

Notes on Tate's thesis

Erzhuo Wang

September 30, 2024

Abstract

This is a note about John Tate's PhD Thesis published in 1950. It gives a beautiful proof of the functional equation of Hecke L-function by using Fourier Analysis on topological group. As a special case, we can obtain analytic continuation and functional equation of Dedekind zeta functions and Dirchlet L-functions.

Moreover, this theory provide a new proof of Analytic Class Number formula

$$\text{res}_{s=1}\zeta_K(s) = \frac{2^{r_1}(2\pi)^{r_2}h_K R_K}{\omega_K \sqrt{|d_K|}}$$

without using Minkowski Theory which is more elegant that before.

Contents

1	Global Theory	7
1.1	Trace and Norm	7
1.2	Minkowski Thoery	10
1.3	Ramification Theory	16
1.4	Adeles and Ideles	24
2	Local Theory	33
2.1	Topological Group	33
2.2	Valuations	42
2.3	p-adic analysis	53
3	Tate's Thesis	59
3.1	Local characters and Haar Measure	59
3.2	Fourier Transform	62

Chapter 1

Global Theory

1.1 Trace and Norm

Definition 1.1.1 (Trace and Norm). L/K finite fields extension. The trace and norm of an element $x \in L$ are defined to be the trace and determinant, respectively, of the endomorphism

$$T_x : L \rightarrow L, \quad T_x(\alpha) = x\alpha,$$

of the K -vector space L :

$$\mathrm{Tr}_{L|K}(x) = \mathrm{Tr}(T_x), \quad N_{L|K}(x) = \det(T_x).$$

Proposition 1.1.2. In the characteristic polynomial

$$f_x(t) = t^n + a_{n-1}t^{n-1} + \cdots + a_0 \in K[t]$$

of T_x , $n = [L : K]$, we recognize the trace and the norm as

$$-a_{n-1} = \mathrm{Tr}_{L|K}(x) \text{ and } (-1)^n a_0 = N_{L|K}(x).$$

Since $T_{x+y} = T_x + T_y$ and $T_{xy} = T_x \circ T_y$, we obtain homomorphisms

$$\mathrm{Tr}_{L|K} : L \longrightarrow K \quad \text{and} \quad N_{L|K} : L^* \longrightarrow K^*.$$

Proposition 1.1.3. If L/K is a finite separable extension, the characteristic polynomial $f_x(t)$ is a power

$$f_x(t) = p_x(t)^d, \quad d = [L : K(x)]$$

of the minimal polynomial

$$p_x(t) = t^m + c_1 t^{m-1} + \cdots + c_m, \quad m = [K(x) : K]$$

of x .

Proof: In fact, $1, x, \dots, x^{m-1}$ is a basis of $K(x)/K$, and if $\alpha_1, \dots, \alpha_d$ is a basis of $L/K(x)$, then

$$\alpha_1, \alpha_1 x, \dots, \alpha_1 x^{m-1}; \dots; \alpha_d, \alpha_d x, \dots, \alpha_d x^{m-1}$$

is a basis of L/K .

Proposition 1.1.4. If L/K is a finite separable extension and $\sigma : L \rightarrow \bar{K}$ varies over the different K -embeddings of L into an algebraic closure \bar{K} of K , then we have

- (1) $f_x(t) = \prod_{\sigma} (t - \sigma x)$,
- (2) $\text{Tr}_{L|K}(x) = \sum_{\sigma} \sigma x$,
- (3) $N_{L|K}(x) = \prod_{\sigma} \sigma x$.

Proposition 1.1.5. The discriminant of a basis $\alpha_1, \dots, \alpha_n$ of a separable extension $L | K$ is defined by

$$d(\alpha_1, \dots, \alpha_n) = \det((\sigma_i \alpha_j))^2$$

where $\sigma_i, i = 1, \dots, n$, varies over the K -embeddings $L \rightarrow \bar{K}$. Because of the relation

$$\text{Tr}_{L|K}(\alpha_i \alpha_j) = \sum_k (\sigma_k \alpha_i)(\sigma_k \alpha_j),$$

the matrix $(\text{Tr}_{L|K}(\alpha_i \alpha_j))$ is the product of the matrices $(\sigma_k \alpha_i)^t$ and $(\sigma_k \alpha_j)$. Thus one may also write

$$d(\alpha_1, \dots, \alpha_n) = \det(\text{Tr}_{L|K}(\alpha_i \alpha_j)).$$

In the special case of a basis of type $1, \theta, \dots, \theta^{n-1}$ one gets

$$d(1, \theta, \dots, \theta^{n-1}) = \prod_{i < j} (\theta_i - \theta_j)^2,$$

where $\theta_i = \sigma_i \theta$.

Remark 1.1.6. Consider a finite separable extension L/K , $(x, y) = \text{Tr}_{L|K}(xy)$ is a bi-linear function from $L \times L$ to K . Above Proposition tells us this bi-linear function is non-degenerated. Hence for any basis $\{\alpha_1, \dots, \alpha_n\}$,

$$d(\alpha_1, \dots, \alpha_n) \neq 0$$

Proposition 1.1.7. Integrally closed integral domain A with field of fractions K , and to its integral closure B in the finite separable extension $L | K$. If $x \in B$ is an integral element of L , then all of its conjugates σx are also integral. Taking into account that A is integrally closed, i.e., $A = B \cap K$ implies that

$$\text{Tr}_{L|K}(x), \quad N_{L|K}(x) \in A$$

Furthermore, for the group of units of B over A , we obtain the relation

$$x \in B^* \iff N_{L|K}(x) \in A^*.$$

Lemma 1.1.8. Let $\alpha_1, \dots, \alpha_n$ be a basis of L/K which is contained in \mathcal{O}_L , of discriminant $d = d(\alpha_1, \dots, \alpha_n)$. Then one has

$$d\mathcal{O}_L \subseteq \mathcal{O}_K \alpha_1 + \dots + \mathcal{O}_K \alpha_n$$

More generally, if \mathcal{O}_K be an integral domain, K be its fraction field, L/K be a separable extension and \mathcal{O}_L be its integral closure, this Lemma also holds.

Proof: If $\alpha = a_1\alpha_1 + \cdots + a_n\alpha_n \in \mathcal{O}_L$, $a_j \in K$, then the a_j are a solution of the system of linear equations

$$\mathrm{Tr}_{L|K}(\alpha_i\alpha) = \sum_j \mathrm{Tr}_{L|K}(\alpha_i\alpha_j) a_j,$$

Definition 1.1.9 (integral basis). K is an algebraic number field with degree n and all the algebraic integer in K form a subring of K , denoted it by \mathcal{O}_K . For any ideal I of \mathcal{O}_K , there's a basis $\omega_1, \omega_2, \dots, \omega_n$ for K/\mathbb{Q} such that $w_i, i = 1, \dots, n \in \mathcal{O}_K$ and $I = \mathbb{Z}\omega_1 \oplus \cdots \oplus \mathbb{Z}\omega_n$. In particular, every ideal of \mathcal{O}_K is a free \mathbb{Z} -module of rank n . We call basis of \mathcal{O}_K as free abelian group integral basis of \mathcal{O}_K

Definition 1.1.10 (discriminant of number field). Define $d_K = d(\omega_1, \omega_2, \dots, \omega_n)$, where $\omega_1, \omega_2, \dots, \omega_n$ is an integral basis of \mathcal{O}_K .

Proposition 1.1.11. Let L/\mathbb{Q} and L'/\mathbb{Q} be two Galois extensions of degree n , resp. n' , such that $L \cap L' = K$. Let $\omega_1, \dots, \omega_n$, resp. $\omega'_1, \dots, \omega'_{n'}$, be an integral basis of $L | \mathbb{Q}$, resp. $L' | \mathbb{Q}$, with discriminant d , resp. d' . Suppose that d and d' are relatively prime. Then $\omega_i\omega'_j$ is an integral basis of LL' , of discriminant $d^n d'^n$.

Example 1.1.12. integral basis of quadratic number field Let D be a squarefree rational integer $\neq 0, 1$ and d the discriminant of the quadratic number field $K = \mathbb{Q}(\sqrt{D})$. Show that

$$\begin{aligned} d &= D, & \text{if } D \equiv 1 \pmod{4}, \\ d &= 4D, & \text{if } D \equiv 2 \text{ or } 3 \pmod{4}, \end{aligned}$$

and that an integral basis of K is given by $\{1, \sqrt{D}\}$ in the second case, by $\{1, \frac{1}{2}(1 + \sqrt{D})\}$ in the first case, and by $\{1, \frac{1}{2}(d + \sqrt{d})\}$ in both cases.

Theorem 1.1.13. Assume $f(x) = x^n + \alpha x + b \in \mathbb{Q}[x]$ is a irreducible polynomial, θ is a root of $f(x)$. Then $\mathbb{Q}(\theta)$ is an algebraic number field. In the extension $\mathbb{Q}(\theta)/\mathbb{Q}$,

$$d(1, \theta, \dots, \theta^{n-1}) = d(f) = (-1)^{n(n-1)/2} [(-1)^{n-1}(n-1)^{n-1}a^n + n^n b^{n-1}]$$

In particular, when $n = 3$, $d(1, \theta, \theta^2) = -(4a^3 + 27b^2)$.

Proposition 1.1.14. The ring \mathcal{O}_K is noetherian, integrally closed, and $\dim \mathcal{O}_K = 1$.

Proof: Noetherian: since every ideal is a free \mathbb{Z} -module of rank $[K : \mathbb{Q}]$.

integrally closed: $\alpha \in K$ integral over \mathcal{O}_K , then $\mathcal{O}_K[\alpha]$ is integral over \mathcal{O}_K , hence over \mathbb{Z} .

$\dim = 1$: It thus remains to show that each prime ideal $p \neq 0$ is maximal. Now, $p \cap \mathbb{Z}$ is a nonzero prime ideal (p) in \mathbb{Z} : the primality is clear, and if $y \in p, y \neq 0$, and

$$y^n + a_1 y^{n-1} + \cdots + a_n = 0$$

is an equation for y with $a_i \in \mathbb{Z}, a_n \neq 0$, then $a_n \in p \cap \mathbb{Z}$. The integral domain $\overline{\mathcal{O}} = \mathcal{O}_K/p$ is a field also follows from above equation.

Proposition 1.1.15. (1)

$$\mathfrak{N}((\alpha)) = |N_{K|\mathbb{Q}}(\alpha)|$$

(2) If $\mathfrak{a} = \mathfrak{p}_1^{\nu_1} \cdots \mathfrak{p}_r^{\nu_r}$ is the prime factorization of an ideal $\mathfrak{a} \neq 0$, then one has

$$\mathfrak{N}(\mathfrak{a}) = \mathfrak{N}(\mathfrak{p}_1)^{\nu_1} \cdots \mathfrak{N}(\mathfrak{p}_r)^{\nu_r}$$

1.2 Minkowski Thoery

Definition 1.2.1 (Lattice). Let V be an n -dimensional \mathbb{R} -vector space. A lattice in V is a subgroup of the form

$$\Gamma = \mathbb{Z}v_1 + \cdots + \mathbb{Z}v_m$$

with linearly independent vectors v_1, \dots, v_m of V . The m -tuple (v_1, \dots, v_m) is called a basis and the set

$$\Phi = \{x_1v_1 + \cdots + x_mv_m \mid x_i \in \mathbb{R}, 0 \leq x_i < 1\}$$

a fundamental mesh of the lattice. The lattice is called complete or a \mathbb{Z} structure of V , if $m = n$.

Definition 1.2.2 (Haar measure on euclidean space). Now let V be a euclidean vector space, i.e., an \mathbb{R} -vector space of finite dimension n equipped with a symmetric, positive definite bilinear form

$$\langle, \rangle : V \times V \longrightarrow \mathbb{R}$$

Then we have on V a notion of volume - more precisely a Haar measure. The cube spanned by an orthonormal basis e_1, \dots, e_n has volume 1, and more generally, the parallelepiped spanned by n linearly independent vectors v_1, \dots, v_n ,

$$\Phi = \{x_1v_1 + \cdots + x_nv_n \mid x_i \in \mathbb{R}, 0 \leq x_i < 1\}$$

has volume

$$\text{vol}(\Phi) = |\det A|,$$

where $A = (a_{ij})$ is the matrix of the base change from e_1, \dots, e_n to v_1, \dots, v_n .

Also,

$$\text{vol}(\Phi) = |\det (\langle v_i, v_j \rangle)|^{1/2}$$

Let Γ be the lattice spanned by v_1, \dots, v_n . Then Φ is a fundamental mesh of Γ , and we write for short

$$\text{vol}(\Gamma) = \text{vol}(\Phi)$$

Theorem 1.2.3 (Minkowski's Lattice Point Theorem). Let Γ be a complete lattice in the euclidean vector space V and X a centrally symmetric, convex, measurable subset of V . Suppose that

$$\text{vol}(X) > 2^n \text{vol}(\Gamma).$$

Then X contains at least one nonzero lattice point $\gamma \in \Gamma$.

