

# Algebraic Number Theory

Ikhan Choi

May 24, 2024

# Contents

<b>I</b>	<b>Algebraic numbers</b>	<b>2</b>
1	Primes	3
1.1	Local fields . . . . .	3
2	Adèles and idèles	4
3	Galois modules	5
3.1	Profinite groups . . . . .	5
3.2	. . . . .	5
3.3	Galois cohomology . . . . .	5
<b>II</b>	<b>Class field theory</b>	<b>6</b>
4	Local class field theory	7
4.1	Lubin-Tate theory . . . . .	7
4.2	Kronecker-Weber theorem . . . . .	7
5	Global class field theory	8
6		9
<b>III</b>	<b>Arithmetic geometry</b>	<b>10</b>
<b>IV</b>	<b>Langlands program</b>	<b>11</b>
7	Modular forms	12
8	$L$ -functions	13
8.1	Dirichlet $L$ -functions . . . . .	13
9	Automorphic representations	14

## **Part I**

# **Algebraic numbers**

# Chapter 1

## Primes

an order defines a ring class group, a ring class group defines an abelian extension. the conductor of this abelian extension divides the conductor of the order.

### 1.1 Local fields

**1.1 (Absolute value).** Let  $K$  be a field. An *absolute value* or a *multiplicative valuation* on  $K$  is a function  $|\cdot| : K \rightarrow [0, \infty)$  such that

- (i)  $x = 0$  if  $|x| = 0$ ,
- (ii)  $|xy| = |x||y|$ ,
- (iii)  $|x + y| \leq |x| + |y|$ .

Non-archimedean

**1.2 (Local fields).** A *local field* is a locally compact field with a non-trivial absolute value. The Ostrowski theorem states that a local field is one of the followings:

- (i) a finite extension of  $\mathbb{Q}_p$  for a rational prime  $p$ ,
- (ii) a finite extension of  $\mathbb{F}_p((T))$  for a rational prime  $p$ ,
- (iii)  $\mathbb{R}$  or  $\mathbb{C}$ .

Let  $K$  be a non-archimedean local field. Then, the ring of integers  $\mathcal{O}_K$  is a discrete valuation ring, and a generator  $\pi$  of the principal maximal ideal  $\mathfrak{m}_K$  is called the *prime element* or the *uniformizer*.

Local reciprocity law: there is a unique homomorphism

$$\phi_K : K^\times \rightarrow \text{Gal}(K^{\text{ab}}/K) = \varprojlim_L \text{Gal}(L/K)$$

such that

1. for each finite unramified extension  $L$  over  $K$ , which is automatically cyclic,  $\phi_{L/K}(\pi)$  is the Frobenius element in  $\text{Gal}(L/K)$ ,
2. for each finite abelian extension  $L$  over  $K$ , it induces an isomorphism  $\phi_{L/K} : K^\times / \text{Nm}_{L/K}(L^\times) \rightarrow \text{Gal}(L/K)$ .

### 1.3 (Places).

**1.4 (Units in non-archimedean local fields).** Let  $K$  be a non-archimedean local field.  $\mathcal{O}_K$

## **Chapter 2**

# **Adèles and idèles**

## Chapter 3

# Galois modules

### 3.1 Profinite groups

### 3.2

3.1 (Galois modules). (a)  $L, L^\times, \mathcal{O}_L, \mathcal{O}_L^\times$  are all  $\text{Gal}(L/K)$ -modules.

(b) The group of torsion points

3.2 (Normal basis theorem).

### 3.3 Galois cohomology

3.3 (Set of invariants).

3.4 (First cohomology groups).

3.5 (Hilbert 90). (a)  $H^1(\text{Gal}(L/K), L^\times) \cong 0$ .

(b)  $H^1(\text{Gal}(\bar{K}/K), \bar{K}) \cong 0$ .

(c)  $H^1(\text{Gal}(\bar{K}/K), \bar{K}^\times) \cong 0$ .

