Define a *ideal group* to be a subgroup of $I_K^{S(\mathfrak{m})}$ which contains $R_K^{S(\mathfrak{m})}$ (so that there is a bijection between ideal groups for a fixed modulus $\mathfrak{m}$ and subgroups of $C_{\mathfrak{m}}$).

For an abelian extension $L$ over $K$, define the subgroup $\mathrm{Nm}(L/K)$ of $I_K^{S(\mathfrak{m})}$ (for $S(\mathfrak{m})$ containing the primes ramifying in $L$) as the group generated by the norms of ideals from $\mathcal{O}_L$. Furthermore, define the ideal group $H_{\mathfrak{m}}(L/K)$ in $I_K^{S(\mathfrak{m})}$ as

$$H_{\mathfrak{m}}(L/K) = R_K^{S(\mathfrak{m})} \cdot \mathrm{Nm}(L/K).$$

It follows that

$$[I_K^{S(\mathfrak{m})} : H_{\mathfrak{m}}(L/K)] \leq [L : K]$$

and Takagi defined $L$ as a *class field of* $K$ to be field extensions $L$ of $K$ for which there exists a modulus $\mathfrak{m}$ for which the above is an equality. With these definitions in hand, we can state the main results of class field theory as proven by Takagi:

**Theorem 7.** *Let $K$ be a number field*

(1) *To each ideal group $H$, there is a unique class field extension of $K$ (existence)*
(2) *If $H \subseteq C_{\mathfrak{m}}$ corresponds to the extension $L/K$, then* $\mathrm{Gal}(L/K)$ *is isomorphic to $C_{\mathfrak{m}}/H$. (isomorphism)*
(3) *Any finite abelian extension is a class field. (completeness)*
(4) *If $H_1, H_2$ are two ideal gropus for a fixed modulus, and $L_1, L_2$ their associated extensions of $K$, then $H_1 \subseteq H_2 \Leftrightarrow L_1 \subseteq L_2$ (comparison)*
(5) *The primes of $K$ appearing in the* conductor *(minimal modulus of $L$) $\mathfrak{f}_{L/K}$ are the ramified places for the field extension $L/K$ (conductor)*
(6) *Any $\mathfrak{p} \nmid \mathfrak{m}$ is unramified in $L$, and the residue field degree $[\mathcal{O}_L/\mathfrak{p} : \mathcal{O}_K/\mathfrak{p}]$ is the order of $\mathfrak{p}$ in $C_{\mathfrak{m}}/H$. (decomposition)*

Let us make some remarks about the above theorem

*Remark* 3.

(1) The existence theorem Takagi proves is more general than the existence theorem that Brian stated in the last lecture, which corresponds to the existence theorem for the trivial subgroup $\{id\} \subseteq C_{\mathfrak{m}}$.
(2) The isomorphism theorem proven by Takagi is non-explicit. The reciprocity theorem from Brian's lecture implies the isomorphism with the explicit isomorphism being given by the reciprocity map $(L/K, -)$. It is not until Artin's proof of his reciprocity theorem that the above isomorphism can be made explicit, and once the isomorphism is selected the decomposition theorem becomes a simple corollary. Artin's original motivation for the proof of his reciprocity theorem was a study of his so-called Artin L-functions. In fact the reciprocity theorem will be seen to be equivalent to a certain equivalence of L-functions which will be the first new topic we cover next time.
(3) The comparison theorem is one of the motivations for getting rid of the moduli $\mathfrak{m}$ in class field theory, which is achieved by stating all the results in the context of the Adeles/Ideles.

## 5. Lecture 5, Matej Penciak, 7/13

sec:lect5

The goal of the next few lectures on L-functions is to tackle the following topics in order

(1) Dirichlet L-series (their motivation, definition, and analytic continuation).
(2) Class field theory over $\mathbb{Q}$ in terms of L-functions.
(3) Weber/Hecke L-series.
(4) Artin reciprocity and class field theory over a general number field $K$.

To begin, we will start with Dirichlet L-series.

Dirichlet wanted to prove his theorem on infinitely many primes in arithmetic progression. The idea of the proof is the copy the proof that there are infinitely many primes via the statement that $\zeta(s)$ has a pole at $s = 1$.

Write

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p \text{ prime}} \left(1 - p^{-s}\right)^{-1}$$

Then $\zeta(s)$ having a pole at $s = 1$ implies that

$$\log \zeta(s) = \sum_{p} \frac{1}{p^s} + O(1) \text{ as } s \to 1$$

Hence $\sum_p \frac{1}{p}$ diverges. In order to differentiate the different conjugacy classes of primes in $(\mathbb{Z}/n\mathbb{Z})^{\times} = C_n$ we introduce characters $\chi : C_n \to \mathbb{C}^{\times}$. Denote the group of characters on $C_n$ by $\widehat{C_n}$.

Any character $\chi \in C_n$ can be extended to a multiplicative function (which we denote by the same character via abuse of notation) $\chi : \mathbb{N} \to \mathbb{C}$ via

$$\chi(m) = \begin{cases} \chi(\bar{m}) & \bar{m} \not\equiv 0 \mod n \\ 0 & \bar{m} \equiv 0 \mod n \end{cases}$$

With this extension, define the Dirichlet L-function associated to $\chi$ By

$$L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$$

which converges absolutely for real part greater than 0. Also in that half-plane the above infinite sum can be decomposed (via the strong multiplicativity of $\chi$) into the Euler product formal

$$L(s, \chi) = \prod_{p \text{ prime}} \left(1 - \chi(p) p^{-s}\right)^{-1}.$$

In order to prove the theorem on arithmetic progression the main results established are

**Lemma 1.** *Let $\chi : (\mathbb{Z}/n\mathbb{Z})^{\times} \longrightarrow \mathbb{C}^{\times}$ be a character.*

*(1) If $\chi$ is not the trivial character, than $L(s, \chi)$ is analytic for $\mathrm{Re}(s) > 0$.*
*(2) If $\chi = \chi_0$ the trivial character, then $L(s, \chi_0)$ has a pole at $s = 1$.*
*(3) For $\chi \neq \chi_0$, then $L(1, \chi) \neq 0$.*

Before we remark on the above results, the remaining part of the proof of Dirichlet's theorem goes as follows: The goal is to prove

$$\sum_{p \equiv k \mod n} \frac{1}{p^s}$$

diverges for $s \to 1$. The indicator function for the $k$ conjugacy class ins $(\mathbb{Z}/n\mathbb{Z})^{\times}$ is not a character on the finite group, but it is a conjugacy invariant function so it can be written as linear combination of characters $\delta_k = \sum_i c_i \chi_i$. Furthermore, $c_0 \neq 0$ by considering the inner product $\langle \delta_k, \chi_0 \rangle$. As $s \to 1$ then

$$\sum_{p \equiv k \mod n} \frac{1}{p^s} = c_0 \sum_p \frac{1}{p^s} + \sum_{\chi_i \neq \chi_0} c_i \left( \sum_p \frac{\chi_i(p)}{p^s} \right)$$

diverges because the summands on the right hand side are equal (up to constant) to $\log L(s,\chi_0)$ and $\log L(s,\chi_i)$ which diverge (and $c_0 \neq 0$) and remain finite and non-zero as $s \to 1$.

The follow are some remarks on the above Lemma

*Remark* 4. As far as my understanding goes, there is no interesting arithmetic content in the first part of the theorem. The second part of the theorem is not hard to prove, it follows from the factorization of the L-function as

$$L(s,\chi_0) = \prod_{p|n}(1-p^{-s}) \cdot \zeta(s)$$

which has a pole at $s = 1$ since the first product is finite and non-zero. This is not difficult to show, but has some interesting arithmetic content, and is the first example of a factorization of $L/\zeta$-functions we have seen. The final part seems to be the hardest to establish.

Though the following is not crucial to establish class field theory over $\mathbb{Q}$, we include it for completeness. We will not show that $L(s,\chi)$ can be extended to a meromorphic function on $\mathbb{C}$ analytic away from $s = 1$. This is established in an argument mirroring Riemann's original argument on the analytic continuation of the $\zeta$-function which is established via a functional equation relating $\zeta(s)$ and $\zeta(1-s)$. Because it serves as a guide, lets understand this argument first.

The argument can be divided into six main steps

(1) Express $\zeta(s)$ as an infinite sum

$$\zeta(s) = \sum_{n=1}^{\infty} n^{-s}$$

which converges for $\operatorname{Re} s > 1$.

(2) Extend $\zeta(s)$ to $\operatorname{Re} s > 0$ except for a pole at $s = 1$. As far as I can tell, the various arguments used for $\zeta(s)$ and other L-functions for which this property holds do not have any interesting arithmetic content. In the particular case for $\zeta(s)$, it amounts to writing $1/(1-s)$ in a clever way in the expression $\zeta(s) - 1/(1-s)$ which converges for $\operatorname{Re} s > 0$.