Moreover, if in addition X is compact, we only need

$$\text{vol}(X) \geq 2^n \text{vol}(\Gamma)$$

Example 1.2.4 (Minkowski's Theorem on Linear Forms). Let

$$L_i(x_1, \dots, x_n) = \sum_{j=1}^n a_{ij}x_j, \quad i = 1, \dots, n,$$

be real linear forms such that $\det(a_{ij}) \neq 0$, and let c_1, \dots, c_n be positive real numbers such that $c_1 \cdots c_n > |\det(a_{ij})|$. Show that there exist integers $m_1, \dots, m_n \in \mathbb{Z}$ such that

$$|L_i(m_1, \dots, m_n)| < c_i, \quad i = 1, \dots, n.$$

Definition 1.2.5 (Minkowski space). Minkowski space $K_{\mathbb{R}}$ can be given in the following manner. Some of the embeddings $\tau : K \rightarrow \mathbb{C}$ are real in that they land already in \mathbb{R} , and others are complex, i.e., not real. Let

$$\rho_1, \dots, \rho_r : K \longrightarrow \mathbb{R}$$

be the real embeddings. The complex ones come in pairs

$$\sigma_1, \bar{\sigma}_1, \dots, \sigma_s, \bar{\sigma}_s : K \longrightarrow \mathbb{C}$$

of complex conjugate embeddings. Thus $n = r + 2s$. Define

$$K_{\mathbb{R}} = \left\{ (z_{\tau}) \in \prod_{\tau} \mathbb{C} \mid z_{\rho} \in \mathbb{R}, z_{\bar{\sigma}} = \bar{z}_{\sigma} \right\}$$

And there's canonical map

$$f : K \rightarrow K_{\mathbb{R}} \quad x \mapsto (\rho_1(x), \dots, \rho_r(x), \sigma_1(x), \bar{\sigma}_1(x), \dots, \sigma_s(x), \bar{\sigma}_s(x))$$

Definition 1.2.6. $K_{\mathbb{C}}$ with canonical map and Hermitian inner product is defined to be

$$j : K \longrightarrow K_{\mathbb{C}} := \prod_{\tau} \mathbb{C}, \quad a \longmapsto ja = (\tau a),$$

$$\langle x, y \rangle = \sum_{\tau} x_{\tau} \bar{y}_{\tau}.$$

$K_{\mathbb{R}}$ is a \mathbb{R} -subspace with inner product $K_{\mathbb{R}} \times K_{\mathbb{R}} \rightarrow \mathbb{R}$.

Proposition 1.2.7. If $\mathfrak{a} \neq 0$ is an ideal of \mathcal{O}_K , then $\Gamma = j\mathfrak{a}$ is a complete lattice in $K_{\mathbb{R}}$. Its fundamental mesh has volume

$$\text{vol}(\Gamma) = \sqrt{|d_K|} (\mathcal{O}_K : \mathfrak{a})$$

Proposition 1.2.8. Let $\mathfrak{a} \neq 0$ be an integral ideal of K , and let $c_\tau > 0$, for $\tau \in \text{Hom}(K, \mathbb{C})$, be real numbers such that $c_\tau = c_{\bar{\tau}}$ and

$$\prod_{\tau} c_\tau > A(\mathcal{O}_K : \mathfrak{a})$$

where $A = \left(\frac{2}{\pi}\right)^s \sqrt{|d_K|}$. Then there exists $a \in \mathfrak{a}, a \neq 0$, such that

$$|\tau a| < c_\tau \quad \text{for all } \tau \in \text{Hom}(K, \mathbb{C}).$$

Proof: The set $X = \{(z_\tau) \in K_{\mathbb{R}} : |z_\tau| < c_\tau\}$ is centrally symmetric and convex. Its volume $\text{vol}(X)$ can be computed via the map

$$f : K_{\mathbb{R}} \xrightarrow{\sim} \prod_{\tau} \mathbb{R}, \quad (z_\tau) \mapsto (x_\tau),$$

given by $x_\rho = z_\rho, x_\sigma = \text{Re}(z_\sigma), x_{\bar{\sigma}} = \text{Im}(z_\sigma)$. It comes out to be 2^s times the Lebesgue-volume of the image

$$f(X) = \left\{ (x_\tau) \in \prod_{\tau} \mathbb{R} : |x_\rho| < c_\rho, x_\sigma^2 + x_{\bar{\sigma}}^2 < c_\sigma^2 \right\}.$$

This gives

$$\text{vol}(X) = 2^s \text{vol}_{\text{Lebesgue}}(f(X)) = 2^s \prod_{\rho} (2c_\rho) \prod_{\sigma} (\pi c_\sigma^2) = 2^{r+s} \pi^s \prod_{\tau} c_\tau.$$

Lemma 1.2.9. In Minkowski space

$$K_{\mathbb{R}} = \left[\prod_{\tau} \mathbb{C} \right]^+$$

, the domain

$$X_t = \left\{ (z_\tau) \in K_{\mathbb{R}} : \sum_{\tau} |z_\tau| < t \right\}$$

has volume

$$\text{vol}(X_t) = 2^r \pi^s \frac{t^n}{n!}.$$

Proof: By Change of Variables, it suffices to figure out

$$I(t) = \int u_1 \cdots u_s dx_1 \cdots dx_r du_1 \cdots du_s d\theta_1 \cdots d\theta_s$$

extended over the domain

$$|x_1| + \cdots + |x_r| + 2u_1 + \cdots + 2u_s \leq t.$$

Restricting this domain of integration to $x_i \geq 0$, the integral gets divided by 2^r . Substituting $2u_j = w_j$ gives

$$I(t) = 2^r 4^{-s} (2\pi)^s I_{r,s}(t),$$

where the integral

$$I_{r,s}(t) = \int w_1 \cdots w_s dx_1 \cdots dx_r dw_1 \cdots dw_s$$

has to be taken over the domain $x_i \geq 0, w_j \geq 0$ and

$$\begin{aligned} x_1 + \cdots + x_r + w_1 + \cdots + w_s &\leq t \\ I_{r,s}(1) &= \int_0^1 I_{r-1,s}(1-x_1) dx_1 = \int_0^1 (1-x_1)^{n-1} dx_1 \cdot I_{r-1,s}(1) \\ &= \frac{1}{n} I_{r-1,s}(1) \end{aligned}$$

By induction, this implies that

$$I_{r,s}(1) = \frac{1}{n(n-1) \cdots (n-r+1)} I_{0,s}(1).$$

In the same way, one gets

$$I_{0,s}(1) = \int_0^1 w_1 (1-w_1)^{2s-2} dw_1 I_{0,s-1}(1),$$

and, doing the integration, induction shows that

$$I_{0,s}(1) = \frac{1}{(2s)!} I_{0,0}(1) = \frac{1}{(2s)!}.$$

Proposition 1.2.10. Show that in every ideal $\mathfrak{a} \neq 0$ of \mathcal{O}_K , there exists an $a \neq 0$ such that

$$|N_{K|\mathbb{Q}}(a)| \leq M (\mathcal{O}_K : \mathfrak{a}),$$

where

$$M = \frac{n!}{n^n} \left(\frac{4}{\pi} \right)^s \sqrt{|d_K|}$$

(the so-called Minkowski bound).

Proof: By Lattice Point Theorem and Lemma 1.2.9.

Remark 1.2.11. If we write

$$\mathfrak{a} = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r},$$

$0 \neq \alpha \in \mathfrak{a}$ means

$$(a) = \mathfrak{P}_1^{e_1+u_1} \cdots \mathfrak{P}_r^{e_r+u_r} \mathfrak{Q}_1^{f_1} \cdots \mathfrak{Q}_r^{f_r}, (\mathfrak{P}_i, \mathfrak{Q}_j) = 1.$$

Hence above inequality becomes

$$\mathfrak{N}(\mathfrak{P}_1)^{u_1} \cdots \mathfrak{N}(\mathfrak{P}_r)^{u_r} \mathfrak{N}(\mathfrak{Q}_1)^{f_1} \cdots \mathfrak{N}(\mathfrak{Q}_r)^{f_r} \leq M$$

That is to say, every integral ideal can be multiplied by a integral ideal whose norm $\leq M$ such that it becomes a integral principal ideal.

Proposition 1.2.12. The ideal class group $Cl_K = J_K/P_K$ is finite. Its order

$$h_K = (J_K : P_K)$$

is called the class number of K .

Proof: If $\mathfrak{p} \neq 0$ is a prime ideal of \mathcal{O}_K and $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$, then $\mathcal{O}_K/\mathfrak{p}$ is a finite field extension of $\mathbb{Z}/p\mathbb{Z}$ of degree, say, $f \geq 1$, and we have

$$\mathfrak{N}(\mathfrak{p}) = p^f.$$

Given p , there are only finitely many prime ideals \mathfrak{p} such that $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$, because this means that $\mathfrak{p} \mid (p)$. It follows that there are only finitely many prime ideals p of bounded absolute norm. Since every integral ideal admits a representation $a = p_1^{\nu_1} \cdots p_r^{\nu_r}$ where $\nu_i > 0$ and

$$\mathfrak{N}(\mathfrak{a}) = \mathfrak{N}(\mathfrak{p}_1)^{\nu_1} \cdots \mathfrak{N}(\mathfrak{p}_r)^{\nu_r},$$

there are altogether only a finite number of ideals \mathfrak{a} of \mathcal{O}_K with bounded absolute norm $\mathfrak{N}(\mathfrak{a}) \leq M$.

It therefore suffices to show that each class $[\mathfrak{a}] \in Cl_K$ contains an integral ideal \mathfrak{a}_1 satisfying

$$\mathfrak{N}(\mathfrak{a}_1) \leq M = \frac{n!}{n^n} \left(\frac{4}{\pi} \right)^s \sqrt{|d_K|}$$

Then this result follows from Remark 1.2.11.

Corollary 1.2.13. The discriminant of an algebraic number field K of degree n satisfies

$$|d_K|^{1/2} \geq \frac{n^n}{n!} \left(\frac{\pi}{4} \right)^{n/2}.$$

Definition 1.2.14. The \mathbb{R} -vector space $[\prod_{\tau} \mathbb{R}]^+$ is explicitly given as follows. Separate as before the embeddings $\tau : K \rightarrow \mathbb{C}$ into real ones, ρ_1, \dots, ρ_r , and pairs of complex conjugate ones, $\sigma_1, \bar{\sigma}_1, \dots, \sigma_s, \bar{\sigma}_s$. We obtain a decomposition which is analogous to the one we saw above for $[\prod_{\tau} \mathbb{C}]^+$,

$$\left[\prod_{\tau} \mathbb{R} \right]^+ = \prod_{\rho} \mathbb{R} \times \prod_{\sigma} [\mathbb{R} \times \mathbb{R}]^+$$

The factor $[\mathbb{R} \times \mathbb{R}]^+$ now consists of the points (x, x) , and we identify it with \mathbb{R} by the map $(x, x) \mapsto 2x$. In this way we obtain an isomorphism.

$$\left[\prod_{\tau} \mathbb{R} \right]^+ \cong \mathbb{R}^{r+s}$$

Definition 1.2.15. Consider a commutative diagram as follow:

$$\begin{array}{ccccc} K^* & \xrightarrow{j} & K_{\mathbb{R}}^* & \xrightarrow{l} & [\prod_{\tau} \mathbb{R}]^+ \\ N_{K/\mathbb{Q}} \downarrow & & N \downarrow & & \downarrow \text{Tr} \\ \mathbb{Q}^* & \longrightarrow & \mathbb{R}^* & \xrightarrow{\log |\cdot|} & \mathbb{R} \end{array}$$

where $l : K_{\mathbb{R}}^* \rightarrow [\prod_{\tau} \mathbb{R}]^+ : (z_{\tau}) \mapsto (\log(|z_{\tau}|))$ and Tr is sum of the elements in $[\prod_{\tau} \mathbb{R}]^+$.

In the upper part of the diagram we consider the subgroups

$$\begin{aligned} \mathcal{O}_K^* &= \{\varepsilon \in \mathcal{O}_K \mid N_{K|\mathbb{Q}}(\varepsilon) = \pm 1\}, & \text{the group of units,} \\ S &= \{y \in K_{\mathbb{R}}^* \mid N(y) = \pm 1\}, & \text{the "norm-one surface",} \\ H &= \{x \in [\prod_{\tau} \mathbb{R}]^+ \mid \text{Tr}(x) = 0\}, & \text{the "trace-zero hyperplane".} \end{aligned}$$

We obtain the homomorphisms

$$\mathcal{O}_K^* \xrightarrow{j} S \xrightarrow{\ell} H$$

and the composite $\lambda := \ell \circ j : \mathcal{O}_K^* \rightarrow H$. The image will be denoted by

$$\Gamma = \lambda(\mathcal{O}_K^*) \subseteq H$$

Proposition 1.2.16 (roots of unit). The sequence

$$1 \rightarrow \mu(K) \rightarrow \mathcal{O}_K^* \xrightarrow{\lambda} \Gamma \rightarrow 0$$

is exact, where $\mu(K)$ is the roots of unity lie in K .

Definition 1.2.17 (Dirchlet Unit Theorem). The group Γ is a complete lattice in the $(r+s-1)$ dimensional vector space H , and is therefore isomorphic to \mathbb{Z}^{r+s-1} .

Definition 1.2.18 (regulator). Identifying $[\prod_{\tau} \mathbb{R}]^+ = \mathbb{R}^{r+s}$, H becomes a subspace of the euclidean space \mathbb{R}^{r+s} and thus itself a euclidean space. We may therefore speak of the volume of the fundamental mesh $\text{vol}(\lambda(\mathcal{O}_K^*))$ of the unit lattice $\Gamma = \lambda(\mathcal{O}_K^*) \subseteq H$, and will now compute it. Let $\varepsilon_1, \dots, \varepsilon_t, t = r+s-1$, be a system of fundamental units and Φ the fundamental mesh of the unit lattice $\lambda(\mathcal{O}_K^*)$, spanned by the vectors $\lambda(\varepsilon_1), \dots, \lambda(\varepsilon_t) \in H$. The vector

$$\lambda_0 = \frac{1}{\sqrt{r+s}}(1, \dots, 1) \in \mathbb{R}^{r+s}$$

is obviously orthogonal to H and has length 1. The t -dimensional volume of Φ therefore equals the $(t+1)$ -dimensional volume of the parallelepiped spanned by $\lambda_0, \lambda(\varepsilon_1), \dots, \lambda(\varepsilon_t)$ in \mathbb{R}^{t+1} . But this has volume

$$\left| \det \begin{pmatrix} \lambda_{01} & \lambda_1(\varepsilon_1) & \cdots & \lambda_1(\varepsilon_t) \\ \vdots & \vdots & & \vdots \\ \lambda_{0t+1} & \lambda_{t+1}(\varepsilon_1) & \cdots & \lambda_{t+1}(\varepsilon_t) \end{pmatrix} \right|$$

where $[\lambda_1(\varepsilon_i), \dots, \lambda_{t+1}(\varepsilon_i)] = \lambda(\varepsilon_i) \in \mathbb{R}^{r+s}$. Adding all rows to a fixed one, say the i -th row, this row has only zeroes, except for the first entry, which equals $\sqrt{r+s}$. We therefore get the the volume of the fundamental mesh of the unit lattice $\lambda(\mathcal{O}_K^*)$ in H is

$$\text{vol}(\lambda(\mathcal{O}_K^*)) = \sqrt{r+s} R$$

where R is the absolute value of the determinant of an arbitrary $t = r+s-1$ rows of the following matrix:

$$\begin{pmatrix} \lambda_1(\varepsilon_1) & \cdots & \lambda_1(\varepsilon_t) \\ \vdots & & \vdots \\ \lambda_{t+1}(\varepsilon_1) & \cdots & \lambda_{t+1}(\varepsilon_t) \end{pmatrix}.$$

This absolute value R is called the regulator of the field K .

