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.