(3) Define $\Lambda(s) = \pi^{-s/2}\Gamma(\frac{s}{2})\zeta(s)$. It will be $\Lambda$ that satisfies a clean functional equation relating $\Lambda(s)$ to $\Lambda(1-s)$ (which would establish analyticity for $\zeta$ for $\operatorname{Re} s < 0$.)

(4) Write $\Lambda(s)$ as the Mellin transform

$$\Lambda(s) = \frac{1}{2}\int_0^{\infty} (\theta(t)-1)\, t^{\frac{s}{2}-1}\, dt$$

where $\theta(t)$ is the Riemann $\theta$-functions

$$\theta(t) = \sum_{n=-\infty}^{\infty} \exp(-\pi n^2 t).$$

Sometimes it is worth writing the Mellin transform in terms of the factor $t^{\frac{s}{2}}\frac{dt}{t}$. (make a comment about $\theta(t)$ being a section of a bundle on $\mathcal{M}_{g,1}$?)

(5) Show that $\theta(t)$ satisfies the functional equation

$$\theta\left(\frac{1}{t}\right) = t^{\frac{1}{2}}\theta(t).$$

Intuitively then the "multiplicative" functional equation for $\theta$ becomes an "additive" functional equation for $\zeta$. (this argument is very vague and doesn't't) The functional equation for $\theta$ can be established in a number of ways (some more abstract than others), but the generalizable argument follows from the Poisson summation formula

**Theorem 8**. *Let $f$ be a Schwartz-class function and $\hat{f}$ its Fourier transform. Then*

$$\sum_{n=-\infty}^{\infty} f(n) = \sum_{m=-\infty}^{\infty} \hat{f}(m).$$

Applying this theorem for $f(u) = \exp(-\pi t u^2)$ implies the above theorem. $f(u)$ in this case is a nice function with an easy Fourier-transform.

(6) Split the integral from part 4 up into a sum of integrals

$$\int_0^\infty (\ldots) = \int_0^1 (\ldots) + \int_1^\infty (\ldots).$$

The on the first integral, use the functional equation on $\theta(t)$ to relate it to $\theta(1/t)$. Simplify further with the substitution of $t \to 1/t$ in the first integral and arrive at

$$\int_0^\infty (\ldots) = \int_1^\infty (\ldots\theta(t)\ldots)\, t^{-\frac{s}{2}+1}\frac{dt}{t} + \int_1^\infty (\ldots\theta(t)\ldots)\, t^{\frac{s}{2}}\frac{dt}{t}$$

which is manifestly symmetric under the change of variables $s \leftrightarrow 1-s$. Hence arrive at the functional equation $\Lambda(s) = \Lambda(1-s)$.

For Dirichlet $L$-series the argument follows in a similar way

(1) This follows immediately from the definition, and that the characters are mapped to roots of unity.
(2) As stated above, this doesn't seem to have much interesting arithmetic content (except maybe the residue of $L(s, \chi_0)$ at $s = 1$ which will contain arithmetic content about the field $\mathbb{Q}(\zeta_n)$.)
(3) At this point we need to distinguish between two different classes of Dirichlet characters, those for which $\chi(-1) = 1$ which we call even and $\chi(-1) = -1$ which we call odd.

$$\Lambda(\chi, s) = \pi^{\frac{s}{2}}\Gamma(\frac{s}{2})L(\chi, s) \quad \chi \text{ even}$$
$$\Lambda(\chi, s) = \pi^{\frac{s+1}{2}}\Gamma(\frac{s+1}{2})L(\chi, s) \quad \chi \text{ odd}$$

We will see later that the distinction between even and odd characters will be related to the reality of the character on $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$. This is an indication that the extra factors of $\pi$ and $\Gamma$ appearing in $\Lambda$ has some important arithmetic content relating to the infinite places of the field $K = \mathbb{Q}$.

(4) We can define the $\theta$-function

$$\theta_\chi(t) = \sum_{n=-\infty}^{\infty} \chi(n)\exp(-\pi n^2 t)$$

for $\chi$ even note that if $\chi$ is odd, then the above function becomes trivial because $\exp(-\pi n^2 t)$ is even in $n$. In order to alleviate this, we replace $\exp(-x^2)$

with the odd counterpart $x\exp(-x^2)$ and define the theta function for odd characters $\chi$:

$$\theta_\chi(t) = \sum_{n=-\infty}^{\infty} n\chi(n)(-it)^{\frac{1}{2}}\exp(-\pi n^2 t)$$

We can then compare terms and re-express $L(s,\chi)$ as an integral from 0 to $\infty$ of some expression involving $\theta_\chi$.

(5) We derive a functional equation for $\theta_\chi$ as we did for the Riemann $\theta$-function. At this point though, we need to restrict to ***primitive*** characters

**Definition 6**. A character $\chi : (\mathbb{Z}/n\mathbb{Z})^\times \to \mathbb{C}^\times$ is called ***primitive*** if it is not induced from a character $\bar{\chi} : (\mathbb{Z}/m\mathbb{Z})^\times \to \mathbb{C}^\times$ for some $m \mid n$, $m < n$. A ***modulus*** for $\chi$ is an $m$ such that $\chi$ defines a character on $(\mathbb{Z}/n\mathbb{Z})^\times$, and the ***conductor*** is the minimal modulus.

If $\widetilde{\chi}$ is not primitive, then we can write $L(\widetilde{\chi}, s) = L(s,\chi)\cdot C$ where $C$ is some finite product over Euler factors of primes. Hence even though we are restricting ourselves to primitive characters, we're not losing out on too much by making this restriction.

*Remark* 5. Even though we can re-express a non-primitive character's L-function in terms of a primitive character's L-function, the conductor (which will show up in the functional equation) will show up. So somehow the L-function of $\widetilde{\chi}$ knows about $\chi$.

Returning now to the functional equation for $\theta_\chi$, let $N$ be the conductor of $\chi$. Then we can write (for $\chi$ even)

$$\theta_\chi(t) = \sum_{b\in\mathbb{Z}/N\mathbb{Z}} \chi(b)\left(\sum_{l\in\mathbb{Z}} \exp(-\pi(lN+b)^2 t)\right).$$

Though we can't apply the Poisson summation formula for the full sum defining $\theta_\chi$ because of the factors of $\chi(n)$ in front of the terms, the inner sums can be re-evaluated using Poisson summation to arrive At

$$\sum_{k\in\mathbb{Z}} \frac{1}{N\sqrt{it}}\exp(-\pi\frac{k^2}{N^2 t})$$

with an extra coefficient of (combining the $\chi(b)$ from before, with terms arriving from the Fourier transform of the shifted-Gaussian)

$$\sum_{b\in\mathbb{Z}/N\mathbb{Z}} \chi(b)\cdot\exp(2\pi ikb)/N.$$

Replacing $b$ with $k^{-1}b$ (and noting that this can always be done by some business about character theory) we get that

$$\chi(k^{-1})\sum_{b\in\mathbb{Z}/N\mathbb{Z}} \chi(b)\cdot\exp(2\pi ib)/N = \chi(k^{-1})\sum_{b\in\mathbb{Z}/N\mathbb{Z}} \chi(b)\cdot\zeta_N^b$$

Where we now use the notation $\tau(\chi)$ for the above Gauss-sum.

The final functional equation for (even) $\theta_\chi$ is

$$\theta_\chi(t) = \frac{\tau(\chi)}{N\sqrt{it}}\theta_{\chi^{-1}}\left(\frac{1}{N^2 t}\right).$$

(6) Now finally apply the same trick using the integral representation from (4) by splitting the integral up as

$$\int_0^\infty = \int_{\frac{1}{N}}^\infty + \int_0^{\frac{1}{N}}$$

(note that $1/N = 1/N^2(1/N))$ and applying the functional equation for $\theta_\chi$. We arrive at the functional equations

$$\Lambda(\chi,s) = \tau(\chi)N^{-s}\Lambda(\chi^{-1},1-s)$$
$$\Lambda(\chi,s) = (-i)\tau(\chi)N^{-s}\Lambda(\chi^{-1},1-s)$$

for even and odd $\chi$. Note the appearance of the conductor, and the arithmetically interesting Gauss-sum in the functional equation. We'll see that this is a general pattern for more complicated $L$-functions.

Anyway, now we return to the main goal: Class field theory over $\mathbb{Q}$. We will do this next lecture, among other things. Note in the above arguments on Dirichlet $L$-functions, I largely followed [Gar], and [Min].

