Part III - Algebraic Number Theory

Lectured by Hanneke Wiersema

Artur Avameri

Contents

0 Introduction

19 Jan 2024, Lecture 1

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

- 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 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 $\mathcal{P}_1/\mathfrak{p}$. 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 $\mathcal{P}/\mathfrak{p}$ (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 $\mathrm{Gal}(L/K)$ 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

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

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

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

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

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

Proposition 0.1. (i) The Galois group $\mathrm{Gal}((\mathcal{O}_L/\mathcal{P})/(\mathcal{O}_K/\mathfrak{p}))$ is a cyclic group with canonical generator the Frobenius automorphism $x \mapsto x^q$ for $q = |\mathcal{O}_K/\mathfrak{p}|$.

(ii) The map $D_{\mathcal{P}} \overset{\sigma \mapsto \overline{\sigma}}{\to} \mathrm{Gal}((\mathcal{O}_L/\mathcal{P})/(\mathcal{O}_K/\mathfrak{p}))$ 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 $\sigma \in \mathrm{Gal}(L/K)$ 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 $\overline{\sigma} \in \mathrm{Gal}((\mathcal{O}_L/\mathcal{P})/(\mathcal{O}_K/\mathfrak{p}))$ 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 $D_{\mathcal{P}} \overset{(\star)}{\cong} \mathrm{Gal}((\mathcal{O}_L/\mathcal{P})/(\mathcal{O}_K/\mathfrak{p}))$. Recall that $\mathrm{Gal}((\mathcal{O}_L/\mathcal{P})/(\mathcal{O}_K/\mathfrak{p}))$ 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 $\sigma \in \mathrm{Gal}(L/K)$ satisfying this condition will be an element of $D_{\mathcal{P}}$. □

22 Jan 2024, Lecture 2

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 $\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if} a \text{ is a QR mod } p. \\ -1 & \text{if } a \text{ is not a QR mod } p. \text{ Now let } n \in \mathbb{Z} \\ 0 & \text{if } a \equiv 0 \pmod{p}. \end{cases}$ be nonzero and write $= u p_1^{k_1} \dots p_u^{r_u}$ for $u = \pm 1$. Again let a be an integer, then the **Kronecker symbol** is

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

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 $\mathrm{Gal}(L/K)$ has order 2 with $1 : \sqrt{N} \to \sqrt{N}$ and $\sigma : \sqrt{N} \to -\sqrt{N}$ and we can identify $\mathrm{Gal}(L/K)$ 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 $\sigma \in \mathrm{Gal}(L/K)$. 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 $\mathrm{Gal}(L/K)$.

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 $\sigma \in \mathrm{Gal}(L/K)$. 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

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

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** $\mathrm{Cl}(K)$, 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

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

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 $\sigma : K \to \mathbb{R}$ and a complex infinite prime is a pair of conjugate embeddings $\sigma, \overline{\sigma} : K \to \mathbb{C}$ with $\sigma \neq \overline{\sigma}$.

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 $\sigma(\sqrt{-2}) = \sqrt{-2}$, $\overline{\sigma}(\sqrt{-2}) = -\sqrt{-2}$.

Remark. If we have an extension L/K, then an infinite prime σ of K **ramifies** in L is 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 $\mathfrak{m}_\infty$ is a product of distinct real infinite primes.

24 Jan 2024, Lecture 3

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

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 $I_{\mathbb{Q}}(\mathfrak{m}) = \{\left(\frac{a}{b}\right)\mathbb{Z} \mid (a, m) = (b, m) = 1\}$.

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

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

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 $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \cong (\mathbb{Z}/m\mathbb{Z})^\times$ 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 $\Phi_{\mathfrak{m}} : I_{\mathbb{Q}}(\mathfrak{m}) \to \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \cong (\mathbb{Z}/m\mathbb{Z})^\times$.

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 $P_{\mathbb{Q}}(\mathfrak{m}) = \{\left(\frac{a}{b}\right)\mathbb{Z} \in I_{\mathbb{Q}}(\mathfrak{m}) \mid a \equiv b \pmod{m}\}$. 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 $\sigma : K \to \mathbb{C}$, 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 $\sigma : K \to \mathbb{R}$. If $\alpha\beta \neq 0$ and $|\alpha - \beta|_{\mathfrak{p}} < \epsilon$, then $\sigma\left(\frac{a}{b}\right) > 0$.
- 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 $\mathrm{Cl}(K)$ 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

$$1 \to P_{\mathfrak{m}} \to I_K(\mathfrak{m}) \to \mathrm{Cl}(K) \to 1$$
$$1 \to P_{\mathfrak{m}}/P_K(\mathfrak{m}) \to I_K(\mathfrak{m})/P_K(\mathfrak{m}) \to \mathrm{Cl}(K) \to 1.$$

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

26 Jan 2024, Lecture 4

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

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

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

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 $K_\mathfrak{m} \to P_\mathfrak{m}/P_K(\mathfrak{m})$ by $\alpha \mapsto (\alpha)P_K(\mathfrak{m})$. (TODO: add definition of $K_\mathfrak{m}$ defined at the beginning of this lecture during the recap). This is a surjective homomorphism with kernel

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

□

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 $\overline{a}, \overline{b} \in \mathcal{O}_K/\mathfrak{m}_0$ lie in $(\mathcal{O}_K/\mathfrak{m}_0)^\times$. Consider the map

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

for $\overline{\alpha} = \overline{a}\overline{b}^{-1} \in (\mathcal{O}_K/\mathfrak{m}_0)^\times$. 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. $\mathcal{O}_K^\times K_{\mathfrak{m},1}/K_{\mathfrak{m},1} \cong \mathcal{O}_K^\times/(\mathcal{O}_K^\times \cap K_{\mathfrak{m},1})$.

Putting is all together:

$$I_K(\mathfrak{m})/P_K(\mathfrak{m}) \cong (I_K(\mathfrak{m})/P_\mathfrak{m})/(P_K(\mathfrak{m})/P_(\mathfrak{m}))$$

and

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

and

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

by Proposition 1.5.

This gives

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

□

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

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

via the Artin map, so $\ker(\Phi_{\mathfrak{m}}) = P_K(\mathfrak{m})$ (TODO: what is this $\mathbb{Q}(\zeta_m)/\mathbb{Q}$ in the lecture?)

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 $\Phi_\mathfrak{n} : I_K(\mathfrak{n}) \to \mathrm{Gal}(L/K)$ is well–defined and $\Phi_\mathfrak{n} = \Phi_\mathfrak{m}|_{I_K(\mathfrak{m})}$, 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**.