(d)  $H^1(\text{Gal}(\bar{K}/K), \mu_m) \cong \bar{K}/\bar{K}^\times$ .

*Proof.*

□

## **Part II**

# **Class field theory**

## Chapter 4

# Local class field theory

### 4.1 Lubin-Tate theory

### 4.2 Kronecker-Weber theorem

**4.1 (Local Kronecker-Weber theorem).** Let  $K/\mathbb{Q}_p$  be a finite abelian extension.

Let  $K/\mathbb{Q}$  be a finite abelian extension. A *conductor*  $f(L/K)$  of  $K/\mathbb{Q}$  is the smallest non-negative integer  $n$  such that the higher unit group

$$U^{(n)} = 1 + \mathfrak{m}_K^n$$

is contained in  $N_{L/K}(L^\times)$ .

Let  $m$  be a conductor of a finite abelian extension  $K/\mathbb{Q}$ . Then, we have a surjective group homomorphism

$$\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \rightarrow \mathrm{Gal}(K/\mathbb{Q})$$

by the Kronecker-Weber theorem. For a prime  $p \in \mathbb{Z}$  that does not divide  $m$  so that  $p$  is not ramified, then the decomposition group  $G_p \leq \mathrm{Gal}(K/\mathbb{Q})$  is a cyclic group generated by the Frobenius element  $x \rightarrow x^p$ , denoted by  $\mathrm{Frob}_p$  or  $\left(\frac{K/\mathbb{Q}}{p}\right)$ . Artin map  $I_{\mathbb{Q}}^m \rightarrow \mathrm{Gal}(K/\mathbb{Q})$  of  $K/\mathbb{Q}$  maps each prime  $p \nmid m$  to the Frobenius element  $\mathrm{Frob}_p$ . Artin map factors through  $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \rightarrow \mathrm{Gal}(K/\mathbb{Q})$ !



## **Chapter 5**

# **Global class field theory**

## Chapter 6

## **Part III**

# **Arithmetic geometry**

## **Part IV**

# **Langlands program**

## **Chapter 7**

# **Modular forms**

# Chapter 8

## $L$ -functions

Riemann  $\zeta(s)$   
Dedekind  $\zeta_K(s)$   
Hasse-Weil  $\zeta_X(s)$

### 8.1 Dirichlet $L$ -functions

**8.1** (Hecke character). Dirichlet character can be understood as a group homomorphism  $\chi : \hat{\mathbb{Z}}^\times \rightarrow \mathbb{C}$  of finite order, which means that there is  $n$  such that  $\chi$  factors through  $(\mathbb{Z}/n\mathbb{Z})^\times$ .

In order to construct an  $L$ -function from a character, we need to extend a character as a function of ideals. We interpret  $(\mathbb{Z}/n\mathbb{Z})^\times$  as the ray class group modulo  $\mathfrak{m}$ .

To extend the order of a character to possibly infinite cases, Hecke character is defined a character of an idele class group  $C_K := \mathbb{A}_K^\times / K^\times$ .

Dirichlet (Hecke)  $L$ -functions for ray-class characters  $\chi : C_K \rightarrow \mathbb{C}$ :

$$L(\chi, s) = \sum_{\mathfrak{a}} \frac{\chi(\mathfrak{a})}{N(\mathfrak{a})^s} = \prod_{\mathfrak{p} \text{ prime}} \frac{1}{1 - \chi(\mathfrak{p})N(\mathfrak{p})^{-s}}$$

Artin  $L$ -functions for a Galois representation  $\rho : \text{Gal}(L/K) \rightarrow GL_n(\mathbb{C})$ :

$$L(\rho, s) = \prod_{\mathfrak{p} \text{ prime}} \frac{1}{\det(1 - \rho(\text{Frob}_{\mathfrak{p}})N(\mathfrak{p})^{-s})}$$

Elliptic curves  $L(E, s)$   
Modular forms  $L(f, s)$

## **Chapter 9**

# **Automorphic representations**