

Part III - Algebraic Number Theory

Lectured by Hanneke Wiersema

Artur Avameri

Contents

0	Introduction	2
0.1	Rough goals of class field theory.	2
0.2	Review of basic Algebraic Number Theory	3
1	The Artin symbol	4
1.1	Reciprocity theorems	18

0 Introduction

19 Jan 2024,

The lecturer will provide typed notes at the end of the course. The topics of the course are

Lecture 1

- global class field theory;
 - both ideal-theoretic and idele-theoretic.
- zeta functions;
- L -series;
- density theorems.

0.1 Rough goals of class field theory.

- (1) Given a number field K , what are its abelian extensions? If $K = \mathbb{Q}$, we have the Kronecker–Weber theorem (which we will prove): Every finite abelian extension of \mathbb{Q} is contained in some cyclotomic field, i.e. by adjoining a complex root of unity to \mathbb{Q} . We write $\mathbb{Q}(\zeta_n)$ for $\zeta_n = e^{2\pi i/n}$.

Finite abelian extensions of \mathbb{Q} can be generated by special values of the exponential function $e^{2\pi iz}$. It is an open problem to explicitly construct all abelian extensions for arbitrary number fields. Kronecker solved the case of imaginary quadratic fields using special values of analytic functions (elliptic and modular functions).

In class field theory, we classify extensions introducing the notion of a **class field**: for any K we will show that any finite abelian extension will be contained in a class field. Moreover, the Galois group of this extension will be isomorphic to the generalized ideal class group (in the ideal case) or a subgroup of the Idele class group (in the idele case).

- (2) Given a finite abelian extension, how do the prime ideals in the smaller field behave in the extension? In the quadratic case, we will prove quadratic reciprocity. There exist higher reciprocity laws. The most general answer we will see is the decomposition law, which is a consequence of the Artin reciprocity theorem.

Warning. There is no one convention for the notation for many objects – different textbooks may use different notation.

0.2 Review of basic Algebraic Number Theory

Let K be a number field and write \mathcal{O}_K for its ring of integers. This is a Dedekind domain, so any ideal has a unique factorization into a product of prime ideals. Let L/K be an extension of number fields and \mathfrak{p} a prime ideal of K . Then $\mathfrak{p}\mathcal{O}_L$ is an ideal of L and by unique factorization $\mathfrak{p}\mathcal{O}_L = \mathcal{P}_1^{e_1} \dots \mathcal{P}_g^{e_g}$ with \mathcal{P}_i distinct prime ideals in \mathcal{O}_L . Write $\mathcal{P}_i \mid \mathfrak{p}$ to mean that \mathcal{P}_i appears in the factorization of \mathcal{O}_L . The number e_i is called the ramification index $\mathcal{P}_i/\mathfrak{p}$. We also write $e_i = e_{\mathcal{P}_i/\mathfrak{p}}$.

- If $e_i = 1$ for all i , we say \mathfrak{p} is unramified in L .
- If $e_i > 1$ for some i , we say \mathfrak{p} is ramified.
- If there is a unique prime \mathcal{P} dividing \mathfrak{p} with $e_{\mathcal{P}/\mathfrak{p}} = [L : K]$, we say \mathfrak{p} is totally ramified.
- If $\mathfrak{p}\mathcal{O}_L$ is prime, we say \mathfrak{p} is inert (or remains inert) in L .
- If $g = [L : K]$, we say \mathfrak{p} splits completely.

The quotient $\mathcal{O}_K/\mathfrak{p}$ is a finite field of characteristic p ($\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$), called a residue field. If $\mathcal{P} \mid \mathfrak{p}$ (for $\mathcal{P} \in \mathcal{O}_L, \mathfrak{p} \in \mathcal{O}_K$), view $\mathcal{O}_K/\mathfrak{p}$ as a subfield of $\mathcal{O}_L/\mathcal{P}$. We call $f_{\mathcal{P}/\mathfrak{p}} = [\mathcal{O}_L/\mathcal{P} : \mathcal{O}_K/\mathfrak{p}]$ the residue field degree. If as before $\mathfrak{p}\mathcal{O}_L = \mathcal{P}_1^{e_1} \dots \mathcal{P}_g^{e_g}$, then $\sum_{i=1}^g e_{\mathcal{P}_i/\mathfrak{p}} f_{\mathcal{P}_i/\mathfrak{p}} = [L : K]$. If L/K is Galois, then the Galois group permutes the \mathcal{P}_i transitively, so $e_1 = \dots = e_g = e$. Also if L/K is Galois, $f_{\mathcal{P}_1/\mathfrak{p}} = \dots = f_{\mathcal{P}_g/\mathfrak{p}} = f$, so $efg = [L : K]$. Recall also that

- We can find the factorization of $\mathfrak{p}\mathcal{O}_L$ using the Kummer–Dedekind theorem.
- A prime \mathfrak{p} in \mathcal{O}_K ramifies in L/K if and only if $\mathfrak{p} \mid d_{L/K}$ for $d_{L/K}$ the discriminant.

If L/K is Galois, write $\text{Gal}(L/K)$ for the Galois group. Let \mathcal{P} be a prime ideal in \mathcal{O}_L .

Definition 0.1. The **decomposition subgroup** of \mathcal{P} is

$$D_{\mathcal{P}} = \{\sigma \in \text{Gal}(L/K) \mid \sigma(\mathcal{P}) = \mathcal{P}\}.$$

The **inertial subgroup** of \mathcal{P} is

$$I_{\mathcal{P}} = \{\sigma \in \text{Gal}(L/K) \mid \sigma(\alpha) \equiv \alpha \pmod{\mathcal{P}} \forall \alpha \in \mathcal{O}_L\}.$$

Remark. We have $I_{\mathcal{P}} \subset D_{\mathcal{P}}$. Easy exercise: show this.

Let $\sigma \in D_{\mathcal{P}}$. This induces an automorphism $\bar{\sigma} : \mathcal{O}_L/\mathcal{P} \rightarrow \mathcal{O}_L/\mathcal{P}$ such that $\bar{\sigma}|_{\mathcal{O}_K/\mathfrak{p}} = \text{Id}|_{\mathcal{O}_K/\mathfrak{p}}$ for $\mathfrak{p} = \mathcal{P} \cap \mathcal{O}_K$. This gives a map $D_{\mathcal{P}} \rightarrow \text{Gal}((\mathcal{O}_L/\mathcal{P})/(\mathcal{O}_K/\mathfrak{p}))$ by $\sigma \mapsto \bar{\sigma}$.

- Proposition 0.1.** (i) The Galois group $\text{Gal}((\mathcal{O}_L/\mathcal{P})/(\mathcal{O}_K/\mathfrak{p}))$ is a cyclic group with canonical generator the Frobenius automorphism $x \mapsto x^q$ for $q = |\mathcal{O}_K/\mathfrak{p}|$.
- (ii) The map $D_{\mathcal{P}} \xrightarrow{\sigma \mapsto \bar{\sigma}} \text{Gal}((\mathcal{O}_L/\mathcal{P})/(\mathcal{O}_K/\mathfrak{p}))$ defines a surjective homomorphism with kernel $I_{\mathcal{P}}$.
- (iii) $|I_{\mathcal{P}}| = e_{\mathcal{P}/\mathfrak{p}}$ and $|D_{\mathcal{P}}| = e_{\mathcal{P}/\mathfrak{p}} f_{\mathcal{P}/\mathfrak{p}}$.

Recall that if \mathfrak{p} is a prime in \mathcal{O}_K and \mathcal{P} is a prime in \mathcal{O}_L such that $\mathcal{P} \mid \mathfrak{p}$, then the norm of \mathcal{P} is $N_{L/K}(\mathcal{P}) = \mathfrak{p}^{f_{\mathcal{P}/\mathfrak{p}}}$. Note that if \mathfrak{p} is a prime of K , we also write $N(\mathfrak{p})$ for $N_{K/\mathbb{Q}}(\mathfrak{p})$ and $N(\mathfrak{p}) = |\mathcal{O}_K/\mathfrak{p}|$.