Definition 1.2.19 (cyclotomic units). Let ζ be a primitive m -th root of unity, $m \geq 3$. Show that the numbers $\frac{1-\zeta^k}{1-\zeta}$ for $(k, m) = 1$ are units in the ring of integers of the field $\mathbb{Q}(\zeta)$. The subgroup of the group of units they generate is called the group of cyclotomic units.

1.3 Ramification Theory

Assume some notations: L/K is an extension of number field, $\mathcal{O}_L, \mathcal{O}_K$ are ring of integers of L and K respectively. For $0 \neq \mathfrak{p} \in \text{Spec}(\mathcal{O}_K)$, denote the ideal generated by \mathfrak{p} by in \mathcal{O}_L by $\mathfrak{p}\mathcal{O}_L$.

Proposition 1.3.1. $\mathfrak{p}\mathcal{O}_L \neq \mathcal{O}_L$ and $\mathfrak{p}\mathcal{O}_L \cap \mathcal{O}_K = \mathfrak{p}$.

Proof: Take $\pi \in \mathfrak{p} - \mathfrak{p}^2$, we have $(\pi) = \mathfrak{p}\mathfrak{a}$, where $(\mathfrak{p}, \mathfrak{a}) = (1)$. Take $b + s = 1, b \in \mathfrak{p}, s \in \mathfrak{a}$. Then

$$s\mathcal{O}_L = s\mathfrak{p}\mathcal{O}_L \subset \pi\mathcal{O}_L$$

Hence there's $x \in \mathcal{O}_L$ such that $s = \pi x$, which implies $x \in K \cap \mathcal{O}_L = \mathcal{O}_K$. Hence $s \in \mathfrak{p}$, a contradiction!

Proposition 1.3.2. \mathfrak{P} is an ideal of \mathcal{O}_L , Let $\mathfrak{P} \cap \mathcal{O}_K = \mathfrak{p}$, and $e = e(\mathfrak{P}/\mathfrak{p})$. Then $\mathfrak{P}^t \cap \mathcal{O}_K = \mathfrak{p}^d$, where $d = \lceil \frac{t}{e} \rceil$.

Proof: Notice that

$$x \in \mathfrak{P}^t \cap \mathcal{O}_K \iff x \in \mathcal{O}_K, \mathfrak{P}^t \supset x\mathcal{O}_L \iff x \in \mathcal{O}_K, \mathfrak{p}^d \supset x\mathcal{O}_K \text{ with } de \geq t$$

Corollary 1.3.3. \mathfrak{A} is an ideal of \mathcal{O}_K , then $\mathfrak{A}\mathcal{O}_L \cap \mathcal{O}_K = \mathfrak{A}$

Corollary 1.3.4. If $\mathfrak{A} = \mathfrak{p}\mathcal{O}_L$ and \mathfrak{B} are coprime in \mathcal{O}_L , then $\mathfrak{A} \cap \mathcal{O}_K$ and $\mathfrak{B} \cap \mathcal{O}_K$ are coprime in \mathcal{O}_K .

Definition 1.3.5. A prime ideal $\mathfrak{p} \neq 0$ of the ring \mathcal{O}_K decomposes in \mathcal{O}_L in a unique way into a product of prime ideals,

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}.$$

The prime ideals \mathfrak{P}_i occurring in the decomposition are precisely those prime ideals \mathfrak{P} of \mathcal{O}_L which lie over \mathfrak{p} in the sense that one has the relation

$$\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_K.$$

This we also denote for short by $\mathfrak{P} \mid \mathfrak{p}$, and we call \mathfrak{P} a prime divisor of \mathfrak{p} . The exponent e_i is called the ramification index, and the degree of the field extension

$$f_i = [\mathcal{O}_L/\mathfrak{P}_i : \mathcal{O}_K/\mathfrak{p}]$$

Theorem 1.3.6 (fundamental identity).

$$\sum_{i=1}^r e_i f_i = n.$$

Theorem 1.3.7. Suppose now that the number field extension L/K which is given by a primitive element $\theta \in \mathcal{O}_L$ with minimal polynomial

$$p(X) \in \mathcal{O}_K[X],$$

so that $L = K(\theta)$.

First, conductor is defined to be the biggest ideal \mathfrak{F} of \mathcal{O}_L which is contained in $\mathcal{O}[\theta]$. In other words

$$\mathfrak{F} = \{\alpha \in \mathcal{O}_L : \alpha \mathcal{O}_L \subseteq \mathcal{O}_K[\theta]\}$$

To show \mathfrak{F} is non-zero, we consider $1, \theta, \dots, \theta^{n-1}$ a basis of L/K . By Lemma 1.1.8, we have

$$d(1, \theta, \dots, \theta^{n-1}) \mathcal{O}_L \subset \mathcal{O}_K + \dots + \mathcal{O}_K \theta^{n-1} = \mathcal{O}_K[\theta].$$

Hence $d(1, \theta, \dots, \theta^{n-1}) \in \mathfrak{F}$

Let \mathfrak{p} be a prime ideal of \mathcal{O} which is relatively prime to the conductor \mathfrak{F} and let

$$\bar{p}(X) = \bar{p}_1(X)^{e_1} \dots \bar{p}_r(X)^{e_r}$$

be the factorization of the polynomial $\bar{p}(X) = p(X) \bmod \mathfrak{p}$ into irreducibles $\bar{p}_i(X) = p_i(X) \bmod \mathfrak{p}$ over the residue class field $\mathcal{O}_K/\mathfrak{p}$, with all $p_i(X) \in \mathcal{O}_K[X]$ monic. Then

$$\mathfrak{P}_i = \mathfrak{p} \mathcal{O}_L + p_i(\theta) \mathcal{O}_L, \quad i = 1, \dots, r,$$

are the different prime ideals of \mathcal{O}_L above \mathfrak{p} . The inertia degree f_i of \mathfrak{P}_i is the degree of $\bar{p}_i(X)$, and one has

$$\mathfrak{p} = \mathfrak{P}_1^{e_1} \dots \mathfrak{P}_r^{e_r}.$$

Corollary 1.3.8. If $K = \mathbb{Q}$, $p \nmid |\mathcal{O}_L/\mathcal{O}_K[\alpha]|$ implies $p\mathcal{O}_L$ is coprime to \mathfrak{F} .

Proof: Let $d = |\mathcal{O}_L/\mathcal{O}_K[\alpha]|$, since $(p) + (d) = (1)$, we have $p\mathcal{O}_L + d\mathcal{O}_L = \mathcal{O}_L$. Notice that $d\mathcal{O}_L \subset \mathfrak{F}$, we have

$$\mathfrak{F} + p\mathcal{O}_L = \mathcal{O}_L$$

Definition 1.3.9. The prime ideal \mathfrak{p} is said to split completely (or to be **totally split**) in L , if in the decomposition

$$\mathfrak{p} = \mathfrak{P}_1^{e_1} \dots \mathfrak{P}_r^{e_r},$$

one has $r = n = [L : K]$, so that $e_i = f_i = 1$ for all $i = 1, \dots, r$.

\mathfrak{p} is called nonsplit, or indecomposed, if $r = 1$, i.e., if there is only a single prime ideal of L over \mathfrak{p} .

The prime ideal \mathfrak{P}_i in the decomposition $\mathfrak{p} = \prod_{i=1}^r \mathfrak{P}_i^{e_i}$ is called **unramified** over \mathcal{O}_K if $e_i = 1$. If not, it is called **ramified**, and **totally ramified** if furthermore $f_i = 1$.

The prime ideal \mathfrak{p} is called unramified if all \mathfrak{P}_i are unramified, otherwise it is called ramified.

Theorem 1.3.10. p unramified over K if and only if p divides d_K .

Theorem 1.3.11. Assume $K = \mathbb{Q}(\sqrt{d})$, p is a prime number.

(1) If $p \mid d(K)$, $p\mathcal{O}_K = \mathfrak{P}^2$, $\mathfrak{N}(\mathfrak{P}) = p$, i.e. p is ramified over K .

(2) If $p \geq 3$, and $p \nmid d(K)$

(a) if $\left(\frac{d}{p}\right) = 1$, $p\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2$, where $\mathfrak{p}_1 \neq \mathfrak{p}_2$, $N(\mathfrak{p}_1) = N(\mathfrak{p}_2) = p$.

(b) if $\left(\frac{d}{p}\right) = -1$, $p\mathcal{O}_K = \mathfrak{p}$, $N(\mathfrak{p}) = p^2$.

(3) If $p = 2$ and $p \nmid d(K)$, then $d \equiv 1 \pmod{4}$.

(a) if $d \equiv 1 \pmod{8}$, 2 is totally split.

(b) if $d \equiv 5 \pmod{8}$, $2\mathcal{O}_K$ is a prime ideal.

Proposition 1.3.12. Let L/K be a Galois extension. The Galois group G acts transitively on the set of all prime ideals \mathfrak{P} of \mathcal{O} lying above p , i.e., these prime ideals are all conjugates of each other.

Proof: Let \mathfrak{P} and \mathfrak{P}' be two prime ideals above \mathfrak{p} . Assume $\mathfrak{P}' \neq \sigma\mathfrak{P}$ for any $\sigma \in G$. By the Chinese remainder theorem there exists $x \in \mathcal{O}$ such that $x \equiv 0 \pmod{\mathfrak{P}'}$ and $x \equiv 1 \pmod{\sigma\mathfrak{P}}$ for all $\sigma \in G$. Then the norm $N_{L|K}(x) = \prod_{\sigma \in G} \sigma x$ belongs to $\mathfrak{P}' \cap \mathcal{O}_K = \mathfrak{p}$. On the other hand, $x \notin \sigma\mathfrak{P}$ for any $\sigma \in G$, hence $\sigma x \notin \mathfrak{P}$ for any $\sigma \in G$. Consequently $\prod_{\sigma \in G} \sigma x \notin \mathfrak{P} \cap \mathcal{O}_K = \mathfrak{p}$, a contradiction.

Definition 1.3.13. If \mathfrak{P} is a prime ideal of \mathcal{O} , then the subgroup

$$G_{\mathfrak{P}} = \{\sigma \in G \mid \sigma\mathfrak{P} = \mathfrak{P}\}$$

is called the decomposition group of \mathfrak{P} over K . The fixed field

$$Z_{\mathfrak{P}} = \{x \in L \mid \sigma x = x \text{ for all } \sigma \in G_{\mathfrak{P}}\}$$

is called the decomposition field of \mathfrak{P} over K .

Proposition 1.3.14. $[G : G_{\mathfrak{P}}]$ = the number of prime ideal over \mathfrak{p} . In particular, one has

$$G_{\mathfrak{P}} = 1 \iff Z_{\mathfrak{P}} = L \iff \mathfrak{p} \text{ is totally split,}$$

$$G_{\mathfrak{P}} = G \iff Z_{\mathfrak{P}} = K \iff \mathfrak{p} \text{ is nonsplit.}$$

Proposition 1.3.15. In the Galois case, the inertia degrees f_1, \dots, f_r and the ramification indices e_1, \dots, e_r in the prime decomposition

$$\mathfrak{p} = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$$

of a prime ideal \mathfrak{p} of K are both independent of i ,

$$f_1 = \cdots = f_r = f, \quad e_1 = \cdots = e_r = e$$

In fact, writing $\mathfrak{P} = \mathfrak{P}_1$, we find $\mathfrak{P}_i = \sigma_i \mathfrak{P}$ for suitable $\sigma_i \in G$, and the isomorphism $\sigma_i : \mathcal{O} \rightarrow \mathcal{O}$ induces an isomorphism

$$\mathcal{O}/\mathfrak{P} \xrightarrow{\sim} \mathcal{O}/\sigma_i \mathfrak{P}, \quad a \bmod \mathfrak{P} \mapsto \sigma_i a \bmod \sigma_i \mathfrak{P},$$

so that

$$f_i = [\mathcal{O}/\sigma_i \mathfrak{P} : \mathcal{O}/\mathfrak{p}] = [\mathcal{O}/\mathfrak{P} : \mathcal{O}/\mathfrak{p}], \quad i = 1, \dots, r$$

Furthermore, since $\sigma_i(\mathfrak{p}\mathcal{O}) = \mathfrak{p}\mathcal{O}$, we deduce from

$$\mathfrak{P}^\nu | \mathfrak{p}\mathcal{O} \iff \sigma_i(\mathfrak{P}^\nu) | \sigma_i(\mathfrak{p}\mathcal{O}) \iff (\sigma_i \mathfrak{P})^\nu | \mathfrak{p}\mathcal{O}$$

the equality of the $e_i, i = 1, \dots, r$. Thus the prime decomposition of \mathfrak{p} in \mathcal{O} takes on the following simple form in the Galois case:

$$\mathfrak{p} = \left(\prod_{\sigma} \sigma \mathfrak{P} \right)^e$$

where σ varies over a system of representatives of $G/G_{\mathfrak{P}}$.

