Algebraic Number Theory

Ikhan Choi

October 10, 2022

Contents

I Algebraic numbers 2

1 Primes 3
1.1 Ring of integers . . . 3
1.2 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

II Class field theory 6

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

III Arithmetic geometry 10

IV Langlands program 11

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

1.1 Ring of integers

1.1 (Dedekind domains)**.**

1.2 (Ramification theory)**.**

1.2 Local fields

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

(i) $x = 0$ if $|x| = 0$,

(ii) $|xy| = |x||y|$,

(iii) $|x + y| \le |x| + |y|$.

Non-archimedean

1.4 (Local fields)**.** A *local field* is a field with an absolute value with the induced topology that is locally compact.

1.5 (Ostrowski theorem)**.**

1.6 (Places)**.**

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 $\mathrm{Gal}(L/K)$-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) $H^1(\mathrm{Gal}(L/K), L^\times) \cong 0$.

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

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

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

Proof. $\square$

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

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

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 $x \to x^p$, denoted by Frob_p or $\left(\frac{K/\mathbb{Q}}{p}\right)$. Artin map $I_{\mathbb{Q}}^m \to \mathrm{Gal}(K/\mathbb{Q})$ of $K/\mathbb{Q}$ maps each prime $p \nmid m$ to the Frobenius element Frob_p. Artin map factors through $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \to \mathrm{Gal}(K/\mathbb{Q})$!

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 $\chi : \widehat{\mathbb{Z}}^\times \to \mathbb{C}$ of finite order, which means that there is n such that χ 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 $\chi : C_K \to \mathbb{C}$:

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

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

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

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

Chapter 9

Automorphic representations