1 The Artin symbol

Lemma 1.1. Let L/K be a Galois extension and let \mathfrak{p} be a prime of \mathcal{O}_K , unramified in L . Suppose $\mathcal{P} \subset \mathcal{O}_L$ such that $\mathcal{P} \mid \mathfrak{p}$. Then there exists a unique element $\sigma \in \text{Gal}(L/K)$ such that for all $\alpha \in \mathcal{O}_L$,

$$\sigma(\alpha) \equiv \alpha^{N(\mathfrak{p})} \pmod{\mathcal{P}}.$$

Proof. Let $\sigma \in D_{\mathcal{P}}$ and $\bar{\sigma} \in \text{Gal}((\mathcal{O}_L/\mathcal{P})/(\mathcal{O}_K/\mathfrak{p}))$ its image under the map from Proposition 0.1. By assumption, \mathfrak{p} is unramified, so $|I_{\mathcal{P}}| = 1$, hence by Proposition 0.1 again, we have $D_{\mathcal{P}} \xrightarrow{(\star)} \text{Gal}((\mathcal{O}_L/\mathcal{P})/(\mathcal{O}_K/\mathfrak{p}))$. Recall that $\text{Gal}((\mathcal{O}_L/\mathcal{P})/(\mathcal{O}_K/\mathfrak{p}))$ is generated by $x \mapsto x^q$ for $q = |\mathcal{O}_K/\mathfrak{p}|$. Let $\sigma \in D_{\mathcal{P}}$ be the unique element in $D_{\mathcal{P}}$ which maps to the Frobenius under (\star) . Then $\sigma(\alpha) \equiv \alpha^q \pmod{\mathcal{P}}$ for all $\alpha \in \mathcal{O}_L$ and $q = |\mathcal{O}_K/\mathfrak{p}| = N(\mathfrak{p})$. Uniqueness follows since any $\sigma \in \text{Gal}(L/K)$ satisfying this condition will be an element of $D_{\mathcal{P}}$. \square

Definition 1.1. This unique element is called the **Artin symbol** and we denote it by $\left(\frac{L/K}{\mathcal{P}}\right)$.

Definition 1.2. Let p be an odd prime and let a be any integer. Recall that the

Legendre symbol is $\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a QR mod } p. \\ -1 & \text{if } a \text{ is not a QR mod } p. \\ 0 & \text{if } a \equiv 0 \pmod{p}. \end{cases}$ Now let $n \in \mathbb{Z}$

be nonzero and write $n = up_1^{k_1} \dots p_u^{r_u}$ for $u = \pm 1$. Again let a be an integer, then the **Kronecker symbol** is

$$\left(\frac{a}{n}\right) = \left(\frac{a}{u}\right) \prod_{i=1}^k \left(\frac{a}{p_i}\right)^{r_i}$$

22 Jan 2024,
Lecture 2

with $\left(\frac{a}{p_i}\right)$ the Legendre symbol for odd primes, $\left(\frac{a}{2}\right) = \begin{cases} 0 & a \equiv 0 \pmod{2} \\ 1 & a \equiv \pm 1 \pmod{8} \\ -1 & a \equiv \pm 3 \pmod{8} \end{cases}$

and $\left(\frac{a}{1}\right) = 1$, $\left(\frac{a}{-1}\right) = \begin{cases} -1 & a < 0 \\ 1 & a \geq 0. \end{cases}$

The quadratic case. Let $K = \mathbb{Q}$, $L = \mathbb{Q}(\sqrt{N})$ for $N \neq 0, 1$ squarefree. Recall that

$$d_{L/\mathbb{Q}} = \begin{cases} N & N \equiv 1 \pmod{4} \\ 4N & N \not\equiv 1 \pmod{4} \end{cases}$$

with

$$\mathcal{O}_L = \begin{cases} \mathbb{Z}\left[\frac{1+\sqrt{N}}{2}\right] & N \equiv 1 \pmod{4} \\ \mathbb{Z}[\sqrt{N}] & N \not\equiv 1 \pmod{4}. \end{cases}$$

Then $\text{Gal}(L/K)$ has order 2 with $1 : \sqrt{N} \rightarrow \sqrt{N}$ and $\sigma : \sqrt{N} \rightarrow -\sqrt{N}$ and we can identify $\text{Gal}(L/K)$ with $\{\pm 1\}$.

Let \mathfrak{p} be unramified in L and $\mathcal{P} \subset \mathcal{O}_L$ a prime lying above it (so $\mathcal{P} \mid \mathfrak{p}$). We then get $\sigma(\alpha) \equiv \alpha^{\mathfrak{p}} \pmod{\mathcal{P}}$ for all $\alpha \in \mathcal{O}_L$. We have

$$\left(\frac{L/K}{\mathfrak{p}}\right) = \left(\frac{\mathbb{Q}(\sqrt{N})/\mathbb{Q}}{\mathcal{P}}\right) = \left(\frac{d_{L/\mathbb{Q}}}{p}\right) = \pm 1$$

since $p \nmid d_{L/\mathbb{Q}}$ (more on this on Ex. Sheet 1).

Proposition 1.2. Suppose p is unramified in L . Then p splits in L if and only if $\left(\frac{d_{L/\mathbb{Q}}}{p}\right) = 1$.

The Artin symbol tells us about the decomposition, but more generally:

Lemma 1.3. Let L/K be any Galois extension. Let $\mathfrak{p} \subset \mathcal{O}_K$ be unramified with $\mathcal{P} \subset \mathcal{O}_L$ lying above it. Then:

- (i) Let $\sigma \in \text{Gal}(L/K)$. Then $\sigma\left(\frac{L/K}{\mathcal{P}}\right)\sigma^{-1} = \left(\frac{L/K}{\sigma(\mathcal{P})}\right)$.
- (ii) The order of $\left(\frac{L/K}{\mathcal{P}}\right)$ is the residue field degree $f = f_{\mathcal{P}/\mathfrak{p}}$.
- (iii) The prime \mathfrak{p} splits completely in L if and only if $\left(\frac{L/K}{\mathcal{P}}\right) = 1$ (i.e. the Artin map is trivial).

Proof. Exercise! □

Definition 1.3. In this course, we say L/K is an abelian extension if it is a Galois extension of number fields with abelian Galois group $\text{Gal}(L/K)$.

Suppose L/K is abelian and let $\mathfrak{p} \subset \mathcal{O}_K$ be unramified. Let $\mathcal{P}, \mathcal{P}' \subset \mathcal{O}_L$ be distinct prime ideals lying above \mathfrak{p} . Then $\mathcal{P}' = \sigma(\mathcal{P})$ for some $\sigma \in \text{Gal}(L/K)$. Since the group is abelian, we find

$$\left(\frac{L/K}{\mathcal{P}'} \right) = \left(\frac{L/K}{\sigma(\mathcal{P})} \right) = \sigma \left(\frac{L/K}{\mathcal{P}} \right) \sigma^{-1} = \left(\frac{L/K}{\mathcal{P}} \right).$$

Notation. If L/K is abelian, we also write $\left(\frac{L/K}{\mathfrak{p}} \right)$ for the Artin symbol for any $\mathcal{P} \mid \mathfrak{p}$. So for L/K abelian, the Artin symbol defines a map

$$\begin{aligned} \{\text{unramified primes } \mathfrak{p} \subset \mathcal{O}_K \text{ in } L\} &\rightarrow \text{Gal}(L/K) \\ \mathfrak{p} &\mapsto \left(\frac{L/K}{\mathfrak{p}} \right). \end{aligned}$$

We want to extend this map, for which we introduce fractional ideals. Quick review: recall that a **fractional ideal** of a number field K is a \mathcal{O}_K -submodule \mathfrak{a} of K such that there exists $0 \neq x \in \mathcal{O}_K$ such that $x\mathfrak{a} \subset \mathcal{O}_K$. Equivalently, it is a set of the form αI for $\alpha \in K$ and some ideal I of \mathcal{O}_K .

A principal fractional ideal is a \mathcal{O}_K -submodule generated by a single nonzero element of K . Since \mathcal{O}_K is a Dedekind domain, each fractional ideal is invertible and we obtain a group with identity \mathcal{O}_K .