Proposition 1.3.16. Let $\mathfrak{P}_Z = \mathfrak{P} \cap Z_{\mathfrak{P}}$ be the prime ideal of $Z_{\mathfrak{P}}$ below \mathfrak{P} .

Then we have:

- (1) \mathfrak{P}_Z is nonsplit in L , i.e., \mathfrak{P} is the only prime ideal of L above \mathfrak{P}_Z .
- (2) \mathfrak{P} over $Z_{\mathfrak{P}}$ has ramification index e and inertia degree f .
- (3) The ramification index and the inertia degree of \mathfrak{P}_Z over K both equal 1.

Proposition 1.3.17. Every $\sigma \in G_{\mathfrak{P}}$ induces an automorphism

$$\bar{\sigma} : \mathcal{O}/\mathfrak{P} \longrightarrow \mathcal{O}/\mathfrak{P}, \quad a \bmod \mathfrak{P} \mapsto \sigma a \bmod \mathfrak{P}$$

of the residue class field \mathcal{O}/\mathfrak{P} . Putting $\kappa(\mathfrak{P}) = \mathcal{O}/\mathfrak{P}$ and $\kappa(\mathfrak{p}) = \mathcal{O}/\mathfrak{p}$,

$$G_{\mathfrak{P}} \longrightarrow \text{Gal}(\kappa(\mathfrak{P})/\kappa(\mathfrak{p})), \sigma \mapsto \bar{\sigma}$$

is surjective.

Definition 1.3.18. The kernel $I_{\mathfrak{P}} \subseteq G_{\mathfrak{P}}$ of the homomorphism,

$$G_{\mathfrak{P}} \longrightarrow \text{Gal}(\kappa(\mathfrak{P})/\kappa(\mathfrak{p}))$$

is called the inertia group of \mathfrak{P} over K . The fixed field

$$T_{\mathfrak{P}} = \{x \in L \mid \sigma x = x \quad \text{for all } \sigma \in I_{\mathfrak{P}}\}$$

is called the inertia field of \mathfrak{P} over K .

This inertia field $T_{\mathfrak{P}}$ appears in the tower of fields

$$K \subseteq Z_{\mathfrak{P}} \subseteq T_{\mathfrak{P}} \subseteq L$$

and we have the exact sequence

$$1 \longrightarrow I_{\mathfrak{P}} \longrightarrow G_{\mathfrak{P}} \longrightarrow \text{Gal}(\kappa(\mathfrak{P})/\kappa(\mathfrak{p})) \longrightarrow 1$$

Proposition 1.3.19. One has

(1) $I_{\mathfrak{P}}$ is a normal subgroup of $G_{\mathfrak{P}}$ and

$$\text{Gal}(T_{\mathfrak{P}}/Z_{\mathfrak{P}}) \cong \text{Gal}(\kappa(\mathfrak{P})/\kappa(\mathfrak{p})), \quad \text{Gal}(L/T_{\mathfrak{P}}) = I_{\mathfrak{P}}$$

(2)

$$\#I_{\mathfrak{P}} = [L : T_{\mathfrak{P}}] = e, \quad (G_{\mathfrak{P}} : I_{\mathfrak{P}}) = [T_{\mathfrak{P}} : Z_{\mathfrak{P}}] = f$$

(3) The ramification index of \mathfrak{P} over \mathfrak{P}_T is e and the inertia degree is 1.

(4) The ramification index of \mathfrak{P}_T over \mathfrak{P}_Z is 1 and the inertia degree is f .

Proposition 1.3.20.

$$G_{\sigma\mathfrak{P}} = \sigma G_{\mathfrak{P}} \sigma^{-1}, I_{\sigma\mathfrak{P}} = \sigma I_{\mathfrak{P}} \sigma^{-1}, Z_{\sigma\mathfrak{P}} = \sigma(Z_{\mathfrak{P}}), T_{\sigma\mathfrak{P}} = \sigma(T_{\mathfrak{P}})$$

The following diagram demonstrates what we obtain

$$\begin{array}{ccccc}
 & L & & 1 & & \mathfrak{P} \\
 & \uparrow e & & \downarrow \text{index}=e & & \uparrow g_3=1, e_3=e, f_3=1 \\
 \text{Galois} & \swarrow & T_{\mathfrak{P}} & & I_{\mathfrak{P}} & & \mathfrak{P}_T \\
 & \uparrow f & & \downarrow \text{index}=f & & \uparrow g_2=1, e_2=1, f_2=f \\
 \text{Galois} & \swarrow & Z_{\mathfrak{P}} & & G_{\mathfrak{P}} & & \mathfrak{P}_Z \\
 & \uparrow g & & \downarrow \text{index}=g & & \uparrow e(\mathfrak{P}_Z/\mathfrak{p})=f(\mathfrak{P}_Z/\mathfrak{p})=1 \\
 & K & & \text{Gal}(L/K) & & \mathfrak{p}
 \end{array}$$

Definition 1.3.21 (Frobenius automorphism). If L/K is a Galois extension of algebraic number fields, and \mathfrak{P} a prime ideal which is unramified over K , then there is only one automorphism

$$\left(\frac{L/K}{\mathfrak{P}} \right) \in \text{Gal}(L/K)$$

such that

$$\left(\frac{L/K}{\mathfrak{P}} \right) a \equiv a^q \pmod{\mathfrak{P}} \quad \text{for all } a \in \mathcal{O}_{\mathcal{L}}$$

where $q = |\kappa(\mathfrak{p})|$. It is called the Frobenius automorphism. The decomposition group $G_{\mathfrak{P}}$ is cyclic and $\varphi_{\mathfrak{P}}$ is a generator of $G_{\mathfrak{P}}$.

If L/K is abelian, usually we denote Frobenius automorphism by $\left(\frac{L/K}{\mathfrak{p}} \right)$ since it is independent of the choice of prime ideal over \mathfrak{p} .

Proposition 1.3.22. L/K is a Galois extension of algebraic number fields, and \mathfrak{P} a prime ideal which is unramified over K . Let $\left(\frac{L/K}{\mathfrak{P}}\right)$ be the Frobenius automorphism.

(1) The order of $\left(\frac{L/K}{\mathfrak{P}}\right)$ is f .

(2)

$$\left(\frac{L/K}{\sigma(\mathfrak{P})}\right) = \sigma \left(\frac{L/K}{\mathfrak{P}}\right) \sigma^{-1}$$

(3) If E is an intermediate field and E/K is a Galois extension. then

$$\left(\frac{L/K}{\mathfrak{P}}\right)\Big|_E = \left(\frac{E/K}{\mathfrak{P}_E}\right)$$

Theorem 1.3.23. Assume $E_1/K, E_2/K$ are Galois extension, $L = E_1E_2$, then L/K is also Galois extension.

(1) \mathfrak{p} unramified in L if and only if unramified in E_1 and E_2 .

(2) \mathfrak{p} totally split in L if and only if totally split in E_1 and E_2 .

Proof: (1): Let \mathfrak{P} be a prime ideal over \mathfrak{p} and $\mathfrak{P}_1 = \mathfrak{P} \cap E_1, \mathfrak{P}_2 = \mathfrak{P} \cap E_2$. Notice that a prime ideal is unramified if and only if its inertia group is trivial, then it suffices to show the inertia group $I_{\mathfrak{P}}$ is trivial. Notice that the embedding

$$\varphi : \text{Gal}(L/K) \rightarrow \text{Gal}(E_1/K) \times \text{Gal}(E_2/K), \sigma \mapsto (\sigma|_{E_1}, \sigma|_{E_2})$$

preserves inertia group and decomposition group.

(2): Since \mathfrak{p} is totally split over E_1 and E_2 , it is unramified over E_1 and E_2 , hence unramified over L . Consider the Frobenius automorphism $\frac{L/K}{\mathfrak{P}}$, under the embedding φ and by Proposition 1.3.22,

$$\mathfrak{P} \text{ totally split} \iff \left(\frac{L/K}{\mathfrak{P}}\right) = \text{id} \iff \left(\frac{E_1/K}{\mathfrak{P}_1}\right) = \text{id}, \left(\frac{E_2/K}{\mathfrak{P}_2}\right) = \text{id}$$

Corollary 1.3.24. If L/K is abelian, $Z_{\mathfrak{P}}$ is the maximal intermediate field such that \mathfrak{p} is totally split and $T_{\mathfrak{P}}$ is the maximal intermediate field such that \mathfrak{p} is unramified.

Example 1.3.25. The Lucas sequence

$$a_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}$$

, where α, β are roots of polynomial $X^2 - X - \frac{q-1}{4}$ with q a prime number congruent to 1(mod 4), we have

$$a_p \equiv \left(\frac{p}{q}\right) \pmod{p}$$

For prime number $p \neq 2, q$

Proof: Consider the Frobenius automorphism $\left(\frac{\mathbb{Q}(\sqrt{q})/\mathbb{Q}}{p}\right)$, on the one hand, $a_p \equiv 1 \pmod{p}$ iff $\left(\frac{\mathbb{Q}(\sqrt{q})/\mathbb{Q}}{p}\right)$ is trivial. On the other hand, $\left(\frac{\mathbb{Q}(\sqrt{q})/\mathbb{Q}}{p}\right)$ is trivial iff $f = 1$ i.e. p is totally split over $\mathbb{Q}(\sqrt{q})$.

Proposition 1.3.26. Let n be a prime power ℓ^ν and put $\lambda = 1 - \zeta$. Then the principal ideal (λ) in the ring \mathcal{O} of integers of $\mathbb{Q}(\zeta)$ is a prime ideal of inertia degree, and we have

$$\ell\mathcal{O} = (\lambda)^d, \quad \text{where } d = \varphi(\ell^\nu) = [\mathbb{Q}(\zeta) : \mathbb{Q}]$$

Furthermore, the basis $1, \zeta, \dots, \zeta^{d-1}$ of $\mathbb{Q}(\zeta)/\mathbb{Q}$ has the discriminant

$$d(1, \zeta, \dots, \zeta^{d-1}) = \pm \ell^s, \quad s = \ell^{\nu-1}(\nu\ell - \nu - 1)$$

Proposition 1.3.27. A \mathbb{Z} -basis of ring of integers of $\mathbb{Q}(\zeta_n)$ is given by $1, \zeta, \dots, \zeta^{d-1}$, with $d = \varphi(n)$, in other words,

$$\mathcal{O} = \mathbb{Z} + \mathbb{Z}\zeta + \dots + \mathbb{Z}\zeta^{d-1} = \mathbb{Z}[\zeta]$$

Proposition 1.3.28. Let $n = \prod_p p^{\nu_p}$ be the prime factorization of n and, for every prime number p , let f_p be the smallest positive integer such that

$$p^{f_p} \equiv 1 \pmod{m}, \quad \text{where } m = n/p^{\nu_p}$$

Then one has in $\mathbb{Q}(\zeta)$ the factorization

$$p = (\mathfrak{p}_1 \cdots \mathfrak{p}_r)^{\varphi(p^{\nu_p})}$$

where $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ are distinct prime ideals, all of degree f_p and $r = \frac{\varphi(m)}{f_p}$.

Proof: Consider the Frobenius Automorphic of p over $\mathbb{Q}(\zeta_m)$, f_p is the root of the Frobenius Automorphic hence equals to the order of p in $(\mathbb{Z}/m\mathbb{Z})^\times$. By Proposition 1.3.26, we have $e = \varphi(p^{\nu_p}), f = f_p, g = \frac{\varphi(m)}{f_p}$.

Moreover, $\mathbb{Q}(\zeta_m)$ is the inertia field of the cyclotomic extension.

In the following content we assume L/K is a finite extension of number fields or a finite extension of \mathbb{Q}_p and $\mathcal{O}_L, \mathcal{O}_K$ be their ring of integers respectively.

Definition 1.3.29. Assume \mathfrak{A} is a fractional ideal of L . Define

$$*\mathfrak{A} = \{x \in L : \text{Tr}_{L/K}(x\mathfrak{A}) \subseteq \mathcal{O}_K\}$$

Since \mathfrak{A} is fractional ideal, $*\mathfrak{A} \neq 0$. If $\alpha_1, \dots, \alpha_n \in \mathcal{O}_L$ is a basis of L/K and $d = \det(\text{Tr}(\alpha_i \alpha_j))$ its discriminant, by Proposition 1.3.2, there's $0 \neq a \in \mathcal{O}_K \cap \mathfrak{A}$. We have $ad*\mathfrak{A} \subseteq \mathcal{O}_L$. Indeed, if $x = x_1\alpha_1 + \dots + x_n\alpha_n \in *\mathfrak{A}$, with $x_i \in K$, then the ax_i satisfy the system of linear equations $\sum_{i=1}^n ax_i \text{Tr}(\alpha_i \alpha_j) = \text{Tr}(xa\alpha_j) \in \mathcal{O}_K$. This implies $dx_i a \in \mathcal{O}_K$ and thus $dax \in \mathcal{O}_L$. Hence $*\mathfrak{A}$ is also a fractional ideal.

Definition 1.3.30. The fractional ideal

$$\mathfrak{C}_{\mathcal{O}_L|\mathcal{O}_K} = *\mathcal{O}_L = \{x \in L : \text{Tr}(x\mathcal{O}_L) \subseteq \mathcal{O}_K\}$$

is called Dedekind's complementary module, or the inverse different. Its inverse,

$$\mathfrak{D}_{\mathcal{O}_L|\mathcal{O}_K} = \mathfrak{C}_{\mathcal{O}_L|\mathcal{O}_K}^{-1}$$

is called the different of $\mathcal{O}_L|\mathcal{O}_K$, an integral ideal of \mathcal{O}_L . We also denote it by $\mathfrak{D}_{L|K}$.

