Algebraic Number Theory

Ikhan Choi

October 1, 2024

Contents

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 $|\cdot| : K \to [0, \infty)$ such that

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

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

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

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

Local reciprocity law: there is a unique homomoprhism

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

such that

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

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 $\mathrm{Gal}(L/K)$-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. □

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* $\mathfrak{f}(L/K)$ 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

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

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

modular forms are sections of some line bundles over a moduli stack $\mathcal{M}$ of complex elliptic curves. By modular forms, we can investigate the algebraic nature of $\mathcal{M}$.

Let $N \geq 1$ and $k \geq 2$. Let $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$ be a Dirichlet character.

Let Γ be a congruence subgroup which acts on $\mathbb{H}$. The vector space of all cusp forms and modular forms weight k with respect to Γ is denoted by $S_k(\Gamma) \subset M_k(\Gamma)$.

Since $\Gamma_1(N)$ acts trivially on $S_k(\Gamma_1(N))$, we have an action of $\Gamma_0(N)/\Gamma_1(N) \cong (\mathbb{Z}/N\mathbb{Z})^\times$ on $S_k(\Gamma_1(N))$, and we define $S_k(N,\chi)$ by the decomposition

$$S_k(\Gamma_1(N)) = \bigoplus_{\chi:(\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times} S_k(N,\chi).$$

We also define $S_k(N) := S_k(N,1) = S_k(\Gamma_0(N))$.

The Hecke operators are defined as a commuting family of endomorphisms $(T_n)_{n=1}^\infty$ on $S_k(\Gamma_1(N))$. Let $f = \sum_{n\geq 1} a_n q^n \in S_k(\Gamma_1(N))$ be a cusp form. We say f is a normalized eigenform if $a_1 = 1$ and it is an eigenvector of Hecke operators, and in this case we have $T_n f = a_n f$. It is known that the field $\mathbb{Q}(f) := \mathbb{Q}(a_n : n \geq 1)$ is a finite extension of $\mathbb{Q}$. We have an L-function given by

$$L(f,s) := \sum_{n\geq 1} a_n n^{-s}.$$

$G_{\mathbb{Q}_p}$ is a subgroup of $G_{\mathbb{Q}}$, called the decomposition group, well-defined up to conjugacy.

Let $f \in S_k(N,\chi)$ be a normalized eigenform, and let $\lambda \mid \ell$ be a place. Then, there is a two-dimensional representation $V_{f,\lambda}$ over an ℓ-adic field $\mathbb{Q}(f)_\lambda$ of $G_{\mathbb{Q}}$ such that

$$\mathrm{Tr}_{V_{f,\lambda}}(\mathrm{Frob}_p) = a_p$$

for every prime p such that $p \nmid N\ell$ and $V_{f,\lambda}$ is unramified at p.

Chapter 8

L-functions

Riemann $\zeta(s)$

Dedekind $\zeta_K(s)$

Hasse-Weil $\zeta_X(s)$

8.1 Dirichlet L-functions

By the Kronecker-Weber theorem, a continuous one-dimensional complex representation $G_{\mathbb{Q}} \to \mathbb{C}^\times$ of the absolute Galois group factors through the Galois group $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$ of some cyclotomic extension to be a Dirichlet character.

We also want to study ℓ-adic Galois representations.

8.1 (Hecke character)**.** Let $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$ be a Dirichlet character. 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