Notation. Write I_K for the group of fractional ideals and P_K for the subgroup of principal fractional ideals. The quotient I_K/P_K is called the **ideal class group** $\text{Cl}(K)$, which is a finite abelian group with order h_K called the **class number** of K .

Recall that for any $\mathfrak{a} \in I_K$, we have unique factorization

$$\mathfrak{a} = \prod_{i=1}^n \mathfrak{p}_i^{r_i}, r_i \in \mathbb{Z}$$

with \mathfrak{p}_i distinct prime ideals in \mathcal{O}_K .

Definition 1.4. Suppose L/K is an abelian unramified extension (i.e. every prime in K is unramified in L). Then we define the **Artin map** to be the homomorphism

$$\left(\frac{L/K}{\cdot} \right) : I_K \rightarrow \text{Gal}(L/K)$$

by setting $\left(\frac{L/K}{\mathfrak{a}} \right) = \prod_{i=1}^n \left(\frac{L/K}{\mathfrak{p}_i} \right)^{r_i}$.

To define this more generally, we need to define **moduli**.

Interlude. Finite and infinite primes. Let K be a number field. Then a prime ideal is also called a finite prime to distinguish it from infinite primes.

Infinite primes are determined by the embeddings of K into \mathbb{C} . These correspond to archimedean absolute values (from local fields).

A real infinite prime is an embedding $\sigma : K \rightarrow \mathbb{R}$ and a complex infinite prime is a pair of conjugate embeddings $\sigma, \bar{\sigma} : K \rightarrow \mathbb{C}$ with $\sigma \neq \bar{\sigma}$.

Example 1.1. • \mathbb{Q} has one infinite real prime $\sigma\left(\frac{a}{b}\right) = \frac{a}{b}$.

- $\mathbb{Q}(\sqrt{2})$ has two infinite real primes $\sigma_1(\sqrt{2}) = \sqrt{2}$ and $\sigma_2(\sqrt{2}) = -\sqrt{2}$.
- $\mathbb{Q}(\sqrt{-2})$ has one infinite complex prime determined by $\sigma(\sqrt{-2}) = \sqrt{-2}$, $\bar{\sigma}(\sqrt{-2}) = -\sqrt{-2}$.

Remark. If we have an extension L/K , then an infinite prime σ of K **ramifies** in L if σ is real, but has an extension to L which is complex.

Example 1.2. The infinite prime of \mathbb{Q} is unramified in $\mathbb{Q}(\sqrt{2})$, but it is ramified in $\mathbb{Q}(\sqrt{-2})$.

Definition 1.5. Let K be a number field. Then a **modulus** in K is a formal product

$$\mathfrak{m} = \prod_{\mathfrak{p}} \mathfrak{p}^{n_{\mathfrak{p}}}$$

over all primes \mathfrak{p} , finite or infinite, of K , such that

- (i) $n_{\mathfrak{p}} \geq 0$, and at most finitely many of these are nonzero.
- (ii) $n_{\mathfrak{p}} = 0$ for \mathfrak{p} infinite complex primes.
- (iii) $n_{\mathfrak{p}} \leq 1$ for \mathfrak{p} infinite real primes.

If $n_{\mathfrak{p}} = 0$ for all \mathfrak{p} , set $\mathfrak{m} = 1$.

Note that if K is a purely imaginary field (i.e. it has no real primes), then a modulus of K is just an ideal of \mathcal{O}_K . We can write any modulus \mathfrak{m} as a product $\mathfrak{m} = \mathfrak{m}_0 \mathfrak{m}_{\infty}$, where \mathfrak{m}_0 is an ideal of \mathcal{O}_K and \mathfrak{m}_{∞} is a product of distinct real infinite primes.

Recall we write $v_{\mathfrak{p}_i}(\mathfrak{a}) = r_i$. We now extend this map using moduli.

24 Jan 2024,
Lecture 3

Definition 1.6. Let \mathfrak{m} be a modulus. Define $I_K(\mathfrak{m})$ to be the group of fractional ideals coprime to \mathfrak{m} , where $\mathfrak{a} \in I_K$ is coprime to \mathfrak{m} if $v_{\mathfrak{p}}(\mathfrak{a}) = 0$ for all primes $\mathfrak{p} \mid \mathfrak{m}_0$.

Non-infinite primes play no role in this definition, i.e. $I_K(\mathfrak{m}) = I_K(\mathfrak{m}_0)$.

Example 1.3. • Let $\mathfrak{m} = (1)$, then $I_K(\mathfrak{m}) = I_K$.

- Let $K = \mathbb{Q}$ and $\mathfrak{m} = (m)$ for m a positive integer. Then $I_{\mathbb{Q}}(\mathfrak{m}) = \left\{ \left(\frac{a}{b} \right) \mathbb{Z} \mid (a, m) = (b, m) = 1 \right\}$.

Now let L/K be abelian, not necessarily unramified.

Definition 1.7. Let \mathfrak{m} be a modulus of K divisible by all prime ideals that ramify in L . The Artin map for L/K and \mathfrak{m} is a homomorphism

$$\Phi_{\mathfrak{m}} = \Phi_{L/K, \mathfrak{m}} : I_K(\mathfrak{m}) \rightarrow \text{Gal}(L/K)$$

given by $\mathfrak{a} \mapsto \left(\frac{L/K}{\mathfrak{a}} \right)$.

Example 1.4. Let \mathfrak{m} be a positive integer and ζ_m a primitive m^{th} root of unity. Let $K = \mathbb{Q}$ and $L = \mathbb{Q}(\zeta_m)$. Recall that $\text{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \cong (\mathbb{Z}/m\mathbb{Z})^\times$ given by $\{\sigma : \zeta_m \mapsto \zeta_m^a\} \mapsto [a]$. Also, if a prime p ramifies in $\mathbb{Q}(\zeta_m)$, then $p \mid m$.

Hence let $\mathfrak{m} = (m)$, which contains all ramified prime ideals. We have a well-defined map $\Phi_{\mathfrak{m}} : I_{\mathbb{Q}}(\mathfrak{m}) \rightarrow \text{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \cong (\mathbb{Z}/m\mathbb{Z})^\times$.

Let $\left(\frac{a}{b} \right) \mathbb{Z} \in I_{\mathbb{Q}}(\mathfrak{m})$ with $\frac{a}{b} > 0$, then

$$\Phi_{\mathfrak{m}} \left(\left(\frac{a}{b} \right) \mathbb{Z} \right) = [a][b]^{-1} \in (\mathbb{Z}/m\mathbb{Z})^\times.$$

Exercises: verify this above claim, show that (here?) the Artin map is surjective and work out its kernel.

Definition 1.8. Let $P_K(\mathfrak{m})$ be the subgroup of $I_K(\mathfrak{m})$ generated by

$$\{(\alpha) \mid \alpha \in \mathcal{O}_K, \alpha \equiv 1 \pmod{\mathfrak{m}_0}, \sigma(\alpha) > 0 \text{ for all real primes } \sigma \mid \mathfrak{m}_\infty\}.$$

Note $\alpha \equiv 1 \pmod{\mathfrak{m}_0}$ can also be written as $v_{\mathfrak{p}}(\alpha - 1) \geq v_{\mathfrak{p}}(\mathfrak{m}_0)$ (here $v_{\mathfrak{p}}(\alpha) = v_{\mathfrak{p}}(\alpha \mathcal{O}_K)$). This is called the **ray** or **ray group** for \mathfrak{m} .

Remark. Definitions in the literature might differ a bit, but we use the one above.

Example 1.5. Let $K = \mathbb{Q}, L = \mathbb{Q}(\zeta_m)$. Suppose $\mathfrak{m} = (m)$, then $P_{\mathbb{Q}}(\mathfrak{m}) = \left\{ \left(\frac{a}{b} \right) \mathbb{Z} \in I_{\mathbb{Q}}(\mathfrak{m}) \mid a \equiv b \pmod{m} \right\}$. Note $I_{\mathbb{Q}}(\mathfrak{m}) = I_{\mathbb{Q}}(\mathfrak{m}_0)$, which is not true for $P_{\mathbb{Q}}(\mathfrak{m})$!