## 6. Lecture 6, Matej Penciak, 7/22

sec:lect6

The goal of this lecture is to state class field theory over $\mathbb{Q}$ in terms of Dirichlet L-functions as we defined in the last lecture, and see what the formulation will look like in general for class field theory over general number fields in terms of the to-be-defined Hecke L-functions. We will also end with a brief overview of the kinds of calculations that go into the proof of the analytic continuation of Hecke L-functions.

We first begin, as we usually do, with some remarks about last time

*Remark* 6. (1) First, I want to point out that [Neu99] has an execellent chapter on L-functions where all of the considerations above and below are treated in great detail. As part of his treatment of the subject, he has a very general consideration about how functional equations for $\theta$-functions lead immediately to the functional equations for $L$-functions. The general statement goes something like the following (which Neukirch refers to as the "Mellin Principle"):

Associated to a *nice* function $f$ we can define an $L$-function which we denote $L(f,s)$ via the formula

$$L(f,s) = \int_0^\infty (f(y) - f(\infty))y^s\,\frac{dy}{y}$$

where $f(\infty) := \lim_{y\to\infty} f(y)$ (assumed to exist because $f$ is nice). Then the Mellin principle states that if $f$ satisfies the functional equation

$$f(\frac{1}{y}) = Cy^k g(y)$$

for some other nice function $g$ and a constant $C$, then the associated $L$-functions satisfy

$$L(f,s) = CL(g,k-s).$$

We can therefore restrict our attention to the definition and functional equations of $\theta$-functions to derive any of the analytic continuation properties of $L$-functions from here on out

(2) So far these $\Gamma$-factors appearing in the formulas for analytic continuation have been a necessity and have been fairly unmotivated. For example, for the $\zeta$ function a quick way to see where the $\Gamma$ function comes from is by starting with its integral form and doing a change of variables $y \mapsto \pi n^2 y$:

$$\Gamma(s) = \int_0^\infty e^{-y} y^s \, \frac{dy}{y} = \int_0^\infty e^{-\pi n^2 y} \pi^s n^{2s} y^s \, \frac{dy}{y}$$

then re-arranging terms

$$\pi^{-s}\Gamma(s)\frac{1}{n^{2s}} = \int_0^\infty e^{-\pi n^2 y} y^s \, \frac{dy}{y}$$

and summing over $n$. For now, my speculation is that since the $\zeta$ function in some sense encodes the local information about finite primes, then by some form of product identity

$$\prod_v \|a\|_v = 1$$

the information can be also gathered for infinite places.

Ok now we return to our original goal. Let $K/\mathbb{Q}$ be an abelian extension, and introduce the *Artin* L-function associated to a character $\rho : \mathrm{Gal}(K/\mathbb{Q}) \to \mathbb{C}^\times$ as

$$L(\rho, s) = \prod_{\mathfrak{p}\text{ prime}} \left(1 - \rho(\mathrm{Frob}_\mathfrak{p})(\mathrm{Nm}\,\mathfrak{p})^{-s}\right)^{-1}$$

where $\mathrm{Nm}\,\mathfrak{p}$ is the absolute norm from $K$ to $\mathbb{Q}$ of the prime $\mathfrak{p}$. The above definition is not entirely precise as stated. Either we restrict the product to be over unramified primes, in which case $\mathrm{Frob}_\mathfrak{p}$ is well-defined, or we need to modify the local factor at ramified primes. Solution 1 is perhaps the easiest, but it prevents the L-function from having a nice formula for its functional equation. Solution 2 took Artin some time to figure out, but in the end isn't terribly complicated.

First note that if $\mathfrak{p}$ is a prime lying over $p$ in $\mathbb{Z}$, then $\mathrm{Frob}_\mathfrak{p}$ is naturally an element of $\mathrm{Gal}(\mathcal{O}_K/\mathfrak{p}/\mathbb{Z}/p\mathbb{Z})$ which we can identify with $D_\mathfrak{p}/I_\mathfrak{p}$ where $D_\mathfrak{p}$ is the decomposition group of $\mathfrak{p}$ (the subgroup of $\mathrm{Gal}(K/\mathbb{Q})$ which fixes $\mathfrak{p}$) and $I_\mathfrak{p}$ is the inertia group (the normal subgroup of $D_\mathfrak{p}$ which fixes elements of $\mathfrak{p}$ point-wise). If $\rho$ is a character of $\mathrm{Gal}(K/\mathbb{Q})$ we can restrict it to a character of $D_\mathfrak{p}$, and the value of $\rho(\mathrm{Frob}_\mathfrak{p})$ will depend only on this restriction. Now restrict to the case when $\mathfrak{p}$ is unramified. For unramified $\mathfrak{p}$, the inertia group $I_\mathfrak{p}$ is trivial, so usiing the above remarks we can re-write the 1-dimensional representation $\rho$ as

$$\rho(\mathrm{Frob}_\mathfrak{p}) = \left(\mathrm{Res}^{\mathrm{Gal}(K/\mathbb{Q})}_{D_\mathfrak{p}} \rho\right)(\mathrm{Frob}_\mathfrak{p}) = \left(\mathrm{Res}^{\mathrm{Gal}(K/\mathbb{Q})}_{D_\mathfrak{p}} \mathrm{Inf}^{D_\mathfrak{p}}_{D_\mathfrak{p}/I_\mathfrak{p}} \rho\right)|_{\mathbb{C}^{I_\mathfrak{p}}} (\mathrm{Frob}_\mathfrak{p})$$

where Res and Inf are the restriction and inflation to subgroups from quotient groups respectively, and in the last formula we are restricting the representation onto the subspace $\mathbb{C}^{I_\mathfrak{p}}$ of vectors fixed by $I_\mathfrak{p}$. It is this last formula which is well-defined even for ramified primes, and what we take to be the coefficient of $(\mathrm{Nm}\,\mathfrak{p})^s$ in the formula for the Artin L-function.

Having made the above modification on the the local factors at ramified primes, we can finally state the Kronecker-Weber theorem (which is in essence class field theory over $\mathbb{Q}$) as an equality of L-functions:

**Theorem 9** (Kronecker-Weber, v. 2). *Let $K$ be an abelian extension of $\mathbb{Q}$, and $\rho : \mathrm{Gal}(K/\mathbb{Q}) \longrightarrow \mathbb{C}^\times$ a character, then there is a unique primitive Dirichlet character $\chi$ on $(\mathbb{Z}/N\mathbb{Z})^\times$ such that we have an equality of L-functions*

$$L(\rho, s) = L(\chi, s)$$

*where the left hand side of the equality is an Artin L-function, and the right is a Dirichlet L-function.*

We see that the original formulation of Kronecker-Weber follows as a corollary of the above statement (in fact, it seems relatively clear that the two are equivalent)

**Corollary 1**. *Any abelian extension $K$ is contained in a cyclotomic extension $\mathbb{Q}(\zeta_N)$ for some $N$.*

*Proof.* If we write $G = \mathrm{Gal}(K/\mathbb{Q})$, and define

$$\zeta_K(s) = \sum_{I \text{ ideal in} \mathcal{O}_K} \frac{1}{(\mathrm{Nm}\, I)^s} = \prod_{\mathfrak{p} \text{ prime}} (1 - \mathrm{Nm}\, \mathfrak{p}^{-s})^{-1}$$

it can be shown that

$$\zeta_K(s) = \prod_{\rho \in \widehat{G}} L(\rho, s) = \prod_{\chi} L(\chi, s)$$

where the second equality comes from the above Kronecker-Weber theorem. Let $N$ be the least common multiple of all the conductors $f_\chi$ for the characters $\chi$.

Now we have the following chain of implications: $p$ splits in $\mathbb{Q}(\zeta_N)$ if and only if $p \equiv 1 \mod N$. Therefore $\chi(p) = 1$ for every character $\chi$ appearing in the above product of Dirichlet L-series. By Kronecker-Weber, we therefore know that $\rho(\mathrm{Frob}_p) = 1$ for every character $\rho \in \widehat{G}$, and hence $\mathrm{Frob}_p = \mathrm{Id}$ in $G$. Hence $p \in \mathrm{Spl}(K)$.