Definition 1.3.31 (different of the element). $f(X) \in \mathcal{O}_K[X]$ be the minimal polynomial of α . We define the different of the element α by

$$\delta_{L|K}(\alpha) = \begin{cases} f'(\alpha) & \text{if } L = K(\alpha) \\ 0 & \text{if } L \neq K(\alpha) \end{cases}$$

Lemma 1.3.32. $f(X) = a_0 + a_1X + \dots + a_nX^n \in F[X]$ with $a_n \neq 0$, F algebraically closed, and $\alpha_1, \dots, \alpha_n$ be roots of $f(X)$. Suppose $\alpha_1, \dots, \alpha_n$ are distinct, then

$$\sum_{i=1}^n \frac{f(X)}{X - \alpha_i} \frac{\alpha_i^r}{f'(\alpha_i)} = X^r, \quad 0 \leq r \leq n-1$$

Proposition 1.3.33. If $\mathcal{O}_L = \mathcal{O}_K[\alpha]$, the different is the principal ideal

$$\mathfrak{D}_{L|K} = (\delta_{L|K}(\alpha))$$

Proof: Let $f(X) = a_0 + a_1X + \dots + a_nX^n, a_n = 1, \in \mathcal{O}_K[X]$ be the minimal polynomial of α and

$$\frac{f(X)}{X - \alpha} = b_0 + b_1X + \dots + b_{n-1}X^{n-1}$$

By above Lemma,

$$\text{Tr} \left[\frac{f(X)}{X - \alpha} \frac{\alpha^r}{f'(\alpha)} \right] = X^r$$

Considering now the coefficient of each of the powers of X , we obtain

$$\text{Tr} \left(\alpha^i \frac{b_j}{f'(\alpha)} \right) = \delta_{ij}, \quad 0 \leq i, j \leq n-1$$

Since $\mathcal{O}_L = \mathcal{O}_K + \dots + \mathcal{O}_K\alpha^{n-1}$, $b_j/f'(\alpha) \in *\mathcal{O}_L, j = 0, \dots, n-1$ form a basis of L/K and

$$\mathfrak{C}_{\mathcal{O}_L|\mathcal{O}_K} = f'(\alpha)^{-1} (\mathcal{O}_K b_0 + \dots + \mathcal{O}_K b_{n-1}) = f'(\alpha)^{-1} \mathcal{O}_L$$

Theorem 1.3.34. A prime ideal \mathfrak{P} of L is ramified over K if and only if $\mathfrak{P} \mid \mathfrak{D}_{L|K}$. Let \mathfrak{P}^s be the maximal power of \mathfrak{P} dividing $\mathfrak{D}_{L|K}$, and let e be the ramification index of \mathfrak{P} over K . Then one has

$$\begin{aligned} s &= e - 1, & \mathfrak{P} \text{ is tamely ramified,} \\ e \leq s \leq e - 1 + v_{\mathfrak{P}}(e), & \mathfrak{P} \text{ is widely ramified} \end{aligned}$$

Proposition 1.3.35. If K is an algebraic number field, $\mathfrak{D}_{K/\mathbb{Q}}$ be its different. Then

$$|d_K| = \mathfrak{N}(\mathfrak{D}_{K/\mathbb{Q}})$$

Proposition 1.3.36. K is an algebraic number field, if $\mathfrak{D}_{K|\mathbb{Q}} = P_1^{e_1} \dots P_s^{e_s}$. We have

$$\mathfrak{D}_{K_{P_i}|\mathbb{Q}_{P_i}} = \mathfrak{p}_i^{e_i}$$

where \mathfrak{p}_i be the unique maximal ideal in the ring of integers of K_{P_i} .

1.4 Adeles and Ideles

Definition 1.4.1. Let K be a number field. Let K_{ν} be the completion of K at the ν th place of K . The restricted direct product of K_{ν} , under addition, with respect to \mathfrak{o}_{ν} , is called the adele group of K , and is denoted \mathbb{A}_K . We set $J_{\infty} = \{\nu : \nu \text{ an infinite place of } K\}$. Note that K_{ν} is an LCHA and \mathfrak{o}_K is a compact-open subgroup of K_{ν} for all finite places ν of K . Every element of K is divisible by finitely many prime ideals, and hence the embedding of K into K_{ν} for all ν lies in \mathfrak{o}_{ν} for all but finitely many places. Therefore, K embeds diagonally into \mathbb{A}_K :

$$\begin{aligned} K &\rightarrow \mathbb{A}_K \\ x &\mapsto (x, x, x, \dots) \end{aligned}$$

The idele group, denoted \mathbb{I}_K , is the restricted direct product of K_{ν}^* , as a multiplicative group, with respect to $\mathfrak{o}_{\nu}^{\times}$, an open compact subgroup of K_{ν}^* . Since every element of K^* is locally an integer, and hence a unit for all but finitely many places, K^* diagonally embeds into \mathbb{I}_K :

$$\begin{aligned} K^* &\rightarrow \mathbb{I}_K \\ x &\mapsto (x, x, x, \dots) \end{aligned}$$

Proposition 1.4.2. K is a number field, \mathbb{A}_K be the adele group of K and \mathbb{I}_K be the idele group of K .

- (1) \mathbb{A}_K is a commutative ring with identity and $\mathbb{A}_K^{\times} = \mathbb{I}_K$.
- (2) Restricted direct product topology on \mathbb{I}_K is stronger than subspace topology from \mathbb{A}_K on \mathbb{I}_K

(3) \mathbb{I}_K is a topological isomorphism onto its image in \mathbb{A}_K^2 under the map

$$\begin{aligned}\phi : \mathbb{I}_K &\longrightarrow \mathbb{A}_K^2 \\ x &\mapsto \left(x, \frac{1}{x}\right)\end{aligned}$$

(4) Define the subgroup \mathbb{A}_∞ of \mathbb{A}_K to be

$$\mathbb{A}_\infty := \{x = (x_\nu) \in \mathbb{A}_K : x_\nu \in \mathfrak{o}_\nu \text{ for all } \nu \notin J_\infty\}$$

We have

$$\mathbb{A}_K = K + \mathbb{A}_\infty \quad \text{and} \quad K \cap \mathbb{A}_\infty = \mathcal{O}_K$$

(5) K is discrete subgroup of Adele group and \mathbb{A}_K/K is compact.

Proof: (2): Take $K = \mathbb{Q}$ as an example,

$$U = \mathbb{R}^\times \times \prod_{p \neq \infty} \mathbb{Z}_p^\times$$

is open in restricted direct product topology but not open in subspace topology.

(3): Notice that ϕ is continous since

$$K_\nu^* \rightarrow K_\nu^* \times K_\nu^*, x \mapsto \left(x, \frac{1}{x}\right)$$

is continous for all ν . Conversely, to show the inverse map

$$\begin{aligned}\varphi : \phi(\mathbb{I}_K) &\longrightarrow \mathbb{I}_K \\ \left(x, \frac{1}{x}\right) &\mapsto x\end{aligned}$$

is continous, it suffices to check that for

$$U = \prod_{\nu \in S} N_\nu^* \times \prod_{\nu \in S^c} \mathfrak{o}_\nu^*$$

where S is finite set of places containing the infinite places and N_ν^* are open subsets of K_ν^* , we have

$$\varphi^{-1}(U) = \left(\prod_{\nu \in S} N_\nu^* \times \prod_{\nu \in S^c} \mathfrak{o}_\nu \times \prod_{\nu \in T} (N_\nu^*)^{-1} \times \prod_{\nu \in T^c} \mathfrak{o}_\nu\right) \cap \phi(\mathbb{I}_K).$$

(4): Take $x = (x_\nu) \in \mathbb{A}_K$, there's $0 \neq m \in \mathbb{Z}$ such that $mx_\nu \in \mathfrak{o}_\nu$ for all finite place ν . Assume

$$S = \{\nu \text{ finite} : |m|_\nu \neq 1 \text{ or } x_\nu \notin \mathfrak{o}_\nu\}.$$

By Chinese Remainder Theorem, there's $y \in \mathcal{O}_K$ such that $|y_\nu - mx_\nu| \leq \varepsilon$ for all $\nu \in S$ (ε sufficiently small). Then $x_\nu - y/m \in \mathfrak{o}_\nu$.

Proposition 1.4.3. K is a discrete subgroup of \mathbb{A}_K (hence closed by Proposition 2.1.13) and \mathbb{A}_K/K is compact.

Proof: Consider

$$C_1 = \{x = (x_\nu) \in \mathbb{A}_K : |x_\nu|_\nu < 1/([K : \mathbb{Q}]!) \text{ for infinite place and } |x_\nu| \leq 1 \text{ for finite place}\}$$

and

$$C_2 = \{x = (x_\nu) \in \mathbb{A}_K : |x_\nu| \leq M \text{ for infinite place and } |x_\nu| \leq 1 \text{ for finite place}\}$$

for M sufficiently large. By definition of restricted direct topology, C_1 is an open subset. If $k_1, k_2 \in K$ and $k_1 + c = k_2$ for some $c \in C_1$, notice that $k_2 - k_1 = c \in K \cap C \subset \mathcal{O}_K$, we have

$$\prod_{\sigma} (x - \sigma(c)) = p_c(x)^d, d = [K : \mathbb{Q}(c)].$$

where $p_c(x)$ is the minimal polynomial of c . Hence $\prod_{\sigma} (x - \sigma(c)) \in \mathbb{Z}[x]$. Therefore, $x^n = \prod_{\sigma} (x - \sigma(c))$, which implies $c = 0$. Hence, K is a discrete subgroup of Adele. On the other hand, by Proposition 2.1.43, C_2 is compact for arbitrary $M > 0$. Since \mathcal{O}_K is a complete lattice in $K_{\mathbb{R}}$ and $\mathbb{A}_K = K + \mathbb{A}_{\infty}$, we have $\mathbb{A}_K = K + C_2$. Hence, \mathbb{A}_K/K is compact.

Proposition 1.4.4. K^* is a discrete subgroup of \mathbb{I}_K (hence closed by Proposition 2.1.13) and \mathbb{I}_K/K^* is a LCHG but not compact. We call \mathbb{I}_K/K^* idele class group and denoted by C_K .

Definition 1.4.5. Let F be a local field of characteristic zero. We define the normalized absolute value on F as follows:

- (1) If $F = \mathbb{R}$, then let $|\cdot|_F$ be the standard absolute value.
- (2) If $F = \mathbb{C}$, then let $|\cdot|_F$ be the square of the standard absolute value.
- (3) If F is non-Archimedean, then let $|\cdot|_F$ be such that $|\pi_F|_F = \frac{1}{q}$, where π_F is the uniformizing parameter of F , and q is the order of the residue field $\mathfrak{o}_F/\pi_F\mathfrak{o}_F$.

Definition 1.4.6. Now we will fix a Haar measure for each completion of K .

- (1) If $F = \mathbb{R}$, then let dx be the standard Lebesgue measure.
- (2) If $F = \mathbb{C}$, then let dx be twice the standard Lebesgue measure.
- (3) If F is non-Archimedean, then let dx be such that $\text{Vol}(\mathfrak{o}_F, dx) = N(\mathfrak{D}_F)^{-1/2}$, where \mathfrak{D}_F denotes the different of F , which is an integral ideal of \mathfrak{o}_F .

Remark 1.4.7. By Theorem 1.3.34, for all the completion K_ν , there are only finite many finite places such that $\text{Vol}(\mathfrak{o}_F, dx) \neq 1$.

Theorem 1.4.8. Let $|\cdot|_F$ be the normalized absolute value of F . If μ is a Haar measure on F , then

$$\frac{\mu(y \cdot M)}{\mu(M)} = |y|_F$$

for any $y \in F^\times$ and for any measurable set M with $0 < \mu(M) < \infty$.

Proof: The cases when $F = \mathbb{R}$ and \mathbb{C} are trivial. Now we show the case when F is a p-adic field. Notice that

$$\mu(\pi_F^s \mathfrak{o}_F) = \sum_{a \in \pi_F^s \mathfrak{o}_F / \pi_F^{s+1} \mathfrak{o}_F} \mu(a + \pi_F^s \mathfrak{o}_F) = |\pi_F|_F^{-1} \mu(\pi_F^{s+1} \mathfrak{o}_F)$$

for all $s \in \mathbb{Z}$.

Definition 1.4.9. Define

$$|\cdot|_{\mathbb{I}_K} : \mathbb{I}_K \rightarrow \mathbb{R}_{>0}, (x_\nu) \mapsto \prod_{\nu} |x_\nu|_{\nu}$$

to be the absolute value on \mathbb{I}_K . By Proposition 2.1.50, $|\cdot|_{\mathbb{I}_K}$ is continuous and surjective. Hence, \mathbb{I}_K/K^* cannot be compact.

Theorem 1.4.10 (Artin's product formula). For all $x \in K^*$, $|x|_{\mathbb{I}_K} = 1$ and $|\cdot|_{\mathbb{I}_K}$ is surjective.

Proof: By Theorem 2.2.41, we have

$$\begin{aligned} |x|_{\mathbb{I}_K} &= |N_{K/\mathbb{Q}}(x)| \prod_p \prod_{\nu|p} |x_\nu|_{\nu} \\ &= |N_{K/\mathbb{Q}}(x)| \prod_p \prod_{i=1}^r |N_{\mathbb{Q}_p(\alpha_i)/\mathbb{Q}_p}(\sigma_i(x))|_p \\ &= |N_{K/\mathbb{Q}}(x)| \prod_p |N_{K/\mathbb{Q}}(x)|_p \\ &= 1 \end{aligned}$$

Definition 1.4.11. Define $\text{Ker } |\cdot|_{\mathbb{I}_K} = \mathbb{I}_K^1$ and we call it ideles of norm one.

Proposition 1.4.12. For every $\alpha = (\alpha_\nu) \in \mathbb{I}_K$, let $|\alpha|_{\mathbb{I}_K} = \prod_{\nu} |\alpha_\nu|_{\nu}$. If μ is a Haar measure on \mathbb{A}_K , then

$$\frac{\mu(\alpha \cdot M)}{\mu(M)} = |\alpha|_{\mathbb{I}_K}$$

for any $\alpha \in \mathbb{I}_K$ and for any measurable set M with $0 < \mu(M) < \infty$.

Proof: By Proposition 2.1.50.