Now suppose $\mathfrak{m} = (m)_\infty$ – the infinite prime of \mathbb{Q} . Then

$$P_{\mathbb{Q}}(\mathfrak{m}) = \left\{ \left(\frac{a}{b} \right) \mathbb{Z} \in I_{\mathbb{Q}}(\mathfrak{m}) \mid a \equiv b \pmod{m}, \frac{a}{b} > 0 \right\}.$$

We have $I_{\mathbb{Q}}((m))/P_{\mathbb{Q}}((m)) \cong (\mathbb{Z}/m\mathbb{Z})^\times / \{\pm 1\}$ and $I_{\mathbb{Q}}((m)_\infty)/P_{\mathbb{Q}}((m)_\infty) \cong (\mathbb{Z}/m\mathbb{Z})^\times$.

In general, $P_K(\mathfrak{m})$ has finite index in $I_K(\mathfrak{m})$.

Definition 1.9. The quotient $I_K(\mathfrak{m})/P_K(\mathfrak{m})$ is called the **ray class group**.

Our goal is to show that this is a finite group. Recall by Ostrowski's theorem that every nontrivial absolute value is equivalent to either $|\cdot|_{\mathfrak{p}}$ for some prime ideal \mathfrak{p} of \mathcal{O}_K or $|\cdot|_{\sigma}$ for some embedding $\sigma : K \rightarrow \mathbb{C}$, where $|\cdot|_{\sigma} = |x|_{\mathbb{C}}$ with $|\cdot|_{\mathbb{C}}$ the complex absolute value; and $|x|_{\mathfrak{p}} = C^{v_{\mathfrak{p}}(x)}$ for $x \neq 0$ for some $0 < C < 1$ (often $C = \frac{1}{p}$) and 0 for 0. (Recall $v_{\mathfrak{p}}(x) = \alpha$ if $x\mathcal{O}_K = \mathfrak{p}^{\alpha}\mathfrak{p}_1^{\alpha_1} \dots \mathfrak{p}_r^{\alpha_r}$.)

We quote a result proved in Local Fields:

Theorem 1.4 (Approximation theorem). Let $|\cdot|_1, \dots, |\cdot|_n$ be nontrivial pairwise inequivalent absolute values on K . Let $\beta_1, \dots, \beta_n \in K$ be nonzero. Then for any $\epsilon > 0$, there exists $\alpha \in K$ such that $|\alpha - \beta_j|_j < \epsilon$ for each $j = 1, \dots, n$.

Consequences.

- Let \mathfrak{p} be a real infinite prime corresponding to $\sigma : K \rightarrow \mathbb{R}$. If $\alpha\beta \neq 0$ and $|\alpha - \beta|_{\mathfrak{p}} < \epsilon$, then $\sigma\left(\frac{\alpha}{\beta}\right) > 0$.
- Let \mathfrak{p} be a finite prime. Then $|\alpha - \beta|_{\mathfrak{p}} < \epsilon$ is equivalent to $\left|\frac{\alpha}{\beta} - 1\right|_{\mathfrak{p}} < \frac{\epsilon}{|\beta|_{\mathfrak{p}}}$.
Let $\epsilon' = \frac{\epsilon'}{|\beta|_{\mathfrak{p}}}$. If ϵ' is small, say $\epsilon' < C^n$ for some n , then $v_{\mathfrak{p}}\left(\frac{\alpha}{\beta} - 1\right) > n$ and so $\alpha \equiv \beta \pmod{\mathfrak{p}^n}$.

Remark/Exercise. Let I be an ideal of \mathcal{O}_K , then every class in $\text{Cl}(K)$ has a representative which is coprime to I .

Definition 1.10. Let $P_{\mathfrak{m}} \subset I_K(\mathfrak{m})$ be the subgroup of principal fractional ideals which are coprime to \mathfrak{m} .

Proposition 1.5. Let $P_{\mathfrak{m}} \subset I_K(\mathfrak{m})$ be as above. Then we have two exact sequences

$$\begin{aligned} 1 \rightarrow P_{\mathfrak{m}} \rightarrow I_K(\mathfrak{m}) \rightarrow \text{Cl}(K) \rightarrow 1 \\ 1 \rightarrow P_{\mathfrak{m}}/P_K(\mathfrak{m}) \rightarrow I_K(\mathfrak{m})/P_K(\mathfrak{m}) \rightarrow \text{Cl}(K) \rightarrow 1. \end{aligned}$$

Proof. Let $\mathfrak{a} \in I_K(\mathfrak{m})$ and define $f : I_K(\mathfrak{m}) \rightarrow \text{Cl}(K)$ by $\mathfrak{a} \mapsto [a]$. This is a group homomorphism, it is surjective by the previous remark with kernel $P_{\mathfrak{m}}$, so $1 \rightarrow P_{\mathfrak{m}} \rightarrow I_K(\mathfrak{m}) \rightarrow \text{Cl}(K) \rightarrow 1$. The second sequence follows immediately because f is trivial on $P_K(\mathfrak{m})$. \square

Definition 1.11. For \mathfrak{m} a modulus, let

$$\begin{aligned} K_{\mathfrak{m}} &= \{\alpha \in K^{\times} \mid (\alpha) \in I_K(\mathfrak{m})\} \\ K_{\mathfrak{m},1} &= \{\alpha \in K^{\times} \mid \alpha \equiv 1 \pmod{\mathfrak{m}_0}, \sigma(\alpha) > 0 \ \forall \sigma \mid \mathfrak{m}_{\infty}\}. \end{aligned}$$

Note $P_k(\mathfrak{m}) = \{(\alpha) \in I_K(\mathfrak{m}) \mid \alpha \in K_{\mathfrak{m},1}\}$.

26 Jan 2024,
Lecture 4

Theorem 1.6. The ray class group $I_K(\mathfrak{m})/P_K(\mathfrak{m})$ is a finite group with size

$$h_K(\mathfrak{m}) = |I_K(\mathfrak{m})/P_K(\mathfrak{m})| = \frac{h_K \cdot \phi(\mathfrak{m})}{[\mathcal{O}_K^\times : (\mathcal{O}_K^\times \cap K_{\mathfrak{m},1})]},$$

where h_K is the class number of K and $\phi(\mathfrak{m}) = \phi(\mathfrak{m}_0)\phi(\mathfrak{m}_\infty)$ with $\phi(\mathfrak{m}_0) = |(\mathcal{O}_K/\mathfrak{m}_0)^\times| = N(\mathfrak{m}_0) \cdot \prod_{\mathfrak{p}|\mathfrak{m}_0} (1 - N(\mathfrak{p}^{-1}))$ and $\phi(\mathfrak{m}_\infty) = 2^{\#\mathfrak{m}_\infty}$ where $\#\mathfrak{m}_\infty$ is the number of infinite real primes dividing \mathfrak{m} .

Proof. Step 1. $P_{\mathfrak{m}}/P_K(\mathfrak{m}) \cong K_{\mathfrak{m}}/\mathcal{O}_K^\times K_{\mathfrak{m},1}$.

Proof of Step 1. Consider $K_{\mathfrak{m}} \rightarrow P_{\mathfrak{m}}/P_K(\mathfrak{m})$ by $\alpha \mapsto (\alpha)P_K(\mathfrak{m})$. This is a surjective homomorphism with kernel

$$\begin{aligned} & \{\alpha \in K_{\mathfrak{m}} \mid (\alpha) \in P_K(\mathfrak{m})\} \\ &= \{\alpha \in K_{\mathfrak{m}} \mid \exists \beta \in K_{\mathfrak{m},1} \text{ s.t. } (\alpha) = (\beta)\} \\ &= \{\alpha \in K_{\mathfrak{m}} \mid \exists \beta \in K_{\mathfrak{m},1} \text{ s.t. } \beta = \alpha \cdot \epsilon \text{ for some } \epsilon \in \mathcal{O}_K^\times\}. \end{aligned}$$

□

Step 2. $K_{\mathfrak{m}}/K_{\mathfrak{m},1} \cong \{\pm 1\}^{\#\mathfrak{m}_\infty} \times (\mathcal{O}_K/\mathfrak{m}_0)^\times$.