The containment $\mathrm{Spl}(\mathbb{Q}(\zeta_N)) \subseteq \mathrm{Spl}(K)$ implies, by the theorem from the first Brian lecture, that $\mathbb{Q}(\zeta_N) \subseteq K$. □

*Remark* 7.
(1) The Artin L-function doesn't have a naively defined series expension as $\sum \frac{a_n}{n^s}$ unless we go out of our way to factor all the ideas $I = \prod \mathfrak{p}$. The Kronecker-Weber theorem implies that in fact the series expansion for the Artin L-function is actually just that of a carefully chosen Dirichlet L-function.
(2) The L-functions and $\zeta$-functions from above all contain interesting arithmetic information about the field $K$. For example writing $\zeta_K$ as

$$\zeta_K(s) = \sum_I \frac{1}{\mathrm{Nm}\, I^s} = \sum_n \frac{r_K(n)}{n^s}$$

where $r_K(n)$ is the number of ideals in $\mathcal{O}_K$ of norm $n$. For example $r_K(p) = [K : \mathbb{Q}]$ if and only if $p$ splits completely, and $r_K(p) = 1$ if and only if $p$ is totally ramified. This theorem gives us some "generalized congruence conditions" for the splitting of primes in abelian extensionf of $\mathbb{Q}$ as was one of our original goals.
(3) This theorem can be used to prove that the Artin L-function has a functional equation, but my understanding is that this is a generally known fact indepdendent of the knowledge of Kronecker-Weber. The theorem *does* imply that Artin L-series for Abelian extensions are meromorphic functions on $\mathbb{C}$ though, which is a special case of the Artin conjecture.

*Example* 7. Lets see quadratic reciprocity (again). Let $K = \mathbb{Q}(\sqrt{q^*})$ where $q^* = (-1)^{q-1/2}q$. We know that we can identify $\mathrm{Gal}(K/\mathbb{Q})$ as the group of order 2 given By

$$\mathrm{Gal}(K/\mathbb{Q}) = \left(\mathbb{Z}/q\mathbb{Z}\right)/\left(\mathbb{Z}/q\mathbb{Z}\right)^{\times^2}$$

and the group has two characters, the trivial character $\chi_0$ and the non-trivial character $\chi_1$ which is exactly given by

$$\chi_1(n) = \left(\frac{n}{q}\right)$$

We can expand

$$\begin{aligned}\zeta_K(s) &= \prod_{\mathfrak{p}\text{ prime}} (1-\mathrm{Nm}(\mathfrak{p})^{-s})^{-1} \\ &= \prod_{p\text{ split}} (1-p^{-s})^{-2} \prod_{p\text{ inert}} \left(1-p^{-2s}\right)^{-1} \prod_{p\text{ ramified}} (1-p^{-s})^{-1}\end{aligned}$$

We also know that we can expand the $\zeta$-function as

$$\begin{aligned}\zeta_K(s) &= L(\chi_0, s)\cdot L(\chi_1, s) \\ &= \prod_{\substack{p \\ p\neq q}} (1-p^{-s})^{-1} \prod_p \left(1-\left(\frac{p}{q}\right)p^{-s}\right)^{-1}\end{aligned}$$

Comparing the coefficients of the above two expressions, we see that

$$\begin{cases} p \text{ ramifies} & \Longleftrightarrow p \mid q \\ p \text{ splits} & \Longleftrightarrow \left(\frac{p}{q}\right) = 1 \\ p \text{ is inert} & \Longleftrightarrow \left(\frac{p}{q}\right) = -1 \end{cases}$$

but by elementary algebraic number theory, we know that all we need to do is factor the polynomial $x^2 - q^*$ modulo $p$ in which case we arrive at

$$\begin{cases} p \text{ ramifies} & \Longleftrightarrow p \mid q \\ p \text{ splits} & \Longleftrightarrow \left(\frac{q^*}{p}\right) = 1 \\ p \text{ is inert} & \Longleftrightarrow \left(\frac{q^*}{p}\right) = -1 \end{cases}$$

which is exactly quadratic reciprocity.

Now what about class field theory over general number fields? We'll formulate it as an equality of L-functions, one of which will be the same Artin L-function from above. We must only find a generalization of Dirichlet L-series to L-series defined in terms of characters on the ray class groups $C_\mathfrak{m}$ we defined previously. This is exactly what Weber (and in a more general context, Hecke) did. In particular, we can easily define a *Weber-character* to be a character $\chi : C_\mathfrak{m} \longrightarrow \mathbb{C}^\times$. Since $C_\mathfrak{m}$ is finite, its image must land in the image of unit complex numbers of finite multiplicative order.

It should be noted that Weber characters generalize Dirichlet characters in the obvious way, with the on remark that since

$$\begin{aligned}C_n &\cong (\mathbb{Z}/n\mathbb{Z})^\times/\{\pm 1\} \\ C_{n\infty} &\cong (\mathbb{Z}/n\mathbb{Z})^\times\end{aligned}$$

we see the difference of even and odd Dirichlet characters as coming from the inclusion and exclusion of the real place in the defining modulus.

A generalization of the Weber character was produced by Hecke. Its definition using ideal-theoretic language is pretty complicated to state, so I will delay precisely defining Hecke characters (also known as größencharaktere). For now though, the vague idea of a Hecke character is that it's a multiplicative character

$$\chi : I_K^{S(\mathfrak{m})} \longrightarrow \mathbb{C}^\times$$

which can be written as a product $\chi = \chi_\infty \chi_f$ where $\chi_f$ is a character of finite order, and $\chi_\infty$ is a map

$$\chi_\infty : (K \otimes \mathbb{R})^\times \cong \left(\mathbb{R}^\times\right)^{r_1} \otimes \left(\mathbb{C}^\times\right)_2^{r} \longrightarrow \mathbb{C}^\times$$

not necessarily of finite order. Therefore $\chi$ may not be of finite order. The prototypical example of this situation is the character on ideals of $\mathbb{Z}$ given By

$$\chi\left((n)\right) = \chi(n) \left(\frac{n}{|n|}\right)^p$$

for $p = 0$ or $p = 1$ depending on if $\chi$ is even or odd (coming from $C_n$ or $C_{n\infty}$ as seen above). This extra $\chi_\infty$ factor fixes the fact that $\chi\left((n)\right)$ may not be defined if we choose a different generator for the ideal. Again, this definition is somewhat mysterious to me even at this point, so we'll return to it later once we have some more of the adelic language under our belt.

Whether we take the Weber or Hecke approach, in either case we can define the L-series

$$L(\chi, s) = \sum_{\mathfrak{a} \text{ integral}} \frac{\chi(\mathfrak{a})}{\mathrm{Nm}(\mathfrak{a})^s}.$$

Then class field theory, interpreted as a statement about L-functions, is simply the statement that

$$L_W(\chi, s) = L_A(\rho, s).$$

(i.e. that for any character $\rho$ of your galois group $\mathrm{Gal}(L/K)$ there exists a Weber character $\chi$ blahblahblah). In particular, this interpretation implies that the isomorphism

$$\begin{aligned} C_{\mathfrak{m}} &\longrightarrow \mathrm{Gal}(L/K) \\ [\mathfrak{p}] &\mapsto \mathrm{Frob}_{\mathfrak{p}} \text{ (at least for unramified primes)} \end{aligned}$$

is the explicit isomorphism that Takagi was missing. Artin's original motivation was a formulation of non-abelian class field theory, which he unfortunately did not achieve. But he did get this explicit isomorphism (the Artin symbol from before), so I'd say that's a pretty decent consolation prize.

We'll end this lecture with a comment about the analytic continuation of the Hecke $L$-functions. This is pretty much taken verbatim from the second lecture in the lecture notes [Kow]. In particular, we'll be restricting as the author does to the case of $\chi = \chi_0$ so that $L(\chi, s) = \zeta_K(s)$. First write

$$\zeta_K(s) = \sum_{a \in \mathrm{Cl}(K)} \zeta(s; a)$$

where

$$\zeta(s; a) = \sum_{[\mathfrak{a}] = a} \frac{1}{\mathrm{Nm}(\mathfrak{a})^s}.$$

Then let

$$\Lambda(s;a) = \pi^{-r_1 s/2}(2\pi)^{-r_2 s}\Gamma(s/2)^{r_1}\Gamma(s)^{r_2}\zeta(s;a)$$

which we will show satisfies the functional equation

$$\Lambda(s;a) = |D|^{1/2-s}\Lambda(1-s,(a\mathfrak{d})^{-1})$$

where $\mathfrak{d}$ is the *different ideal*. It's worth mentioning what the different is. First, the definition that seems to be the most common is as follows:

The trace paring $\mathrm{Tr}(--)$ is a quadratic form on $\mathscr{O}_K$, and $\mathfrak{d}^{-1} = \{x \in \mathscr{O}_K | \mathrm{Tr}(xy) \in \mathscr{O}_K \text{ for every } y\}$. More geometrically, the discriminant is simply the ramification divisor on the base, and the different ideal is the branch locus divisor on the branched cover.