Proposition 1.4.13. LCHA $C_K^1 = \mathbb{I}_K^1/K^*$ is compact.

Definition 1.4.14. For $\xi = (\xi_v) \in \mathbf{A}_K^\times = \mathbb{I}_K$, define the closed subset

$$X_\xi = \{(x_v) \in \mathbf{A}_K \mid \|x_v\|_v \leq \|\xi_v\|_v\} \subseteq \mathbf{A}_K$$

There exists $C = C_K > 0$ such that if $|\xi|_{\mathbb{I}_K} > C$ then $X_\xi \cap K$ contains a nonzero element.

Proof: Let μ be the unique Haar measure on \mathbf{A}_K that is adapted to counting measure on the discrete subgroup K and the volume-1 measure on the compact quotient \mathbf{A}_K/K . Let $Z \subseteq \mathbf{A}_K$ denote the compact set of adeles $z = (z_v)$ such that $|z_v|_v \leq 1$ for non-archimedean v , $|z_v|_v \leq |1/2|_v$ for $v \mid \infty$, so if $z, z' \in Z$ then $\|z_v - z'_v\|_v \leq 1$ for all v . Since Z is compact and contains an open neighborhood around the origin, $\mu(Z)$ is finite and positive.

Take $C = 1/\mu(Z)$, if $|\xi| > C$, we have $\mu(\xi Z) > 1$. We claim that this forces the existence of a pair of distinct elements in ξZ with the same image in \mathbf{A}_K/K , which is to say that the projection map $\pi : \xi Z \rightarrow \mathbf{A}_K/K$ has some fiber with size at least 2. Indeed, if χ on \mathbf{A}_K is the characteristic function of the subset ξZ , then by Theorem 2.1.38 (we need to find $f_n \in C_c(\mathbb{A}_K)$, $n = 1, \dots$ such that $f_n \rightarrow \chi$ pointwise and $f_n \leq f_{n+1}$ for all $n \geq 1$)

$$\mu(\xi Z) = \int_{\mathbf{A}_K} \chi d\mu = \int_{\mathbf{A}_K/K} \left(\sum_{c \in K} \chi(c + x) \right) \bar{\mu} = \int_{\mathbf{A}_K/K} \# \pi^{-1}(x + K) \bar{\mu}$$

with $\bar{\mu}$ the volume-1 Haar measure on \mathbf{A}_K/K , and so if all fibers of π have size at most 1 then we get $\mu(\xi Z) \leq \int_{\mathbf{A}_K/K} d\bar{\mu} = 1$, contradicting that $\mu(\xi Z) > 1$.

We conclude that there exists $x, x' \in \xi Z$ such that $x - x' = a \in K^\times$. Thus, if we write $x = \xi z$ and $x' = \xi z'$ with $z, z' \in Z$ then

$$|a|_v = \|\xi_v(z_v - z'_v)\|_v \leq |\xi|_v$$

for all places v . Hence, $a \in X_\xi \cap K^\times$.

Theorem 1.4.15 (strong approximation). Let $M_K = S \sqcup T \sqcup \{w\}$ be a partition of the places of K with S finite (contains infinite place). Given any $a_v \in K$ and $\epsilon_v \in \mathbb{R}_{>0}$ with $v \in S$, there exists an $x \in K$ for which

$$\begin{aligned} \|x - a_v\|_v &\leq \epsilon_v \text{ for all } v \in S \\ \|x\|_v &\leq 1 \text{ for all } v \in T \end{aligned}$$

(note that there is no constraint on $\|x\|_w$).

Proof: Consider C_2 a compact subset of \mathbb{A}_K . For any nonzero $u \in K \subseteq \mathbb{A}_K$ we also have $\mathbb{A}_K = K + uC_2$. Now choose $z \in \mathbb{A}_K$ such that

$$0 < \|z\|_v \leq \epsilon_v/M \text{ for } v \in S, \quad 0 < \|z\|_v \leq 1 \text{ for } v \in T, \quad \|z\|_w > C_K \prod_{v \neq w} \|z\|_v^{-1}$$

We have $\|z\| > B$, so there is a nonzero $u \in K \subseteq \mathbb{A}_K$ with $\|u\|_v \leq \|z\|_v$ for all $v \in M_K$.

Now let $a = (a_v) \in \mathbb{A}_K$ be the adele with a_v given by the hypothesis of the theorem for $v \in S$ and $a_v = 0$ for $v \notin S$. We have $\mathbb{A}_K = K + uW$, so $a = x + y$ for some $x \in K$ and $y \in uW$. Therefore

$$\|x - a_v\|_v = \|y\|_v \leq \|u\|_v \leq \|z\|_v \leq \begin{cases} \epsilon_v & \text{for } v \in S \\ 1 & \text{for } v \in T \end{cases}$$

as desired.

Definition 1.4.16. Let K be a global field. Let ν be a place of K and K_ν be the completion of K with respect to ν . Define

$$S(\mathbb{A}_K) = \otimes'_\nu S(K_\nu) = \{f = \otimes f_\nu : f_\nu \in S(K_\nu) \forall \nu \text{ and } f_\nu = \mathbf{1}_{\mathfrak{o}_\nu} \text{ for almost all } \nu\}$$

where $\mathbf{1}_{\mathfrak{o}_\nu}$ is a characteristic function of \mathfrak{o}_ν . A function $f \in S(\mathbb{A}_K)$ is called an adelic Schwartz-Bruhat function.

Proposition 1.4.17. For each place ν of K , let ψ_ν be the standard unitary character on K_ν . Then the restriction of ψ_ν to \mathfrak{o}_ν is trivial for almost all ν . Hence,

$$\psi_K \left(\prod_\nu x_\nu \right) = \prod_\nu \psi_\nu(x_\nu) \text{ for } x = (x_\nu) \in \mathbb{A}_K$$

is a well-defined non-trivial character on \mathbb{A}_K . And ψ_K is trivial on K .

Proof:

$$\psi_K(\alpha) = \prod_p \prod_{\nu|p} \psi_p(\text{tr}_{K_\nu/\mathbb{Q}_p}(\alpha)) = \prod_p \psi_p \left(\sum_{\nu|p} \text{tr}_{K_\nu/\mathbb{Q}_p}(\alpha) \right) = \prod_p \psi_p(\text{tr}_{K/\mathbb{Q}}(\alpha)) = 1$$

Proposition 1.4.18. Let K be a number field with the standard character ψ_K , as defined above. Then the following assertions hold:

- (1) The map $\alpha_{\psi_K} : \mathbb{A}_K \rightarrow \widehat{\mathbb{A}_K}$, defined by $y \mapsto \psi_{K,y}$, where $\psi_{K,y}(x) = \psi_K(xy)$, is an isomorphism(as topological groups).
- (2) The map $\beta_{\psi_K} : K \rightarrow \widehat{\mathbb{A}_K/K}$, defined by $x \mapsto \psi_{K,x}$, where x is identified with its embedding in \mathbb{A}_K , is an isomorphism(as topological groups).

Proof: (1): Since the different of K_ν is trivial for all but finite many ν .

(2): We still denote the image of K under the self-dual map defined in (1) by K . Hence $\mathbb{A}_K/K \cong \widehat{\mathbb{A}_K}/K$. Notice that K^\perp is a closed subgroup of $\widehat{\mathbb{A}_K}$, we have K^\perp/K is a closed(hence compact) subgroup of $\widehat{\mathbb{A}_K}/K$. On the other hand, $K^\perp \cong \widehat{\mathbb{A}_K/K}$, hence K^\perp is discrete. For all $x \in K^\perp$, there's U open in $\widehat{\mathbb{A}_K}$ such that $U \cap K^\perp = x$, hence

$$x + K = K^\perp \cap \bigcup_{y \in K} y + U$$

Therefore, K^\perp/K is discrete. Notice that $\alpha(\psi K) = (y \mapsto \psi(\alpha y))K$ is a well-defined K -vector space structure on K^\perp/K . Hence $K^\perp = K$.

Proposition 1.4.19. The mapping $f \mapsto \hat{f}$ defines an automorphism of $S(\mathbb{A}_K)$ that, moreover, extends to an isometry of $L^2(\mathbb{A}_K)$.

Theorem 1.4.20 (Poisson summation formula for \mathbb{A}_K). If $f \in S(\mathbb{A}_K)$, then

$$\sum_{\kappa \in K} f(\kappa) = \sum_{\kappa \in K} \hat{f}(\kappa).$$

Proof: Fix a self-dual Haar measure on \mathbb{A}_K and a suitable measure on \mathbb{A}_K/K such that Theorem 2.1.38 holds. (Haar measure on K is counting measure). Then, we define

$$F : \mathbb{A}_K/K \rightarrow \mathbb{C}, x + K \mapsto \int_K f(x + y) dy$$

Hence,

$$\hat{F}(z) = \int_{\mathbb{A}_K/K} \int_K f(x + y) \psi_{K,z}(x) dy dx = \int_{\mathbb{A}_K} f(x) \psi_{K,z}(x) dx = \hat{f}(z), \forall z \in K$$

Then by Fourier Inversion Formula, we have

$$CF(-x) = \hat{F}(x) = \int_K \hat{f}(t) \psi_{K,x}(t) dt, x \in \mathbb{A}_K/K$$

for some $C > 0$. Take $x = 0$, we have

$$C \sum_{\kappa \in K} f(\kappa) = \sum_{\kappa \in K} \hat{f}(\kappa).$$

Replace f by \hat{f} , we have

$$C \sum_{\kappa \in K} \hat{f}(\kappa) = \sum_{\kappa \in K} \hat{\hat{f}}(\kappa) = \sum_{\kappa \in K} f(\kappa)$$

Then $C = 1$.

Corollary 1.4.21. Above content shows that there's unique measure on \mathbb{A}_K/K such that Fourier Inversion Theorem (with respect to counting measure on K) and Theorem 2.1.38 hold simultaneously. Moreover, under this measure, the volume of the entire group \mathbb{A}_K/K is 1.

Proof: Let D_∞ be a fundamental domain for $K_\mathbb{R}/\mathcal{O}_K$, and let $D = D_\infty \times \prod_{v \text{ finite}} \mathcal{O}_v$. Then

$$\begin{aligned} \text{Vol}(D) &= \text{Vol}(D_\infty) \prod_{v \text{ finite}} \text{Vol}(\mathcal{O}_v) \\ &= (d_K)^{1/2} \prod_{v \text{ finite}} \left(N(\mathfrak{D}_{K_{P_i}|\mathbb{Q}_{p_i}}) \right)^{-1/2} = 1 \end{aligned}$$

Notice that

$$\text{Vol}(D) = \int_{\mathbb{A}_K} \chi_D = \int_{\mathbb{A}_K/K} \int_K \chi_D = \text{Vol}(\mathbb{A}_K/K)$$

Corollary 1.4.22 (Poisson summation formula, another form). Let $x \in \mathbb{I}_K$. Let $f \in S(\mathbb{A}_K)$. Then

$$\sum_{\gamma \in K} f(\gamma x) = \frac{1}{|x|_{\mathbb{I}_K}} \sum_{\gamma \in K} \hat{f}(\gamma x^{-1})$$

Proposition 1.4.23. Every idele-class character χ has the factorization $\chi = \chi_0 |\cdot|^s$ where χ_0 is a unitary character. Moreover, real part of s and the value of χ_0 on norm-one idèle are uniquely determined by χ .

Definition 1.4.24. An idele-class character, χ , is called unramified if $\chi|_{\mathbb{I}_1} = 1$. We say that two idele-class characters are equivalent if their quotient is unramified. Each equivalence class is of the form

$$\{\chi_0 |\cdot|^s : s \in \mathbb{C}\}$$

for some fixed unitary character χ_0 . Hence, if we fix a unitary character for each equivalence class, s is uniquely determined by χ .

Definition 1.4.25. An idèle-class character or Hecke character or Größencharakter is a continuous homomorphism $\chi : \mathbb{I}_K \rightarrow \mathbb{C}^\times$ such that $\chi|_{K^\times} = 1$.

Proposition 1.4.26. There's a one-to-one correspondence between primitive Dirichlet character and continuous homomorphism from $\hat{\mathbb{Z}}^\times$ to \mathbb{C}^\times .

Proof: Notice that if $N = p_1^{e_1} \dots p_s^{e_s}$,

$$(\mathbb{Z}/m\mathbb{Z})^\times \cong (\mathbb{Z}/p_1^{e_1}\mathbb{Z})^\times \times \dots (\mathbb{Z}/p_s^{e_s}\mathbb{Z})^\times$$

Since each \mathbb{Z}_p^\times is compact group, each quasi-character is induced by Dirichlet character (mod p^n) for sufficiently large n . Hence, by Lemma 2.1.45, Each quasi-character of $\hat{\mathbb{Z}}^\times$ is induced by a primitive Dirichlet character.

Theorem 1.4.27. For any Dirichlet character $\chi : \hat{\mathbb{Z}}^\times \rightarrow \mathbb{S}^1$, it induces an idèle-class character as follow: Consider the canonical isomorphism

$$\mathbb{I}_{\mathbb{Q}} \cong \mathbb{Q}^* \times \mathbb{R}_+^\times \times \hat{\mathbb{Z}}^\times.$$

This holds since for every idèle $(x_v)_v \in \mathbb{I}_{\mathbb{Q}}$, there's unique $q \in \mathbb{Q}^*$ such that $x_\infty/q \in \mathbb{R}_{>0}$ and $x_p/q \in \mathbb{Z}_p^\times$.

Moreover, all the finite order idèle-class character $\chi \in \text{Hom}_{\text{cont}}(\mathbb{I}_{\mathbb{Q}}/\mathbb{Q}^*, \mathbb{C}^*)$ are induced by Dirichlet Character.

Chapter 2

Local Theory

2.1 Topological Group

Definition 2.1.1. A topological group is a group G with a topology such that the maps $(g, h) \mapsto gh$ from $G \times G$ (with the product topology) to G and $g \mapsto g^{-1}$ from G to G are continuous.

