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 $D_{\mathcal{P}}$. $\square$