To see where this functional equation comes from we'll follow the lead from previous proofs of the functional equation and try to find a $\theta$-function with appropriate functional equation given by the Poisson summation formula. To this end restrict further to the case we're taking the trivial ideal class $a = 1$ (corresponding to $[\mathscr{O}_K]$). Hence ideals are principal, and correspond to elements $z \in \mathscr{O}/\mathscr{O}^\times$. For each real and complex embedding $\sigma$ we can define

$$(d_\sigma \pi)^{d_\sigma s/2}\Gamma(d_\sigma s/2)|z|_\sigma^{-s} = \int_0^\infty \exp(-d_\sigma \pi y|z|_\sigma^2)y^{s/2}\,\frac{dy}{y}$$

where $d_\sigma = 1$ for real $\sigma$ and 2 for complex. We can write

$$\Lambda(s;\mathscr{O}) = \int \Theta_1(y;\mathscr{O})\|y\|^{s/2}\,\frac{dy}{y}$$

where $\|y\| = \prod_\nu |y|_\nu^{d_\nu}$ and $\frac{dy}{y} = \prod_\nu \frac{d|y|_\nu}{|y|_\nu}$ and

$$\Theta_1(y;\mathscr{O}) = \sum_{\substack{z\in\mathscr{O}/\mathscr{O}^\times \\ z\neq 0}} \exp\left(-\pi\sum_\nu y_\nu d_\nu |z|_\nu^2\right).$$

The theta function above $\Theta_1$ isn't quite a theta function in the traditional sense, since it's not a sum over a lattice. But what we can do instead is to split the integral up into an integral over $t = \|y\|$ first, and what we're left with is an integral over the unit sphere $G_1 = \{y \mid \|y\| = 1\}$. By the Dirichlet unit theorem the rank of $\mathscr{O}^\times$ is $r_1 + r_2 - -1$, and hence $G_1/\mathscr{O}^\times$ is compact. So we can split the integral up in the following schematic way

$$\begin{aligned}\int\sum_{\mathscr{O}/\mathscr{O}^\times} &= \int_0^\infty dt\int_{G_1/\mathscr{O}^\times}\frac{dy}{y}\sum_{\mathscr{O}^\times}\sum_{\mathscr{O}/\mathscr{O}^\times} \\ &= \int_0^\infty dt\int_{G_1/\mathscr{O}^\times}\sum_{\mathscr{O}}(\dots)\end{aligned}$$

which leaves us with a sum which *is* a $\theta$-function in the traditional sense, given by

$$\Theta(x;\mathscr{O}) = \sum_{z\in\mathscr{O}}\exp(-\pi\langle |z|^2, x\rangle)$$

for $x \in (\mathbb{R}^+)^{r_1+r_2}$ and $\langle x,y\rangle = \sum_\nu d_\nu x_\nu y_\nu$, and $|z|^2 = (|z|_\nu^2)_\nu$. It is this $\Theta$ which can be analyzed using the Poisson summation formula to obtain a functional equation.

## 7. Lecture 7, Matej Penciak, 8/13

sec:lect7

The goal of this lecture is to arrive at a formulation for class field theory for local fields. We'll see that historically this first came via the global formulation, but we will end at a truly local definition that can be used to re-derive global class field theory via a local-to-global analysis. In this lecture I'm largely following the historical development in history_of_cft [Con], in particular sections 7 and 8.

First we begin by casting quadratic reciprocity in a new light. For $a, b \in \mathbb{Q}_v^\times$ introduce the *Hilbert symbol*:

$$(a,b)_v = \begin{cases} 1 & \text{if } a = x^2 - by^2 \text{ has a solution in } \mathbb{Q}_v^\times \\ -1 & \text{else} \end{cases}$$

Note that equivalently $(a,b)_v = 1$ when $ax^2+by^2 = z^2$ has a solution in $\mathbb{Z}_v$. The Hilbert symbol is eminently generalizable to more settings outside the context of quadratic reciprocity or even reciprocity theorems in general. For example, this is an example of a Steinberg symbol (a consequence of the properties stated below), and is part of Matsumoto's computations of $K_2$ for fields.

The Hilbert symbol satisfies the following properties:

$$\begin{aligned} (a,b)_v &= (b,a)_v \\ (a,-a)_v &= (a,1-a)_v = 1 \\ (aa',b)_v &= (a,b)_v(a',b)_v. \end{aligned}$$

The first two properties are more or less obvious from the definition, but the last property is by no means clear. The proof relies on a clever application of Hensel's lemma and some basic principles of arithmetic geometry. The next property is in fact equivalent to Quadratic reciprocity: For every $a, b$ in $\mathbb{Q}_v$

$$\prod_v (a,b)_v = 1.$$

In fact, from the definition it is possible to nail down the exact expression for $(a,b)_v$, for any inputs $a$ and $b$. Quadratic reciprocity then follows from the following calculations. First, it can be shown that for odd primes $p$ and $q$, $p \neq q$, the Hilbert symbol $(a,b)_v = 1$ for all $v \neq 2, p, q, \infty$. Finally, quadratic reciprocity then follows from the explicit calculations

$$\begin{aligned} (p,q)_2 &= (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \\ (p,q)_\infty &= 1 \\ (p,q)_q &= \left(\frac{p}{q}\right) \end{aligned}$$

The upside to this formulation of quadratic reciprocity is that:

- All the places are taken on an equal footing
- We can rephrase the value of the symbol $(a,b)_v$ in terms of the solvability of $a = \mathrm{Nm}_L(\beta)$ for some $\beta \in L = \mathbb{Q}(\sqrt{b})$. This gets us close to Artin reciprocity, as the reciprocity map's kernel is exactly the norms of elements coming from field extensions.

In fact, continuing on the the logic from the second item above, we can view $(a,b)_q$ as a map:

$$\mathbb{Q}_q(\sqrt{b})^*/\left(\mathbb{Q}_q(\sqrt{b})^*\right)^2 \longrightarrow \{\pm 1\} = \mathrm{Gal}\left(\mathbb{Q}_q(\sqrt{b})/\mathbb{Q}_q\right).$$

So the Hilbert symbol plays the role of some sort of *Local Artin Map* (or the inverse of it). In fact, this is exactly generalized in the following way

**Definition 7.** Let $L/K$ be an abelian extension and $\alpha \in K^\times$, and $\nu$ a place in $K$. Define $(\alpha, L/K)_\nu$ via the following procedure:

Choose an isomorphism

$$\mathrm{Gal}\,(L/K) \overset{(-,L/K)_{\mathfrak{m}}}{\longleftrightarrow} I^{S(\mathfrak{m})}/R^{S(\mathfrak{m})}$$

for some choice of modulus $\mathfrak{m}$.

When $\nu$ is finite, choose $\alpha_0 \in K^\times$ such that:

(1) $\mathrm{ord}_\nu\left(\frac{\alpha_0}{\alpha} - 1\right) \geq \mathrm{ord}_\nu(\mathfrak{m})$ if $\nu \in \mathfrak{m}$
(2) $\gcd(\frac{\alpha_0}{\alpha}, \nu) = 1$ if $\nu \notin \mathfrak{m}$
(3) $\mathrm{ord}_\omega(\alpha_0 - 1) \geq \mathrm{ord}_\omega(\mathfrak{m})$ for $\omega$ finite not equal to $\nu$ in the support of $\mathfrak{m}$.
(4) $u(\alpha_0) > 0$ for real $u$ in the support of $\mathfrak{m}$.

Factor $\alpha_0$ into a product of primes, and let $\mathfrak{a}$ be the $\mathfrak{m}$-coprime part. Define

$$(\alpha, L/K)_\nu = (\mathfrak{a}, L/K)_{\mathfrak{m}}^{-1}.$$

When $\nu$ is infinite, let $(\alpha, L/K)_\nu$ be complex conjugation if

(1) $K_\nu$ is real.
(2) $L_\nu/K_\nu$ is a complex extension.
(3) $\alpha < 0$.

Otherwise let $(\alpha, L/K)_\nu$ be the identity.

This is a complicated procedure to calculate the Artin symbol, but lets do some examples to see how it's not so bad.

*Example* 8. Lets calculate $(-1, \mathbb{Q}(i)/\mathbb{Q})_\nu$ for various places $\nu$: Choose the modulus $\mathfrak{m} = 4\infty$. With this modulus, we are identifying the Ray class group with the units in $\mathbb{Z}/4\mathbb{Z}$, which we can write as $\{\pm 1\}$. First:

$$(-1, \mathbb{Q}(i)/\mathbb{Q})_\infty = -1 \text{ (complex conjugation)}$$

because $-1 < 0$. Next, to calculate $(-1, \mathbb{Q}(i)/\mathbb{Q})_2$ we need to choose an $\alpha_0$ such that $\mathrm{ord}_2(\frac{\alpha_0}{-1} - 1) \geq 2$, and $\alpha_0 > 0$ (there is no additional condition 2 from above because the only finite place in the support of $\mathfrak{m}$ is 2) It's easy to see 3 will exactly satiisfy this property, so

$$(-1, \mathbb{Q}(i)/\mathbb{Q})_2 = (\mathrm{Frob}_3)^{-1} = -1.$$

For any odd prime $p$, to calculate $(-1, \mathbb{Q}(i)/\mathbb{Q})_p$ we want an $\alpha_0$ so that:

(1) $\gcd\left(\frac{\alpha_0}{-1}, p\right) = 1$
(2) $\mathrm{ord}_2(\alpha_0 - 1) \geq 2$
(3) $\alpha_0 > 0$.