Theorem 2.1.2 (topology defined by neighborhood basis). Let G be a topological group, and let \mathcal{N} be a neighbourhood base for the identity element e of G . Then

- (1) for all $N_1, N_2 \in \mathcal{N}$, there exists an $N' \in \mathcal{N}$ such that $e \in N' \subset N_1 \cap N_2$;
- (2) all $a \in N \in \mathcal{N}$, there exists an $N' \in \mathcal{N}$ such that $N'a \subset N$;
- (3) all $N \in \mathcal{N}$, there exists an $V \in \mathcal{N}$ such that $V^{-1}V \subset N$;
- (4) all $N \in \mathcal{N}$ and all $g \in G$, there exists an $N' \in \mathcal{N}$ such that $g^{-1}N'g \subset N$;

Conversely, if G is a group and \mathcal{N} is a nonempty set of subsets of G contain e satisfying (1), (2), (3), (4), then there is a (unique) topology on G such that G is a topological group and \mathcal{N} form a neighborhood base at e . Moreover, if subsets in \mathcal{N} are all subgroup of G , we only need (1) and (4)

Proposition 2.1.3. G is a topological group.

- (1) If H is a subgroup of G , so is \bar{H} .
- (2) Every open subgroup of G is also closed.
- (3) If K_1, K_2 are compact subsets of G , so is K_1K_2 .
- (4) Every subgroup of G , endowed with the subspace topology, is a topological group.
- (5) Let G_1 and G_2 be topological groups. The direct product $G_1 \times G_2$ endowed with the product topology and componentwise group operation is a topological group.

Proposition 2.1.4. G, H are topological groups. $\varphi : G \rightarrow H$ is a group homomorphism, then φ is continuous if and only if φ is continuous at identity.

Definition 2.1.5. Let f be a function on a group G . We define left and right translates of f by $L_h f(g) = f(h^{-1}g)$ and $R_h f(g) = f(gh)$, respectively. If f is a continuous function from G to \mathbb{R} or \mathbb{C} , then we say that f is left uniformly continuous if, for all $\epsilon > 0$, there exists a neighborhood V of the identity such that

$$\|L_h f - f\|_u < \epsilon \quad \forall h \in V$$

where $\|\cdot\|_u$ is the uniform, or supremum, norm. And right uniform continuity is defined similarly. Let $C_c(G)$ be the space of continuous functions on G with compact support.

Proposition 2.1.6. Let G be a topological group. Every function $f \in C_c(G)$ is both left and right uniformly continuous.

Proposition 2.1.7. Let G be a topological group. Then the following assertions are equivalent:

- (1) G is T_1 .
- (2) G is Hausdorff.
- (3) The identity e is closed in G .
- (4) Every point of G is closed in G .

Definition 2.1.8. X is a topological space, G is a topological group. If a topological group action is a group $G \times S \rightarrow S$ which is also continuous. If in addition the action is transitive, we call it transitive topological group action.

Example 2.1.9. G is a topological group and H be a subgroup of G . Give G/H , the set of left cosets, quotient topology. Then the group action $\rho : G \times G/H \rightarrow G/H : (g, aH) \mapsto gaH$ is a transitive topological group action.

Proof: If U open in G/H , let

$$W = \bigcup_{u \in U} u$$

and $\varphi : G \times G \rightarrow G$ be the multiplication and $\pi : G \times G \rightarrow G \times G/H$ be the product of identity and projection, we have $\rho^{-1}(U) = \pi(\varphi^{-1}(W))$.

Proposition 2.1.10. Let G be a topological group and let H be a subgroup of G . Then the following assertions hold:

- (1) The canonical projection $\rho : G \rightarrow G/H$ is an open map.
- (2) The quotient space G/H is T_1 if and only if H is closed.

- (3) The quotient space G/H is discrete if and only if H is open. Moreover, if G is compact, then H is open if and only if G/H is finite.
- (4) If H is normal in G , then G/H is a topological group with respect to coset multiplication and the quotient topology.

Proposition 2.1.11. Let G be a Hausdorff topological group. Then:

- (1) The product of a closed subset F and a compact subset K is closed.
- (2) If H is a compact subgroup of G , then $\rho : G \rightarrow G/H$ is a closed map.

Proposition 2.1.12. Let $\{G_i\}_i \in I$ be a set of LCHG (locally compact Hausdorff) such that G_i is compact for all but finitely many $i \in I$. Then

$$\prod_{i \in I} G_i$$

is a LCHG.

Proposition 2.1.13 (LCHG subgroup). Let G be a Hausdorff topological group. Then a subgroup H of G is a LCHG (in the subspace topology) if and only if H is closed. In particular, every discrete subgroup of G is closed.

Proposition 2.1.14 (LCHG quotient group). If G is LCHG and H is a closed subgroup, then G/H is a locally compact and Hausdorff space.

Theorem 2.1.15. Inverse limit exists in category of topological group.

Proof:

Example 2.1.16 (completion of \mathbb{Z}). Define

$$\widehat{\mathbb{Z}} = \varprojlim \mathbb{Z}/n\mathbb{Z}$$

Since $\widehat{\mathbb{Z}}$ is completion, by Chinese Remainder Theorem, and Tychonoff theorem

$$\widehat{\mathbb{Z}} \cong \prod_p \mathbb{Z}_p$$

Hence

$$\widehat{\mathbb{Z}}^\times = \varprojlim (\mathbb{Z}/n\mathbb{Z})^\times \cong \prod_p \mathbb{Z}_p^\times$$

Definition 2.1.17 (pro-finite group). A topological group is pro-finite if it is isomorphic to a inverse limit of finite discrete topological group.

Proposition 2.1.18. A pro-finite group is compact, Hausdorff and totally disconnected.

Proof: Let G be a pro-finite group and $G \cong \varprojlim G_i$, since G_i is compact for each $i \in I$, it suffice to show $\varprojlim G_i$ is closed in product of G_i and also totally disconnected (connected component is one-point set).

Given $(g_i)_{i \in I} \notin \varprojlim G_i$, then there will exist p_{ij} such that $p_{ij}(g_j) \neq g_i$. Define

$$U = \{g_i\} \times \{g_j\} \times \prod_{k \neq i, j} G_k$$

which is open in $\prod_i G_i$ since G_i 's are discrete. Then $(g_i) \in U$, but $U \cap \varprojlim G_i = \emptyset$, which means $\prod_i G_i - \varprojlim G_i$ is open.

Given any two elements $(g_i)_i$ and $(h_i)_i$ in $\prod_i G_i$ such that $(g_i)_i \neq (h_i)_i$, then there will exist some $j, g_j \neq h_j$. Define open subsets $U_j = \{g_j\} \times \prod_{i \neq j} G_i$ and $V_j = (G_j - \{g_j\}) \times \prod_{i \neq j} G_i$. Then $(g_i)_i \in U_j$ and $(h_i)_i \in V_j$ but $U_j \cap V_j = \emptyset$. Hence any subspace containing more than one element of X is not connected.

Definition 2.1.19 (compact-open topology). Let G be a locally compact Hausdorff abelian group(LCHA). We will write the group operation multiplicatively. Define \hat{G} (group of unitary characters) to be the set of all continuous homomorphisms of G into the circle group, $S^1 := \{z \in \mathbb{C} : |z| = 1\}$, of the complex numbers.

Sets of the form

$$W(K, V) = \{\chi \in \hat{G} : \chi(K) \subseteq V\}$$

where K is a compact subset of G and V is a neighborhood of the identity in S^1 satisfies the four conditions in Theorem 2.1.2. Hence, it induces a topological group structure of \hat{G} . We call it compact-open topology.

Proposition 2.1.20. G is discrete, then \hat{G} is compact.

Proof: G is compact, then by Yychonoff's Theorem, $(S^1)^G$ with product topology is compact. And its compact subspace \hat{G} with subspace topology is the same as \hat{G} itself with compact-open topology.

Proposition 2.1.21. G is comact, then \hat{G} is discrete.

Proposition 2.1.22. χ_n converges to χ in \hat{G} if and only if for each compact set K in G , $\chi_n|_K$ converges uniformly to $\chi|_K$. If G is compact, then the compact open topology coincides the topology of uniform convergence. If G is finite, then the compact-open topology coincides with the topology of pointwise convergence.

Proposition 2.1.23. G is a LCHA, then \hat{G} is also LCHA.

Proof: Consider universal covering map $\phi : \mathbb{R} \rightarrow S^1, x \mapsto e^{2\pi i x}$, define $N(\varepsilon) = \phi((-\frac{\varepsilon}{3}, \frac{\varepsilon}{3}))$.

Hausdorff: if $\chi_1 \neq \chi_2$, there's $g \in G$ such that $\chi_1(g) \neq \chi_2(g)$. Then there's $g \in K \subset U$, where K compact and U open, such that $|\chi_1 - \chi_2| \geq \varepsilon$ in U . Consider a sufficiently small ε_0 , we have $\chi_1 U(K, N(\varepsilon_0)) \cap \chi_2 U(K, N(\varepsilon_0)) = \emptyset$.

Locally compact: Show that for every compact neighborhood K of G ,

$$W(K, \overline{N(1/4)})$$

is a compact subset of \hat{G} .

Proposition 2.1.24. For a LCHA G , \hat{G} is also LCHA. The (G, \hat{G})

(1) $\hat{\mathbb{R}} \cong \mathbb{R}$ as topological group with isometric map

$$\xi \mapsto (x \mapsto e^{2\pi i x \xi})$$

(2) $\hat{S}^1 \cong \mathbb{Z}$ as topological group, with isometric map

$$n \mapsto (z \mapsto z^n)$$

(3) $\hat{\mathbb{Z}} \cong S^1$, with isometric map

$$\alpha \mapsto (n \mapsto \alpha^n)$$

(4) $\widehat{\mathbb{Z}/n\mathbb{Z}} \cong \mathbb{Z}/n\mathbb{Z}$, with isometric map

$$m \mapsto (k \mapsto e^{\frac{2\pi i k m}{n}})$$

Definition 2.1.25. A left Haar measure is a non-zero Radon measure on a LCHG such that it is left-invariant.

Proposition 2.1.26. Let G be a LCHG. Define

$$C_c^+(G) = \{f \in C_c(G) : f \geq 0 \text{ and } \|f\|_u > 0\}.$$

we have

- (1) A Radon measure μ on G is a left Haar measure iff the measure $\tilde{\mu}$ defined by $\tilde{\mu}(E) = \mu(E^{-1})$ is a right Haar measure.
- (2) A nonzero Radon measure μ on G is a left Haar measure iff $\int f d\mu = \int L_y f d\mu$ for all $f \in C_c^+$ and $y \in G$.
- (3) If μ is a left Haar measure on G , then $\mu(U) > 0$ for every nonempty open $U \subset G$, and $\int f d\mu > 0$ for all $f \in C_c^+$.
- (4) If μ is a left Haar measure on G , then $\mu(G) < \infty$ iff G is compact.

Proposition 2.1.27. Every LCHG group G possesses a left Haar measure and it is unique up to a constant.

Example 2.1.28 (Haar measure on \mathbb{T}^n). Define $\varphi : Q = [0, 1]^n \rightarrow \mathbb{T}^n : x \mapsto x + \mathbb{Z}^n$ a bijection map. and notice that $\mu : E \in B_{\mathbb{T}^n} \mapsto m(\varphi^{-1}(E))$ is a left invariant Radon measure.

And by Riesz Representation Theorem, we can show that the measure induced by the positive linear functional

$$f \in C_c(\mathbb{T}^n) \mapsto \int_Q f \circ \pi$$

is left invariant, hence also Haar measure on \mathbb{T}^n .

Theorem 2.1.29 (Pontrjagin Duality). G LCHA. Then the map $G \rightarrow \hat{\hat{G}} : g \mapsto (\chi \mapsto \chi(g))$ is an isomorphism between topological groups.

Definition 2.1.30 (Fourier Transform). Let $f \in L_1(G)$. Then we define $\hat{f} : \hat{G} \rightarrow \mathbb{C}$, the Fourier transform of f , to be

$$\hat{f}(\chi) = \int_G f(y)\chi(y)dy \text{ for } \chi \in \hat{G}$$

Moreover, The Fourier Transform of $f \in L^1(G)$ is a continuous function vanishes at infinity. ($\in C_0(G)$).

Theorem 2.1.31 (The Plancherel Theorem). The Fourier transform on $L^1(G) \cap L^2(G)$ extends uniquely to a unitary map (in the category of Hilbert space) from $L^2(G)$ to $L^2(\hat{G})$.

Theorem 2.1.32 (The Fourier Inversion Theorem). Let $\mathfrak{B}(G)$ denote the set of functions $f \in L^1(G)$ such that f is continuous and $\hat{f} \in L^1(\hat{G})$. There exists a Haar measure $d\chi$ on \hat{G} such that for all $f \in \mathfrak{B}(G)$,

$$f(y) = \int_{\hat{G}} \hat{f}(\chi) \overline{\chi(y)} d\chi$$

That is, $\hat{\hat{f}}(y) = f(-y)$. In addition, the Fourier transform $f \mapsto \hat{f}$ identifies $\mathfrak{B}(G)$ with $\mathfrak{B}(\hat{G})$.

Definition 2.1.33 (modular function). If μ is a left Haar measure on G and $x \in G$, the measure $\mu_x(E) = \mu(Ex)$ is again a left Haar measure, because of the commutativity of left and right translations. Hence, by there is a positive number $\Delta(x)$ such that $\mu_x = \Delta(x)\mu$. The function $\Delta : G \rightarrow (0, \infty)$ thus defined. It is called the modular function of G .

Proposition 2.1.34. Δ is a continuous homomorphism from G to the multiplicative group of positive real numbers. Moreover, if μ is a left Haar measure on G , for any $f \in L^1(\mu)$ and y in G we have

$$\int (R_y f) d\mu = \Delta(y^{-1}) \int f d\mu$$

Proposition 2.1.35. The left Haar measures on G are also right Haar measures precisely when Δ is identically 1, in which case G is called unimodular.