Proof of Step 2. We can write $\alpha \in K_{\mathfrak{m}}$ as $\alpha = \frac{a}{b}$ for $a, b \in \mathcal{O}_K$ coprime, and $(a), (b)$ coprime to \mathfrak{m}_0 . For such a, b , the images $\bar{a}, \bar{b} \in \mathcal{O}_K/\mathfrak{m}_0$ lie in $(\mathcal{O}_K/\mathfrak{m}_0)^\times$. Consider the map

$$\begin{aligned} K_{\mathfrak{m}} &\rightarrow \left(\prod_{\sigma|\mathfrak{m}_\infty} \{\pm 1\} \right) \times (\mathcal{O}_K/\mathfrak{m}_0)^\times \\ \alpha &\mapsto \left(\prod_{\sigma|\mathfrak{m}_\infty} \text{sgn}(\sigma(\alpha)) \right) \times \bar{a} \end{aligned}$$

for $\bar{a} = \bar{ab}^{-1} \in (\mathcal{O}_K/\mathfrak{m}_0)^\times$. This map is surjective: this is an exercise, use the Approximation Theorem. It has kernel

$$\{\alpha \in K_{\mathfrak{m}} \mid \sigma(\alpha) > 0 \ \forall \sigma \mid \mathfrak{m}_\infty, \ \alpha \equiv 1 \pmod{\mathfrak{m}_0}\} = K_{\mathfrak{m},1}.$$

□

Step 3. $\mathcal{O}_K^\times K_{\mathfrak{m},1}/K_{\mathfrak{m},1} \cong \mathcal{O}_K^\times/(\mathcal{O}_K^\times \cap K_{\mathfrak{m},1})$.

Proof of Step 3. This is just the second isomorphism theorem. □

Putting it all together:

$$[I_K(\mathfrak{m}) : P_K(\mathfrak{m})] = [I_K(\mathfrak{m}) : P_{\mathfrak{m}}][P_{\mathfrak{m}} : P_K(\mathfrak{m})]$$

and

$$\begin{aligned} (P_{\mathfrak{m}}/P_K(\mathfrak{m})) &\stackrel{(i)}{\cong} K_{\mathfrak{m}}/\mathcal{O}_K^{\times}K_{\mathfrak{m},1} \\ &\cong (K_{\mathfrak{m}}/K_{\mathfrak{m},1})/(\mathcal{O}_K^{\times}K_{\mathfrak{m},1}/K_{\mathfrak{m},1}) \\ &\stackrel{(iii)}{\cong} (K_{\mathfrak{m}}/K_{\mathfrak{m},1})/(\mathcal{O}_K^{\times}/(\mathcal{O}_K^{\times} \cap K_{\mathfrak{m},1})) \end{aligned}$$

and

$$I_K(\mathfrak{m})/P_{\mathfrak{m}} \cong \text{Cl}(K)$$

by Proposition 1.5.

This gives

$$\begin{aligned} [I_K(\mathfrak{m}) : P_K(\mathfrak{m})] &= [I_K(\mathfrak{m}) : P_{\mathfrak{m}}][P_{\mathfrak{m}} : P_K(\mathfrak{m})] \\ &= |\text{Cl}(K)| \frac{[K_{\mathfrak{m}} : K_{\mathfrak{m},1}]}{[\mathcal{O}_K : (\mathcal{O}_K^{\times} \cap K_{\mathfrak{m},1})]} \stackrel{(ii)}{=} \frac{h_K \cdot \phi(\mathfrak{m})}{[\mathcal{O}_K : (\mathcal{O}_K^{\times} \cap K_{\mathfrak{m},1})]}. \end{aligned}$$

□

Next we have more general class groups, i.e. $I_K(\mathfrak{m})/H$ with $P_K(\mathfrak{m}) \subset H$.

Definition 1.12. A subgroup $H \subset I_K(\mathfrak{m})$ is a **congruence subgroup** for \mathfrak{m} if it satisfies $P_K(\mathfrak{m}) \subset H \subset I_K(\mathfrak{m})$.

Motivation: For "suitably chosen" moduli \mathfrak{m} , the congruence subgroup will be the kernel of the Artin map $\Phi_{\mathfrak{m}}$.

Definition 1.13. Let H be a congruence subgroup for \mathfrak{m} , then the quotient $I_K(\mathfrak{m})/H$ is called a **generalized ideal class group** for \mathfrak{m} .

Remark. Recall that for $K = \mathbb{Q}$ and $\mathfrak{m} = (m)\infty$ for m a positive integer, we saw $I_K(\mathfrak{m})/P_K(\mathfrak{m}) \cong (\mathbb{Z}/m\mathbb{Z})^{\times}$ and

$$(\mathbb{Z}/m\mathbb{Z})^{\times} \cong \text{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \cong I_K(\mathfrak{m})/P_K(\mathfrak{m})$$

via the Artin map, so $\ker(\Phi_{\mathbb{Q}(\zeta_m)/\mathbb{Q}, \mathfrak{m}}) = P_K(\mathfrak{m})$.

The idea of class field theory is that generalized ideal class groups are Galois groups of abelian extensions and that the link between them is given by the Artin map. We will prove that the Artin map is surjective. Determining the kernel is a lot more difficult (not done in this course).

What is the meaning of "suitably chosen" above? For L/K abelian, we want to know for which moduli \mathfrak{m} will $\ker(\Phi_{\mathfrak{m}})$ be a congruence subgroup.

Lemma 1.7. Let L/K be abelian and let \mathfrak{m} be a modulus divisible by all ramified primes. If \mathfrak{n} is another modulus such that $\mathfrak{m} \mid \mathfrak{n}$, then

$$P_K(\mathfrak{m}) \subset \ker(\Phi_{\mathfrak{m}}) \implies P_K(\mathfrak{n}) \subset \ker(\Phi_{\mathfrak{n}}).$$

Proof. Note first that if $\mathfrak{m} \mid \mathfrak{n}$, then $I_K(\mathfrak{n}) \subset I_K(\mathfrak{m})$, so $\Phi_{\mathfrak{n}} : I_K(\mathfrak{n}) \rightarrow \text{Gal}(L/K)$ is well-defined and $\Phi_{\mathfrak{n}} = \Phi_{\mathfrak{m}}|_{I_K(\mathfrak{n})}$, so $\ker(\Phi_{\mathfrak{n}}) = \ker(\Phi_{\mathfrak{m}}) \cap I_K(\mathfrak{n})$. If $\mathfrak{m} \mid \mathfrak{n}$, then $P_K(\mathfrak{n}) \subset P_K(\mathfrak{m})$. Now $P_K(\mathfrak{n}) \subset P_K(\mathfrak{m}) \subset \ker(\Phi_{\mathfrak{m}})$, so

$$(\alpha) \in P_K(\mathfrak{n}) \subset P_K(\mathfrak{m}) \cap I_K(\mathfrak{n}) \subset \ker(\Phi_{\mathfrak{m}}) \cap I_K(\mathfrak{n}) = \ker(\Phi_{\mathfrak{n}}).$$

□

In the above situation, if $\ker(\Phi_{\mathfrak{m}})$ is a congruence subgroup for \mathfrak{m} , then $\ker(\Phi_{\mathfrak{n}})$ is a congruence subgroup for \mathfrak{n} .

Now we find a special modulus that works for each extension, called **the conductor**.

Statements of global class field theory (ideal theoretic). For L/K abelian, we are interested to find out for which $\mathfrak{m} \subset \mathcal{O}_K$ is $\ker(\Phi_{L/K, \mathfrak{m}})$ a congruence subgroup (i.e. $P_K(\mathfrak{m}) \subset \ker(\Phi_{L/K, \mathfrak{m}})$).

Theorem 1.8 (The Conductor Theorem). Let L/K be abelian. Then there is a modulus $\mathfrak{f} = \mathfrak{f}(L/K)$ such that

- a prime of K , finite or infinite, ramifies in L if and only if it divides $\mathfrak{f}_{L/K}$.
- If \mathfrak{m} is divisible by all primes that ramify, then $\ker(\Phi_{L/K, \mathfrak{m}})$ is a congruence subgroup for \mathfrak{m} if and only if $\mathfrak{f}_{L/K} \mid \mathfrak{m}$.