We can simply take $\alpha_0 = 1$, which yields the identity so

$$(-1, \mathbb{Q}(i)/\mathbb{Q})_p = 1$$

for odd $p$.

We can also calculate $(3, \mathbb{Q}(i)/\mathbb{Q})_v$ in the same way:

$$(3, \mathbb{Q}(i)/\mathbb{Q})_\infty = 1$$

because $3 > 0$. Next, in order to calculate $(3, \mathbb{Q}(i)/\mathbb{Q})_2$ we need to find an $\alpha_0$ such that $\alpha_0 > 0$ and $\mathrm{ord}_2(\alpha_0/3 - 1) \geq 2$. I think the smallest $\alpha_0$ we can choose is 27, in which case

$$(3, \mathbb{Q}(i)/\mathbb{Q})_2 = (\mathrm{Frob}_3)^3 = -1.$$

And finally, $(3, \mathbb{Q}(i)/\mathbb{Q})_3$ we need an $\alpha_0 > 0$ with $\mathrm{ord}_2(\alpha_0 - 1) \geq 2$ and $\gcd(\frac{\alpha_0}{3}, 3) = 1$. $\alpha_0 = 39$ works, and we see that

$$(3, \mathbb{Q}(i)/\mathbb{Q})_3 = \mathrm{Frob}_3 \cdot \mathrm{Frob}_{13} = \left(\frac{-1}{3}\right)\left(\frac{-1}{13}\right) = -1 \cdot -1 = 1$$

From these examples we see that the "yoga" to find the Artin symbol is that we want to find an $\alpha_0$ clsoe to $\alpha$ at $v$, and close to 1 at the other places of $\mathfrak{m}$. Then use the Frobenius of the $\mathfrak{m}$-coprime part.

In general, if $\mathfrak{p} \nmid \mathfrak{m}$ then for $\alpha \in K^\times$, let $k = \mathrm{ord}_\mathfrak{p}(\alpha)$. It's "easy" to show that $(\alpha, L/K)_\mathfrak{p} = \mathrm{Frob}_p(L/K)^k$. The only complicated primes to calculate the Artin symbol are the ramified primes, which is as expected.

Also note that $(\alpha, L/K)_v = 1$ for $v \nmid \mathfrak{m}$ and $\mathrm{ord}_\mathfrak{p}(\alpha) = 0$, hence only finitely many of the symbols are not equal to 1. So the following theorem makes sense.

**Theorem 10.** *The following product formula holds:*

$$\prod_v (\alpha, L/K)_v = 1$$

Now we will address the clear downside to this approach to the local Artin symbol: We first need to choose a modulus, use global class field theory, and only then can we calculate it. Our overall goal is to first understand local Artin reciprocity, which is easier to state (and should be easier to prove). Only then do we want to derive global Artin reciprocity.

The next perspective on the local Artin symbol comes closer to this goal, but still falls short as we will see:

Let $E/F$ be an abelian extension of local fields, and identify $F = K_v$ for some global field $K$ and place $v$ (this is the bad part!). It can be shown that $E = LK_v$ for some abelian extension $L/K$ (though $[L : K]$ will not in general equal $[E : F]$!).

For $\alpha \in K^\times$, define $(\alpha, E/F)$ to be $(\alpha, L/K)_v$. This defines a map

$$K^\times \longrightarrow \mathrm{Gal}(E/F)$$

which is $v$-adically locally constent, and hence it extends to a map on $K_v^\times = F^\times$. Hence yielding the local Artin symbol

$$(-, E/F) : F^\times \longrightarrow \mathrm{Gal}(E/F).$$

It can be shown that the definition is independent of the choices of $L$ and $K$ via the functoriality of global class field theory. The following analogue of global class field theory can also be shown:

**Theorem 11.** *The local artin map $\alpha \mapsto (\alpha, E/F)$ is surjective on its image $\mathrm{Gal}(E/F)$ with kernel $\mathrm{Nm}_F^E(E^\times)$.*

*Furthermore the image of $\mathcal{O}_F^\times$ is the inertial group $I(E/F)$ so that*

$$e(E/F) = [\mathcal{O}_F^\times \mathrm{Nm}_F^E(E^\times) : \mathrm{Nm}_F^E(E^\times)] = [\mathcal{O}_F^\times : \mathrm{Nm}_F^E(\mathcal{O}_E^\times)]$$

*and*

$$f(E/F) = \frac{[E:F]}{e(E/F)} = [F^\times : \mathcal{O}_F^\times \operatorname{Nm}_F^E(E^\times)]$$

All of Takagi's theorems on global class field theory also have their local analogues, though the exact definition of the conductor is more complicated.

Moving on we now provide a totally local description of the Artin map, and hence local class field theory. If $E/F$ is unramified, it is easy to define the Artin map in terms of the Frobenius element. So we're essentially left, as usual, with dealing with ramified extensions.

As we will see in the next lecture, a modern formulation of class field theory begins with a study of group cohomology. The cohomology groups in equestion can be viewed as Brauer groups describing $K$-algebras, and these $K$-algebras are precisely given below:

**Definition 8.** Let $L/K$ be a cyclic extension of degree $n$, $\alpha \in K^\times$, and $\sigma \in \operatorname{Gal}(L/K)$ a generator. Define the $K$-algebra $A$ which is equal to the vector space

$$A = L \oplus Lx \oplus Lx^2 \oplus \ldots \oplus Lx^{n-1}$$

with the product defined as

$$x^n = \alpha$$
$$x\gamma = \sigma(\gamma)x \quad \text{for } \gamma \in L$$

We call $A$ a *cyclic algebra* over $K$. We will denote $A$ as $(L/K, \sigma, \alpha)$.

*Example* 9. Take the extension $\mathbb{C}/\mathbb{R}$, and let $c$ be complex conjugation. Then for $\alpha > 0$ and $\alpha < 0$ all the algebras are isomorphic by scaling to the cases when $\alpha = \pm 1$. These two algebras are:

- $(\mathbb{C}/\mathbb{R}, c, -1) \cong \mathbb{H}$
- $(\mathbb{C}/\mathbb{R}, c, 1) \cong \operatorname{Mat}_{2\times 2}(\mathbb{R})$

The main theorem describing the structure of cyclic algebras of use to us is the following:

**Theorem 12.** *Let $L/K$, $\alpha$, and $\sigma$ be as above.*

*(1) $(L/K, \sigma, \alpha)$ is a simple $K$-algebra with center $K$, amd $\dim_K = n^2$.*
*(2) $(L/K, \sigma, 1) \cong \operatorname{Mat}_{2\times 2}(K)$ as a $K$-algebra.*
*(3) $(L/K, \sigma, \alpha) \cong (L/K, \sigma, \beta)$ if and only if $\alpha/\beta \in \operatorname{Nm}_K^L(L^\times)$*
*(4) For $\gcd(t, n) = 1$, we if $tu \equiv 1 \mod n$ then*

$$(L/K, \sigma^t, \alpha) \cong (L/K, \sigma, \alpha^u)$$

*Remark* 8. Note the appearance of the norm in part (3) of the above theorem! This is a first hint that these cyclic algebras may be helpful in describing local class field theory.

In the special case when $K$ is a local field we have the following classification result which will be integral to stating class field theory:

**Theorem 13.** *Every cyclic algebra over a local field $F$ of characteristic $0$ with dimension $n^2$ is of the form*

$$(F_n/F, \operatorname{Frob}, \pi^a)$$

*with $F_n/F$ an unramified extension of degree n, $\pi$ a uniformizer of the maximal ideal of $\mathcal{O}_F$ and $a \in \mathbb{Z}$.*

With this above theorem we are now prepared to define the Artin map: $\mathrm{Nm}_F^{F_n}(F_n^\times)$ is isomorphic to $\pi^{n\mathbb{Z}} \times \mathcal{O}_F^\times$ since $F_n/F$ is unramified, so we can conclude:

(1) $(F_n/F, \mathrm{Frob}, \pi^a) \cong (F_n/F, \mathrm{Frob}, \pi^b)$ if and only if $a \equiv b \mod n$. (part 3 above, and knowing the norm map

(2) $(F_n/F, \mathrm{Frob}, \pi^a)$ is independent of the choice of uniformizer $\pi$. (part 3 again, and any two uniformizers differ by a unit in the image of the norm map)

So the number $a \mod n$ is an *invariant* of the cyclic algebra.