Definition 1.14. The modulus $\mathfrak{f}_{L/K}$ is uniquely determined by L/K and called the **conductor**.

Example 1.6. Let $K = \mathbb{Q}$ and let $L = \mathbb{Q}(\sqrt{N})$ for $N \neq 0, 1$ squarefree. Then

$$\mathfrak{f}_{L/K} = \begin{cases} |d_{L/K}| & N > 0 \\ |d_{L/K}| \infty & N < 0. \end{cases} \quad (|d_{L/K}| \infty \text{ is the real infinite place of } \mathbb{Q}).$$

Remark. The conductor is not just the product of ramified primes. In Ex. Sheet 1, there will be a cubic extension L/\mathbb{Q} which is ramified only at 3. However, for $\mathfrak{m} = (3)$ or $\mathfrak{m} = (3)\infty$, $\ker(\Phi_{L/\mathbb{Q}, \mathfrak{m}})$ is not a congruence subgroup, so $\mathfrak{f}_{L/\mathbb{Q}} \nmid (3)$ and $\mathfrak{f}_{L/\mathbb{Q}} \nmid (3)\infty$.

Next we focus on the kernel. Recall that if $\mathcal{P} \subset \mathcal{O}_L$ is a prime ideal, then we have $N_{L/K}(\mathcal{P}) = \mathfrak{p}^{f_{\mathcal{P}/\mathfrak{p}}}$ if $\mathfrak{p} = \mathcal{P} \cap \mathcal{O}_K$.

Notation. Let $N_{L/K} : I_K \rightarrow I_K$ be the norm map, given by $\mathfrak{a} \mapsto N_{L/K}(\mathfrak{a})$. If $\mathfrak{a} = \prod_{i=1}^n \mathcal{P}_i^{r_i}$, then $N_{L/K}(\mathfrak{a}) = \prod_{i=1}^n (N(\mathcal{P}_i)^{r_i}) = \prod_{i=1}^n (\mathfrak{p}_i^{f_{\mathcal{P}_i/\mathfrak{p}_i} r_i})$.

Definition 1.15. Let L/K be abelian and let \mathfrak{m} be a modulus of K divisible by $\mathfrak{f}(L/K)$. Then the **norm group** (also called a Tahagi group) is the congruence subgroup

$$T_{L/K}(\mathfrak{m}) = P_K(\mathfrak{m})N_{L/K}(I_L(\mathfrak{m})),$$

where $I_L(\mathfrak{m})$ is the subgroup of I_L with elements fractional ideals that are coprime to $\mathfrak{m}\mathcal{O}_L$.

Theorem 1.9 (Artin Reciprocity Theorem). Let L/K be abelian and let \mathfrak{m} be a modulus of K divisible by all ramified primes (both finite and infinite). Then the Artin map $\Phi_{L/K, \mathfrak{m}}(I_K(\mathfrak{m})) \rightarrow \text{Gal}(L/K)$ is surjective.

If also $\mathfrak{f}_{L/K} \mid \mathfrak{m}$, so that $\ker(\Phi_{\mathfrak{m}})$ is a congruence subgroup, then $\ker(\Phi_{L/K, \mathfrak{m}}) = T_{L/K}(\mathfrak{m})$ and the Artin map defines an isomorphism

$$I_K(\mathfrak{m})/T_{L/K}(\mathfrak{m}) \cong \text{Gal}(L/K).$$

So $\text{Gal}(L/K)$ is the generalized ideal class group for \mathfrak{m} .

Artin reciprocity gives us information about the decomposition of primes:

Theorem 1.10 (Decomposition law). Let L/K be abelian of degree n and let $\mathfrak{p} \subset \mathcal{O}_K$ be an unramified prime ideal. Let \mathfrak{m} be divisible by $\mathfrak{f}(L/K)$, but not by \mathfrak{p} . Let $H = \ker(\Phi_{\mathfrak{m}})$ be the congruence subgroup for \mathfrak{m} . Let f be the smallest positive integer such that $\mathfrak{p}^f \in H$, i.e. f is the order of $\mathfrak{p} \bmod H$ in $I_K(\mathfrak{m})/H$. Then \mathfrak{p} decomposes in L into a product

$$\mathfrak{p}\mathcal{O}_L = \mathcal{P}_1 \dots \mathcal{P}_g$$

for $g = \frac{n}{f}$ of distinct prime ideals of degree f over \mathfrak{p} .

Proof. Let $\mathfrak{p}\mathcal{O}_L = \mathcal{P}_1 \dots \mathcal{P}_g$ be the prime decomposition in L . These have to be distinct as \mathfrak{p} is unramified, and all \mathcal{P}_i have the same residue field degree $f_{\mathcal{P}_i/\mathfrak{p}}$ (as the extension is abelian, in particular Galois). We know that $f_{\mathcal{P}_i/\mathfrak{p}}$ is the order of $\left(\frac{L/K}{\mathfrak{p}}\right)$ and so under the isomorphism $I_K(\mathfrak{m})/H \cong \text{Gal}(L/K)$, this means it is also the order of $\mathfrak{p} \bmod H$ in $I_K(\mathfrak{m})/H$. The result follows since $[L : K] = n = efg = fg$. \square

Next we want to show that every generalized ideal class group is the Galois group of some abelian extension and that this extension is unique.

Theorem 1.11 (The Existence Theorem). Let \mathfrak{m} be a modulus of f and let H be a congruence subgroup for \mathfrak{m} . Then there exists a unique abelian extension L/K with the following properties:

- All its ramified primes, finite or infinite, divide \mathfrak{m} .
- $H = T_{L/K}(\mathfrak{m})$.
- $I_K(\mathfrak{m})/H \cong \text{Gal}(L/K)$ under the Artin map $\Phi_{L/K, \mathfrak{m}}$.

So for any number field K , we can find abelian extensions with specified ramification.

Definition 1.16. Let \mathfrak{m} be any modulus and let $H = P_K(\mathfrak{m})$. The **ray class field** is the unique abelian extension $K(\mathfrak{m})$ of K such that $P_K(\mathfrak{m}) = \ker(\Phi_{K(\mathfrak{m})/K, \mathfrak{m}})$. This explains the name $\text{Gal}(K(\mathfrak{m})/K) \cong I_K(\mathfrak{m})/P_K(\mathfrak{m})$.

Example 1.7. Let $K = \mathbb{Q}$ and let $\mathfrak{m} = (m)\infty$ for m odd or divisible by 4. Then $\mathbb{Q}(\mathfrak{m}) = \mathbb{Q}(\zeta_m)$. Taking $\mathfrak{m} = (m)$ instead gives $\mathbb{Q}(\mathfrak{m}) = \mathbb{Q}(\zeta_m + \zeta_m^{-1})$.

Next we want to show that every abelian extension is contained in a ray class field. In other words, given K, \mathfrak{m} , there is a unique abelian extension $K(\mathfrak{m})/K$ such that $P_K(\mathfrak{m}) = \ker(\Phi_{K(\mathfrak{m})/K, \mathfrak{m}})$.

31 Jan 2024,
Lecture 6

Proposition 1.12. Let $K \leq L \leq M$ be a tower of abelian extensions. Suppose \mathfrak{m} contains all prime ideals $\mathfrak{p} \subset \mathcal{O}_K$ that ramify in M . Write $\text{res} : \text{Gal}(M/K) \rightarrow \text{Gal}(L/K)$ for the restriction map $\sigma \mapsto \sigma_L$. Then we have a commutative

$$\begin{array}{ccc} I_K(\mathfrak{m}) & \xrightarrow{\Phi_{M/K, \mathfrak{m}}} & \text{Gal}(M/K) \\ & \searrow \Phi_{L/K, \mathfrak{m}} & \downarrow \text{res} \\ & & \text{Gal}(L/K) \end{array} \quad .$$

diagram

Proof. Exercise on Example Sheet 1. □

Lemma 1.13. Let L/K and M/K be abelian extensions. Then $L \subset M$ if and only if there is a modulus \mathfrak{m} divisible by all primes of K which ramify in either L or M such that $P_K(\mathfrak{m}) \subset \ker(\Phi_{M/K, \mathfrak{m}}) \subset \ker(\Phi_{L/K, \mathfrak{m}})$.