For $E/F$ cyclic, consider $A = (E/F, \sigma, \alpha)$ with invariant $a \mod n$. Define the local Artin symbol of the extension $E/F$ as:

$$(\alpha, E/F) = \sigma^a.$$

Note that as we change the generator $\sigma$ of $\mathrm{Gal}(E/F)$, the invariant $a$ will also change and the quantity $\sigma^a$ is independent of our choices.

When $E/F$ is a general abelian extension, we can write $E = E_1 \cdots E_r$ with each $E_i/F$ cyclic, and we can can bootstrap up to general abelian extensions.

This is our desired local description of the Artin map. We end this section with a computation of the local Artin symbol in the cases we already know the answer in terms of our new definition:

*Example* 10. Let us first compute $(-1, \mathbb{Q}(i)/\mathbb{Q})_v$ again: In this case $n = [\mathbb{Q}(i) : \mathbb{Q}] = 2$, and $\sigma = -1$ is the generator of $\{\pm 1\}$. So the local Artin symbol will simply be $(-1)^a$, where $a$ is the invariant of the cyclic algebras constructed below. These are computed as follows:

The algebra $(\mathbb{Q}(i)/\mathbb{Q}, \sigma, -1)$ is $\mathbb{H}_{\mathbb{Q}}$ and it's easy to see that $\mathbb{Q}_v \otimes_{\mathbb{Q}} \mathbb{H}_{\mathbb{Q}} \cong \mathbb{H}_{\mathbb{Q}_v}$.

So when $v = \infty$, we get the cyclic algebra $\mathbb{H}_{\mathbb{R}}$. Another way of describing this same cyclic algebra is as $(\mathbb{C}/RR, c, -1)$ which we already computed, and its invariant is $1 \mod 2$.

For the place $v = 2$, we are interested in

$$\mathbb{H}_{\mathbb{Q}_2} = (\mathbb{Q}_2(i)/\mathbb{Q}_2, c, -1)$$

But the extension $\mathbb{Q}_2(i)/\mathbb{Q}_2$ is *ramified*, so this is not an appropriate description to calculate the invariant. One can show that a good replacement is:

$$\mathbb{H}_{\mathbb{Q}_2} \cong (\mathbb{Q}_2(\sqrt{-3})/\mathbb{Q}, c, 2)$$

which is unramified with invariant $1 \mod 2$.

Finally, for odd primes $p$, we can always solve $-1 \equiv x^2 + y^2 \mod p$ and hence $-1$ is a sum of squares in $\mathbb{Q}_p$ by Hensel's lemma. Therefore

$$\mathbb{H}_{\mathbb{Q}_p} \cong \mathrm{Mat}_{2\times 2}(\mathbb{Q}_p) = (\mathbb{Q}_p(i)/\mathbb{Q}_p, c, 1)$$

and hence the invariant is $0 \mod 2$. Hence in this case we recover what we had before.

## 8. Lecture 8, Matej Penciak, 8/18

sec:lect8

In this lecture we will give a modern formulation of class field theory that starts first with *local* class field theory, and then derives the global reciprocity map out of it. This local-to-global process is governed by the algebraic object we will introduce known as the adéles and idéles. We start though with some abstract nonsense about group cohomology. Note the following development of class field theory is common between a number of different sources, but we are most closely following Kedlaya's online textbook kedlaya_book [Ked]

Let $G$ be a finite group, and $M$ a $G$-module. Let $H^i(G;M)$ be the right derived functors of the left-exact $M^G$ (invariants), and $H_i(G;M)$ the left derived functors of the right-exact $M_G = M/\{gm - m | g \in G, m \in M\}$ (coinvariants). We can define the norm map from coinvariants to invariants by:

$$\begin{aligned} \mathrm{Nm}_G : M_G &\longrightarrow M^G \\ m &\mapsto \sum_{g \in G} g \cdot m \end{aligned}$$

Given a short exact sequence of $G$-modules $0 \to M' \to M \to M'' \to 0$, the norm map allows us to piece together the long exact sequences in cohomology and in homology:

This is not right, but I'm too tired to actually write the correct LES (copy the one below and plug in the definitions)

$$\ldots \to H_1(G;M') \longrightarrow \frac{\ker \mathrm{Nm}_G}{I_G} \longrightarrow \frac{M''^G}{\mathrm{Nm}_G M''} \longrightarrow H^1(H;M') \to \ldots$$

So if we define the Tate cohomology groups as

$$H_T^i(G;M) = \begin{cases} H_{-i-1}(G;M) & i < -1 \\ \ker \mathrm{Nm}_G / I_G & i = -1 \\ M^G / \mathrm{Nm}_G M & i = 0 \\ H^i(G;M) & i > 0 \end{cases}$$

Then the above bi-infinite long exact sequence can be written as

$$\ldots \to H_T^{i-1}(G, M'') \to H_T^i(G;M') \to H_T^i(G;M) \to H_T^i(G, M'') \to \ldots$$

With this notation, the fundamental result of "abstract class field theory" is that there is a functorial isomorphism

$$H_T^i(G;M) \cong H_T^{i+2}(G;M)$$

for cyclic groups $G$. (more generally, for groups satisfying $H^1(H,M) = 0$ and $\#H^2(H,M) = \#H$ for all subgroups $H$ of $G$).

Once this abstract form of class field theory is derived in general, the concrete statements of local class field theory follow from the calculations that

$$\#H_T^0(\mathrm{Gal}(L/K); L^\times) = [L : K]$$

and

$$\#H_T^{-1}(\mathrm{Gal}(L/K), L^\times) = 1.$$

These are equivalent to the first and second fundamental inequalities that we considered as classical motivation for class field theory in lecture 4. In fact, there is a certain poetry in the fact that the key number theoretic insight in this modern formulation of class field theory comes from fundamental inequalities considered in the 19th century perspective on class field theory.

Having established these inequalities, we can define the local Artin map as coming from the above functorial isomorphism for a local field extension $L/K$:

$$\begin{aligned} H_T^0(\mathrm{Gal}(L/K); L^\times) &\xrightarrow{\sim} H_T^{-2}(\mathrm{Gal}(L/K), L^\times) \\ K^\times / \mathrm{Nm}\, L^\times &\xrightarrow{\sim} H_1(\mathrm{Gal}(L/K), L^\times) \cong \mathrm{Gal}(L/K)^{ab} \end{aligned}$$

Having established local class field theory, the way we glue it all together to global class field theory is via the introduction of the ring of Adéles.

First, the ring of finite adeles $\mathbb{A}_K^{fin}$ for a global field $K$ is defined in any of the following equivalent ways:

(1) $\widehat{\mathscr{O}_K} \otimes_{\mathscr{O}_K} K$
(2) $\varinjlim_{\alpha} \dfrac{1}{\alpha}\widehat{\mathscr{O}_K}$
(3) The "restricted product" $\prod'_{\substack{\mathfrak{p} \text{ finite} \\ \text{place}}} K_{\mathfrak{p}}$ where all but finitely many components are in $\mathscr{O}_{K_{\mathfrak{p}}}$.

These three definitions translate to the following three well-known descriptions of the rational adéles:

(1) $\widehat{\mathbb{Z}} \otimes_{\mathbb{Z}} \mathbb{Q}$
(2) $\varinjlim_{n} \dfrac{1}{n}\widehat{\mathbb{Z}}$
(3) The restricted product $\prod'_{p} \mathbb{Q}_p$ where all but finitely many components are in $\mathbb{Z}_p$.

The full ring of adéles has an additional factor for the completions at real infinite places: $\mathbb{A}_K = \mathbb{A}_K^{fin} \times (K \otimes_{\mathbb{Q}} \mathbb{R})$.

There are many embeddings of $K$ into its ring of adéles. There is one for each place $K \hookrightarrow K_v \hookrightarrow \mathbb{A}_K$, and also a diagonal embedding $K \overset{\Delta}{\hookrightarrow} \mathbb{A}_K$. We endow $\mathbb{A}_K$ with the structure of a topological ring with the $\frac{1}{\alpha}\widehat{\mathscr{O}_K}$ serving as a fundamental system of open neighborhoods of 0. The two kinds of the inclusions above endow $K$ with a topology inherited as a subspace, and the topologies will coincide with the $v$-adic and discrete topologies for each kind of inclusion respectively.

An equivalent formulation for the topology on $\mathbb{A}$ is given by the description of open sets: All open sets are of the form $\prod U_i \times \prod \mathscr{O}_v$ where $U_i \subseteq K_{v_i}$ are open sets, and the first product is over a finite subset of places.