Proof. Suppose $L \subset M$. Then by Artin reciprocity, there exists \mathfrak{m}_1 for L/K and \mathfrak{m}_2 for M/K such that $P_K(\mathfrak{m}_1) \subset \ker(\Phi_{L/K, \mathfrak{m}_1})$ and $P_K(\mathfrak{m}_2) \subset \ker(\Phi_{M/K, \mathfrak{m}_2})$. By Lemma 1.7, we can find \mathfrak{m} such that $P_K(\mathfrak{m}) \subset \ker(\Phi_{L/K, \mathfrak{m}})$ and $P_K(\mathfrak{m}) \subset \ker(\Phi_{M/K, \mathfrak{m}})$. By Proposition 1.12, we have $\text{res} \circ \Phi_{M/K, \mathfrak{m}} = \Phi_{L/K, \mathfrak{m}}$, so $P_K(\mathfrak{m}) \subset \ker(\Phi_{M/K, \mathfrak{m}}) \subset \ker(\Phi_{L/K, \mathfrak{m}})$.

Now suppose we have \mathfrak{m} such that $P_K(\mathfrak{m}) \subset \ker(\Phi_{M/K, \mathfrak{m}}) \subset \ker(\Phi_{L/K, \mathfrak{m}})$. Then we get that under the map $\Phi_{M/K, \mathfrak{m}} : I_K(\mathfrak{m}) \rightarrow \text{Gal}(M/K)$, the subgroup $\ker(\Phi_{L/K, \mathfrak{m}}) \subset I_K(\mathfrak{m})$ maps to a subgroup $H \subset \text{Gal}(M/K)$. By Galois theory, H corresponds to an intermediate field $K \subset \tilde{L} \subset M$. Now apply the first part of the proof to $\tilde{L} \subset M$ to obtain $\ker(\Phi_{L/K, \mathfrak{m}}) = \ker(\Phi_{\tilde{L}/M, \mathfrak{m}})$. By uniqueness, in the Existence Theorem, $L = \tilde{L} \subset M$. □

Corollary 1.14. Let K be a number field. Then any abelian extension is contained in a ray class field.

Proof. Suppose L/K is abelian and let \mathfrak{m} be a modulus of K such that $\mathfrak{f}_{L/K} \mid \mathfrak{m}$. Then $H = \ker(\Phi_{L/K, \mathfrak{m}})$ is a congruence subgroup for \mathfrak{m} . So $P_K(\mathfrak{m}) = \ker(\Phi_{K(\mathfrak{m})/K, \mathfrak{m}}) \subset H = \ker(\Phi_{L/K, \mathfrak{m}})$. By Lemma 1.13, $L \subset K(\mathfrak{m})$. \square

Before stating the Classification Theorem, we define an equivalence relation on the set of congruence subgroups. Why?

- If $\ker(\Phi_{\mathfrak{m}})$ is a congruence subgroup for \mathfrak{m} , then $\ker(\Phi_{\mathfrak{n}})$ is a congruence subgroup for \mathfrak{n} for any modulus $\mathfrak{m} \mid \mathfrak{n}$.
- Say a prime \mathfrak{p} is in the support of \mathfrak{m} if $\mathfrak{p} \mid \mathfrak{m}$. If \mathfrak{m} and \mathfrak{n} have the same support, then $I_K(\mathfrak{m}) = I_K(\mathfrak{n})$, but $P_K(\mathfrak{m})$ may differ from $P_K(\mathfrak{n})$.

Definition 1.17. We say two congruence subgroups H_1 and H_2 are equivalent, written $H_1 \sim H_2$ if there is a modulus \mathfrak{m} such that $I_K(\mathfrak{m}) \cap H_1 = I_K(\mathfrak{m}) \cap H_2$.

Let L/K be abelian. Let \mathfrak{m} be such that $P_K(\mathfrak{m}) \subset \ker(\Phi_{L/K, \mathfrak{m}})$ and let \mathfrak{m}' be such that $P_K(\mathfrak{m}') \subset \ker(\Phi_{L/K, \mathfrak{m}'})$. Then $\ker(\Phi_{L/K, \mathfrak{m}}) \sim \ker(\Phi_{L/K, \mathfrak{m}'})$ because

$$\ker(\Phi_{L/K, \mathfrak{m}}) \cap I_K(\mathfrak{m}\mathfrak{m}') = \ker(\Phi_{L/K, \mathfrak{m}\mathfrak{m}'}) = \ker(\Phi_{L/K, \mathfrak{m}'}) \cap I_K(\mathfrak{m}\mathfrak{m}').$$

The collection of congruence subgroups H for \mathfrak{m} with \mathfrak{m} such that $P_K(\mathfrak{m}) \subset \ker(\Phi_{L/K, \mathfrak{m}})$ lie in a single equivalence class of congruence subgroups. We write $H(L/K)$ for this class.

Theorem 1.15 (The Classification Theorem). Let K be a number field. Then there is a one-to-one inclusion-reversing correspondence

$$\begin{aligned} \{\text{abelian extensions } L/K\} &\leftrightarrow \{\text{congruence subgroups}/\sim\} \\ L/K &\mapsto H(L/K). \end{aligned}$$

”Applications” of main theorems.

Theorem 1.16 (Kronecker–Weber theorem). Let L/\mathbb{Q} be abelian. Then there is a positive integer m such that $L \subset \mathbb{Q}(\zeta_m)$.

Proof. By Artin reciprocity, there is a modulus \mathfrak{m} satisfying the inclusions $P_{\mathbb{Q}}(\mathfrak{m}) \subset \ker(\Phi_{L/\mathbb{Q}, \mathfrak{m}}) \subset I_{\mathbb{Q}}(\mathfrak{m})$. Any modulus of \mathbb{Q} will be (m) or $(m)\infty$ for some m . By Lemma 1.7, we may assume $\mathfrak{m} = (m)\infty$. We have $P_{\mathbb{Q}}(\mathfrak{m}) = \ker(\Phi_{\mathbb{Q}(\zeta_m)/\mathbb{Q}, \mathfrak{m}})$, so $P_{\mathbb{Q}}(\mathfrak{m}) = \ker(\Phi_{\mathbb{Q}(\zeta_m)/\mathbb{Q}, \mathfrak{m}}) \subset \ker(\Phi_{L/\mathbb{Q}, \mathfrak{m}})$. By Lemma 1.13, we have $L \subset \mathbb{Q}(\zeta_m)$. \square

Remark. There exist proofs of Kronecker–Weber that don’t use class field theory (see e.g. *Number Fields* by Marcus).

Hilbert Class Field: Given a number field K , by the Existence Theorem we can find an abelian extension and ”control” the ramification. Now take $\mathfrak{m} = (1)$, then the corresponding abelian extension $K(\mathfrak{m})/K$ will be unramified at all primes (finite and infinite). We have $\Phi_{\mathfrak{m}} : I_K = I_K(1) \rightarrow \text{Gal}(K(1)/K)$ with kernel $P_K((1)) = P_K$, so we obtain $\text{Cl}(K) = I_K/P_K \cong \text{Gal}(K(1)/K)$. By the Existence Theorem, we obtain an unramified abelian extension with Galois group equal to the ideal class group.

Definition 1.18. The Hilbert class field F is the ray class field for the modulus $\mathfrak{m} = (1)$.

Example 1.8. Let $K = \mathbb{Q}$. This is its own Hilbert class group (as $\text{Cl}(K) = 1$).

02 Feb 2024,
Lecture 7

Theorem 1.17. The Hilbert class field F is the maximal unramified extension of K .

Proof. Let M be another unramified abelian extension. By the Conductor theorem, $\mathfrak{f}_{M/K} = (1)$. For $\mathfrak{m} = (1)$ we have

$$P_K(\mathfrak{f}_{M/K}) = \underbrace{P_K(\mathfrak{m})}_{=\ker(\Phi_{F/K, \mathfrak{m}})} \subset \ker(\Phi_{M/K, \mathfrak{f}_{M/K}}).$$

By Lemma 1.13, we have $M \subset F$. □

Corollary 1.18. Let K be a number field. There is a one-to-one correspondence between unramified abelian extensions M of K and subgroups of the ideal class group $\text{Cl}(K)$. Furthermore, if M/K corresponds to $H \subset \text{Cl}(K)$, then the Artin map induces an isomorphism

$$\text{Cl}(K)/H \xrightarrow{\cong} \text{Gal}(M/K).$$

Proof. Let F be the Hilbert class field at K . Then $\text{Gal}(F/K) \cong \text{Cl}(K)$. By Galois theory, there is a one-to-one inclusion-reversing correspondence between intermediate fields and subgroups of $\text{Gal}(F/K) \cong \text{Cl}(K)$. Since each unramified abelian extension is contained in F , the first part of the corollary follows.

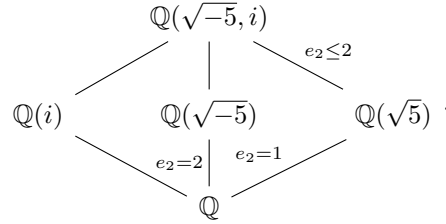
Let H be a subgroup of $\text{Gal}(F/K)$ and let

$$M = F^H = \{x \in F \mid \sigma(x) = x \ \forall \sigma \in H\}.$$

By Proposition 1.12, $\Phi_{M/K, \mathfrak{m}} : \text{Cl}(K) \rightarrow \text{Gal}(M/K)$ with $\Phi_{M/K, \mathfrak{m}} = \text{res} \circ \Phi_{F/K, \mathfrak{m}}$ and $\text{res} : \text{Gal}(F/K) \rightarrow \text{Gal}(M/K)$ by $\sigma \mapsto \sigma_M$. Now if $[a] \in H$, then $\Phi_{M/K, \mathfrak{m}}([a]) = 1$. □

Fact. Let M_1/K and M_2/K be extensions of number fields and $\mathfrak{p} \subset \mathcal{O}_K$ a prime ideal. If \mathfrak{p} is unramified in both M_1 and M_2 , then \mathfrak{p} is unramified in the composite field M_1M_2 .

Example 1.9. Let $K = \mathbb{Q}(\sqrt{-5})$. We want to show the Hilbert class field F is $\mathbb{Q}(\sqrt{-5}, i)$. We know that $h_K = 2$ and $|\text{Gal}(F/K)| = |\text{Cl}(K)| = 2$, so F is a quadratic unramified extension of K . Consider the diagram



Fact. If $\mathfrak{p}_F \subset \mathcal{O}_F$ and $\mathfrak{p}_M \subset \mathcal{O}_M$ with M any of the intermediate fields, and if $p \in \mathbb{Z}$ is such that $\mathfrak{p}_F \mid \mathfrak{p}_M$ and $\mathfrak{p}_M \mid p$, then $e_{\mathfrak{p}_F/p} = e_{\mathfrak{p}_F/\mathfrak{p}_M} e_{\mathfrak{p}_M/p} \leq [F : \mathbb{Q}] = 4$.

Since $\mathbb{Q}(i)/\mathbb{Q}$ has discriminant 8, the only ramified prime is 2. Similarly the only prime that ramifies in $\mathbb{Q}(\sqrt{5})/\mathbb{Q}$ is 5. If $p \neq 2, 5$, then p is unramified in $\mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt{5})$, hence in $\mathbb{Q}(\sqrt{5}, i)$. So p is unramified in $\mathbb{Q}(\sqrt{-5}, i)/\mathbb{Q}(\sqrt{-5})$.

Now $d_{K/\mathbb{Q}} = -20$, so the only ramified primes are 2 and 5. Suppose 2 is ramified in $\mathbb{Q}(\sqrt{-5}, i)/\mathbb{Q}(\sqrt{-5})$. Then $e_{\mathfrak{p}_2/\mathfrak{p}_2} = 2$, where \mathfrak{p}_2 is an ideal in $\mathbb{Q}(\sqrt{-5})$ such that $\mathfrak{p}_2 \mid 2$, $\mathcal{P}_2 \in \mathcal{O}_F$, $\mathcal{P}_2 \mid \mathfrak{p}_2$. Since 2 is unramified in $\mathbb{Q}(\sqrt{5})/\mathbb{Q}$, write \mathfrak{q}_2 for an ideal in $\mathbb{Q}(\sqrt{5})$ such that $\mathfrak{q}_2 \mid 2$. Then $e_{\mathcal{P}_2/2} = e_{\mathcal{P}_2/\mathfrak{q}_2} e_{\mathfrak{q}_2/2} = e_{\mathcal{P}_2/\mathfrak{q}_2} \cdot 1 \leq 2$ since $e_{\mathcal{P}_2/\mathfrak{q}_2}$ is at most $[F : \mathbb{Q}(\sqrt{5})]$. As $e_{\mathcal{P}_2/2} \neq 4$, 2 is unramified in $\mathbb{Q}(\sqrt{-5}, i)/\mathbb{Q}(\sqrt{-5})$. In other words, just look at the diagram above (the notation here is bad but it's an easy example). The case $p = 5$ is similar. Hence $\mathbb{Q}(\sqrt{-5}, i)/\mathbb{Q}(\sqrt{-5})$ is unramified at all finite primes. In $\mathbb{Q}(\sqrt{-5})$ we only have one infinite prime, which is complex, so unramified by definition. Hence $(\sqrt{-5}, i)$ is the Hilbert class field of $\mathbb{Q}(\sqrt{-5})$.

Definition 1.19. The **narrow Hilbert class field** is the maximal abelian extension unramified at all finite primes.

Corollary 1.19. Let f be the Hilbert class field of K . Let \mathfrak{p} be a prime ideal of K . Then \mathfrak{p} splits completely in $F \iff \mathfrak{p}$ is a principal ideal.

We can prove this in two ways: either we deduce this from the decomposition law, or we prove it directly, which we will now do.

Proof. We know \mathfrak{p} splits completely in F if and only if $\left(\frac{F/K}{\mathfrak{p}}\right) = 1$, and $\text{Cl}(K) \cong \text{Gal}(F/K)$. So

$$\left(\frac{F/K}{\mathfrak{p}}\right) = 1 \iff [p] = [1] \text{ in } \text{Cl}(K). \quad \square$$

Theorem 1.20 (Principal ideal theorem). In the Hilbert class field, any ideal \mathfrak{a} of K becomes a principal ideal.

We don't prove this.

Example 1.10. Let $K = \mathbb{Q}(\sqrt{-5})$. Then $\text{Cl}(K) = \langle [\mathcal{O}_K], [(2, 1 + \sqrt{-5})] \rangle$, $F = \mathbb{Q}(\sqrt{-5}, i)$ and $(2, 1 + \sqrt{-5})\mathcal{O}_F$ is generated by $(1 + i)$ in \mathcal{O}_F .

1.1 Reciprocity theorems

Let K be a number field containing a primitive n^{th} root of unity ζ . Then for $\alpha \in \mathcal{O}_K$ coprime to \mathfrak{p} , we have Fermat's little theorem: $\alpha^{N(\mathfrak{p})-1} \equiv 1 \pmod{\mathfrak{p}}$.

Exercise: Suppose $\mathfrak{p} \subset \mathcal{O}_K$, $\alpha \in \mathcal{O}_K$ such that $n, \alpha \notin \mathfrak{p}$. Prove that:

- (i) $1, \zeta, \zeta^{n-1}$ are distinct mod \mathfrak{p} .
- (ii) $n \mid N(\mathfrak{p}) - 1$.
- (iii) $\alpha^{N(\mathfrak{p})-1/n}$ is congruent to a unique n^{th} root of unity mod \mathfrak{p} .

Definition 1.20. This unique root of unity is called the n^{h} power Legendre symbol, written $\left(\frac{\alpha}{\mathfrak{p}}\right)_n$.