We can also define the *adelic $S$-integers* for $S$ a finite set of places: $\mathbb{A}_{K,S} \subseteq \mathbb{A}_K$ where the elements are integral outside the set $S$. We can also define the function $|\cdot|_K : \mathbb{A}_K \to \mathbb{R}$ built out of the $v$-adic valuations

$$|x|_K = \prod_v |x|_v.$$

The product formula implies that $|\alpha|_K = 1$ for all $\alpha \in K \subseteq \mathbb{A}_K$ via the diagonal embedding.

**Proposition 2.** *Let $K$ be a global field and $\mathbb{A}_K$ its ring of adeles.*

*(1) The image of $K$ in $\mathbb{A}_K$ via the diagonal embedding is discrete.*
*(2) $\mathbb{A}_K/K$ is compact. (making $K \subseteq \mathbb{A}_K$ a discrete lattice)*
*(3) Let $S$ be a finite set of places, and $U_v$ be an open set in $K_v$ for every place $v \in S$. Then $K \cap (\bigcap_{v\in S} U_v) \neq \emptyset$. (compare this to the approximation theorem)*

Now we define the idéles: It is given by the restricted product $\prod' K_v$ where all but finitely many components are in $\mathscr{O}_{K_v}^{\times}$. Denote the set of Ideles as $\mathbb{I}_K$. Note that $\mathbb{I}_K \hookrightarrow \mathbb{A}_K$ set-theoretically, but $\mathbb{I}_K$ does not inherit its topology as a subset of $\mathbb{A}_K$. It is better to think of $\mathbb{I}_K = \mathrm{GL}_1(\mathbb{A}_K)$. (in fact, if we embed $\mathbb{I}_K \subseteq \mathbb{A}_K \times \mathbb{A}_K$ via $t \mapsto (t, t^{-1})$, then the topologies match up.)

Define the *idéle class group* as $C_K = \mathbb{I}_K / K^\times$. The relation to our previous notion of class group and ray-class group is as follows: Given a modulus $\mathfrak{m}$, we can define a subgroup of $\mathbb{I}_K$ given by tuples $(\alpha_\nu)_\nu$ where

(1) $\alpha_\nu > 0$ if $\nu \in \mathfrak{m}$ and $\nu$ is real.
(2) $\alpha_\nu \equiv 1 \mod \mathfrak{p}^e$ where $\mathfrak{p}^e \| \mathfrak{m}$ (divides exactly).

Such a subgroup of $\mathbb{I}_K$ is *open*, and its quotient is isomorphic to the ray class group $C_\mathfrak{m}$. In this way we see that $\mathbb{I}_K$ is a universal object that parametrizes between all of the ray class groups.

The function $|\cdot|_K$ on $\mathbb{A}_K$ from before can be further defined on $\mathbb{I}_K$, and by the product formula it descends to a function on the idéle class group $C_K$. The following is a major theorem on the idéle class group that can be proved independently, but implies many of the fundamental finiteness theorems in classical algebraic number theory. For example, the theorem below implies that $\mathrm{Cl}(K)$ is finite, and the Dirichlet unit theorem that states the units in $\mathcal{O}_K$ form an abelian group with free part of finite rank $r_1 + r_2 - 1$ (as we had seen before).

**Theorem 14.** *Let $C_K^\circ$ be the kernel of $|\cdot|_K : C_K \to \mathbb{R}^\times$. Then $C_K^\circ$ is compact.*

Finally, after having built up the machinery of adéles and idéles, we return to class field theory at the end of this lecture. Having established the above local form of Artin reciprocity we can now turn to the global picture. Let $L/K$ be a field extension, then this field extension defines an embedding $\mathbb{A}_K \hookrightarrow \mathbb{A}_L$ (inducing $\mathbb{I}_K \hookrightarrow \mathbb{I}_L$). We also get the "wrong-way maps":

$$\mathrm{Tr}_K^L : \mathbb{A}_L \longrightarrow \mathbb{A}_K$$
$$\mathrm{Nm}_K^L : \mathbb{A}_L \longrightarrow \mathbb{A}_K$$

defined in terms of the trace and the norm coming from the field extension $L/K$ and all of its completions $L_\omega/K_\nu$ for a place $\omega$ of $L$ over $\nu$.

The norm map on $\mathbb{A}_L$ preserves the idéles and the diagonal, so it defines a map

$$\mathrm{Nm}_K^L : C_L \longrightarrow C_K$$

The final statements of class field theory can be stated in this language as:

**Theorem 15.** *Let $K$ be a global field.*

*(1) There is a map*
$$r_K : C_K \longrightarrow \mathrm{Gal}(K^{ab}/K)$$
*which induces an isomorphism for each extension $L/K$:*
$$r_{L/K} : C_K/\mathrm{Nm}_K^L(C_L) \xrightarrow{\sim} \mathrm{Gal}(L/K)^{ab}$$

*(2) For every open subgroup $H \subseteq C_K$, of finite index, there is an abelian extension $L/K$ with $H = \mathrm{Nm}_K^L C_L$.*

*(3) The map $r_K$ is induced by the map*
$$\widetilde{r}_K : \mathbb{I}_K \longrightarrow \mathrm{Gal}(L/K)$$
*defined by*
$$\widetilde{r}_K\left((\alpha_\nu)_\nu\right) = \prod_{\nu \text{ finite}} (\alpha_\nu, L/K)_\nu \cdot \prod_{\nu \text{ real}} \mathrm{sgn}(\alpha_\nu)$$

*where each $(\alpha_v, L/K)_v$ is the local Artin symbol at place $v$.*

Note the structure of this theorem, and compare it to the goals Brian layed out in the first lecture where our definition of "arithmetic of $K$" should be expanded to include the idéle class group $C_K$.

*Remark* 9.
(1) The first goal of classifying finite abelian extensions of $K$ in terms of the arithmetic of $K$ is achieved by part (2) of the theorem. We can now say that the finite abelian extensions are in one to one correspondence with finite index open subgroups of $C_K$. Recalling the classification stated above that open subgroups of $C_K$ are classified by a choice of modulus $\mathfrak{m}$, we see this part is equivalent to the existence and completeness parts of Takagi's statements of class field theory.

    This part is similar to the corresponding statements in infinite Galois theory about open subgroups of the absolute Galois group. In fact, one of the original motivations for the adéles and idéles was in the study of *infinite* class field theory, and it was only later that its applications to global class field theory were spelled out.
(2) Part (1) of the theorem can now be seen as a realization of the Galois group $\mathrm{Gal}(L/K)$ in terms of the arithmetic of $K$.
(3) To achieve the third goal of describing the decomposition of primes in abelian extensions, we need an explicit description of the isomorphism $r_K$. We see this follows from the definition of the reciprocity map $\widetilde{r}_K$as coming from the local Artin symbols, and their definitions in terms of Frobenius elements (at least in the unramified cases).

We also end this lecture with a look ahead at the lectures to come.

(1) The adélic language offers a natural path to move from arithmetic of number fields to the geometry of Riemann surfaces. We will see what a *geometric* class field theory should look like.
(2) Finally, it behooves us to describe the relation between the $L$-function theoretic statements of class field theory and the adélic perspective. We will get in this direction by looking at adélic L-functions, which we will begin with next time in the context of Tate's thesis.
(3) At this point we are very close to writing down a formulation of class field theory that is what is generalized to non-Abelian extensions in the context conjectures in the Langlands program.

## 9. Lecture 9, Matej Penciak, 10/??

sec:lect9

The goal of this lecture is to treat Tate's thesis.

## References


[Con] Keith Conrad. History of class field theory. URL: http://virtualmath1.stanford.edu/~conrad/249BW09Page/handouts/cfthistory.pdf.

[Gar] Paul Garrett. Analytic continuation, functional equation: examples. URL: http://www-users.math.umn.edu/~garrett/m/mfms/notes_c/analytic_continuations.pdf.

[Gar81] Dennis Garbanati. Class field theory summarized. *Rocky Mountain J. Math.*, 11(2):195–225, 1981. URL: https://doi-org.ezproxy.neu.edu/10.1216/RMJ-1981-11-2-195, doi:10.1216/RMJ-1981-11-2-195.

[Ked] Kiran S. Kedlaya. Notes on class field theory. URL: https://kskedlaya.org/cft/.

[Kow] Emmanuel Kowalski. Automorphic forms, l-functions and number theory: Three introductory lectures. URL: `https://people.math.ethz.ch/~kowalski/lectures.pdf`.

[Min] M. W. Mintjes. The proof of dirichlet's theorem on arithmetic progressions and its variations. URL: `https://fse.studenttheses.ub.rug.nl/17834/1/bMATH_2018_MintjesMW.pdf`.

[Neu99] Jürgen Neukirch. *Algebraic number theory*, volume 322 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1999. Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder. URL: `https://doi-org.ezproxy.neu.edu/10.1007/978-3-662-03983-0`, `doi:10.1007/978-3-662-03983-0`.