- (1) If $G/[G, G]$ is finite or G is compact, then G is unimodular.
- (2) If H is a compact subgroup of G , then $\Delta_G|_H = \Delta_H = 1$

Proposition 2.1.36. Let G be a LCHG, S a LCH space, $\rho : G \times S \rightarrow S$ a transitive G -action on S . Take $s_0 \in S$, define $\varphi : G \rightarrow S, g \mapsto gs_0$. Let H be the stabilizer at s_0 , a closed subgroup of G . It induces a continuous bijection $\Phi : G/H \rightarrow S$.

If G is σ -compact, Φ is a homeomorphism.

Definition 2.1.37. G is a LCHG with left Haar measure dx , H is a closed subgroup of G with left Haar measure $d\xi$, $q : G \rightarrow G/H$ is the canonical quotient map $q(x) = xH$, and Δ_G and Δ_H are the modular functions of G and H . We define a map $P : C_c(G) \rightarrow C_c(G/H)$ by

$$Pf(xH) = \int_H f(x\xi)d\xi.$$

Theorem 2.1.38. Suppose G is a LCHG and H is a closed subgroup. There is a G -invariant Radon measure μ on G/H if and only if $\Delta_G|_H = \Delta_H$. In this case, μ is unique up to a constant factor, and if this factor is suitably chosen we have

$$\int_G f(x)dx = \int_{G/H} Pf d\mu = \int_{G/H} \int_H f(x\xi)d\xi d\mu \quad (f \in C_c(G)).$$

Proposition 2.1.39. G a LCHA. Suppose H is a closed subgroup of G . Then H^\perp is a closed subgroup of \widehat{G} . We have

$$(1) \quad (H^\perp)^\perp = H$$

$$(2) \quad \text{Define } \Phi : (G/H)^\wedge \rightarrow H^\perp \text{ and } \Psi : \widehat{G}/H^\perp \rightarrow \widehat{H} \text{ by}$$

$$\Phi(\eta) = \eta \circ q, \quad \Psi(\xi H^\perp) = \xi|_H,$$

where $q : G \rightarrow G/H$ is the canonical projection. Then Φ and Ψ are isomorphisms of topological groups.

Definition 2.1.40 (Restricted Direct Product). Let $J = \{\nu\}$ be a set of indices for which we are given G_ν , a LCHG, and let J_∞ be a fixed finite subset of J such that for each $\nu \notin J_\infty$ we are given a compact open subgroup $H_\nu \leq G_\nu$. The restricted direct product of G_ν with respect to H_ν is defined by

$$G = \prod'_{\nu \in J} G_\nu = \{(x_\nu) : x_\nu \in G_\nu \text{ with } x_\nu \in H_\nu \text{ for all but finitely many } \nu\}$$

Definition 2.1.41 (topology on restricted direct product). Notice that subsets

$$B = \left\{ \prod N_\nu : N_\nu \text{ a neighborhood of } 1 \in G_\nu \text{ and } N_\nu = H_\nu \text{ for all but finitely many } \nu \right\}$$

of G induces a topological group structure by Theorem 2.1.2.

Moreover, for any $S \subseteq J$, which necessarily contains J_∞ , define G_S by

$$G_S = \prod_{\nu \in S} G_\nu \times \prod_{\nu \notin S} H_\nu$$

G_S is a open subgroup of G and product topology on G_S is identical to the subspace topology induced by restricted direct topology defined above.

Proposition 2.1.42. G itself is a LCHG.

Proposition 2.1.43. A subset Y of G has compact closure if and only if $Y \subseteq \prod K_\nu$, for some family of compact subsets $K_\nu \subseteq G_\nu$, such that $K_\nu = H_\nu$ for all but finitely many indices ν .

Proposition 2.1.44. There exists a topological embedding of $G_\nu \longrightarrow G$ given by

$$x \longmapsto (\dots, 1, 1, x, 1, 1, \dots)$$

where the x is in the ν th component. And image of G_ν is a closed subgroup of G .

Lemma 2.1.45. Let $\chi \in \text{Hom}_{\text{Cont}}(G, \mathbb{C}^\times)$ (quasi-characters). Then χ is trivial on all but finitely many H_ν . Therefore, for $y \in G$, $\chi(y_\nu) = 1$ for all but finitely many ν , and

$$\chi(y) = \prod_{\nu} \chi(y_\nu).$$

Lemma 2.1.46. For each ν let $\chi_\nu \in \text{Hom}_{\text{Cont}}(G_\nu, \mathbb{C}^\times)$ and $\chi_\nu|_{H_\nu} = 1$ for all but finitely many indices ν . Then we have that $\chi = \prod_{\nu} \chi_\nu \in \text{Hom}_{\text{Cont}}(G, \mathbb{C}^\times)$.

Theorem 2.1.47. Let G be the restricted direct product of LCHA G_ν with respect to compact-open subgroups H_ν . As topological groups, we have that

$$\hat{G} \cong \prod' \hat{G}_\nu$$

where the restricted direct product on the right is taken with respect to subgroups defined by

$$K(G_\nu, H_\nu) = \left\{ \chi_\nu \in \hat{G}_\nu : \chi_\nu|_{H_\nu} = 1 \right\}$$

for $\nu \notin J_\infty$. This subgroup traditionally is denoted H_ν^\perp .

Proof: We will begin by showing that $K(G_\nu, H_\nu)$ is a compact-open subgroup of \hat{G}_ν . It is clear that $K(G_\nu, H_\nu)$ is a subgroup of G_ν . Let U be a neighborhood of 1 in \mathbb{C}^\times that contains no other subgroup besides the trivial subgroup. Consider the neighborhood of the trivial character on G_ν defined by

$$W(H_\nu, U) = \left\{ \chi \in \hat{G}_\nu : \chi(H_\nu) \subseteq U \right\}$$

Since $\chi(H_\nu)$ is a subgroup of U , then $\chi(H_\nu) = \{1\}$, and hence

$$W(H_\nu, U) = K(G_\nu, H_\nu)$$

This shows that $K(G_\nu, H_\nu)$ is an open subgroup of \hat{G}_ν . By Proposition 2.1.10 and 2.1.39, $K(G_\nu, H_\nu)$ is a compact open subgroup.

Now, we assume Haar measure on G_ν are all σ -finite.

Definition 2.1.48 (Restricted Direct Integration). Let dg_ν denote a left (right) Haar measure on G_ν normalized so that

$$\int_{H_\nu} dg_\nu = 1$$

for almost all $\nu \notin J_\infty$. Then there is a unique left (respectively, right) Haar measure dg on G such that for each finite set of indices S containing J_∞ , the restriction of dg_S of dg to G_S (open subgroup of G) is precisely the product measure (infinite Radon product described in Analysis 2.6.18, hence also Haar measure on G_S). We will write $dg = \prod_\nu dg_\nu$ for this measure.

Proposition 2.1.49. Let $f \in L^1(G)$, for all $S \supset J_\infty$, we have $f|_{G_S} \in L^1(G_S)$. And if S_n be a sequence of subsets of J such that $S_n \supset J_\infty$ with $S_n \subset S_{n+1}$ and

$$\bigcup_{i=1}^{\infty} S_n = J,$$

then

$$\int_G f(g) = \lim_{n \rightarrow \infty} \int_{G_{S_n}} f(g_S) dg_S$$

Proposition 2.1.50. Let S_0 denote the finite set of indices containing both J_∞ and the set of indices for which $\text{Vol}(H_\nu, dg_\nu) \neq 1$. Suppose that for each index ν , we are given a continuous and integrable function f_ν on G_ν , such that $f_\nu|_{H_\nu} = 1$ for all ν outside some finite set S_1 . Then for $g = (g_\nu) \in G$ we can define the function

$$f(g) = \prod_\nu f_\nu(g_\nu)$$

The function f is well-defined and continuous on G . Furthermore, if S is any finite set of indices including S_0 and S_1 , then we have $f|_{G_S} \in L^1(G_S)$ and

$$\int_{G_S} f(g) dg_S = \prod_{\nu \in S} \left(\int_{G_\nu} f_\nu(g_\nu) dg_\nu \right)$$

Furthermore, if

$$\prod_\nu \left(\int_{G_\nu} |f_\nu(g_\nu)| dg_\nu \right) < \infty$$

then $f \in L^1(G)$ and

$$\int_G f(g) dg = \prod_\nu \left(\int_{G_\nu} f_\nu(g_\nu) dg_\nu \right)$$

Now we assume G_ν are all abelian group.

Proposition 2.1.51. Let $f_\nu \in L^1(G) \cap C(G)$ and of f_ν being a characteristic function of H_ν for all but finite many ν . Then $f \in L^1(G)$ and the Fourier transform of f is given by

$$\hat{f}(g) = \prod_\nu \hat{f}_\nu(g_\nu)$$

Moreover, if we additionally assume $f_\nu \in \mathfrak{B}(G_\nu)$ for all ν , $f \in \mathfrak{B}(G)$.

Proof: The key point is to notice that

$$\hat{f}_\nu(\chi_\nu) = \text{Vol}(H_\nu, dg_\nu) \mathbf{1}_{H_\nu^\perp}(\chi_\nu).$$

Now we need to define dual measure on \hat{G} such that Fourier Inversion Theorem holds.

Theorem 2.1.52. The measure $d\chi = \prod_\nu d\chi_\nu$, where $d\chi_\nu = \widehat{dg_\nu}$, is dual the measure $dg = \prod_\nu dg_\nu$. Therefore,

$$f(g) = \int_{\hat{G}} \hat{f}(\chi) \chi(g) d\chi,$$

for all $f \in \mathfrak{B}(G)$.

Proof: Notice that

$$\begin{aligned} \hat{f}_\nu(g_\nu) &= \text{Vol}(H_\nu, dg_\nu) \int_{\hat{G}_\nu} \mathbf{1}_{H_\nu^\perp}(\chi_\nu) \chi_\nu(g_\nu) d\chi_\nu = \\ &= \text{Vol}(H_\nu, dg_\nu) \int_{H_\nu^\perp} \chi_\nu(g_\nu) d\chi_\nu = \text{Vol}(H_\nu, dg_\nu) \text{Vol}(H_\nu^\perp, d\chi_\nu) \mathbf{1}_{(H_\nu^\perp)^\perp} \end{aligned}$$

and $(H_\nu^\perp)^\perp = H_\nu$. We have $\text{Vol}(H_\nu, dg_\nu) \text{Vol}(H_\nu^\perp, d\chi_\nu) = 1$

2.2 Valuations

Definition 2.2.1. A valuation of a field K is a non-trivial function

$$|\cdot| : K \rightarrow \mathbb{R}$$

enjoying the properties

- (1) $|x| \geq 0$, and $|x| = 0 \iff x = 0$,
- (2) $|xy| = |x||y|$,
- (3) $|x + y| \leq |x| + |y|$

Definition 2.2.2. Two valuations of K are called equivalent if they satisfy one of the following equivalent conditions

- (1) they define the same topology on K .
- (2) there exists a real number $s > 0$ such that one has

$$|x|_1 = |x|_2^s$$

for all $x \in K$

(3)

$$|x|_1 < 1 \implies |x|_2 < 1$$

Definition 2.2.3. The valuation $|\cdot|$ is called nonarchimedean if $|n|$ stays bounded, for all $n \in \mathbb{N}$. Otherwise it is called archimedean.

Proposition 2.2.4. The valuation $|\cdot|$ is nonarchimedean if and only if it satisfies the strong triangle inequality

$$|x + y| \leq \max\{|x|, |y|\}.$$

Proposition 2.2.5. K be a field with non-archimedean valuation. Then

- (1) $a, b \in K, a \neq b$, then $|a + b| = \max(|a|, |b|)$.
- (2) If $a_1 + \dots + a_n = 0$, at least two of them take the maximal valuation.

Definition 2.2.6 (prime divisor).

Theorem 2.2.7 (weak Approximation Theorem). Let $|\cdot|_1, \dots, |\cdot|_n$ be pairwise inequivalent valuations of the field K and let $a_1, \dots, a_n \in K$ be given elements. Then for every $\varepsilon > 0$ there exists an $x \in K$ such that

$$|x - a_i|_i < \varepsilon \quad \text{for all } i = 1, \dots, n$$

Theorem 2.2.8. Every valuation of \mathbb{Q} is equivalent to one of the valuations $|\cdot|_p$ or $|\cdot|_\infty$.

Definition 2.2.9. Let $|\cdot|$ be a nonarchimedean valuation of the field K . Putting

$$v(x) = -\log |x| \quad \text{for } x \neq 0, \quad \text{and } v(0) = \infty$$

we obtain a function

$$v : K \longrightarrow \mathbb{R} \cup \{\infty\}$$

verifying the properties

- (1) $v(x) = \infty \iff x = 0$,
- (2) $v(xy) = v(x) + v(y)$,
- (3) $v(x + y) \geq \min\{v(x), v(y)\}$

A non-zero (on K^*) function v on K with these properties is called an [exponential valuation](#) of K . Two exponential valuations v_1 and v_2 of K are called equivalent if $v_1 = sv_2$, for some real number $s > 0$. For every exponential valuation v we obtain a valuation by putting

$$|x| = q^{-v(x)}$$

for some fixed real number $q > 1$. To distinguish it from v , we call $|\cdot|$ an associated multiplicative valuation, or [absolute value](#). Moreover, there's a one-to-one correspondence between equivalence class of non-archimedean absolute value and equivalence class of exponential valuation.

Definition 2.2.10. The subset

$$\mathcal{O} = \{x \in K \mid v(x) \geq 0\} = \{x \in K : |x| \leq 1\}$$

is a ring with group of units

$$\mathcal{O}^* = \{x \in K \mid v(x) = 0\} = \{x \in K : |x| = 1\}$$

and the unique maximal ideal

$$\mathfrak{p} = \{x \in K \mid v(x) > 0\} = \{x \in K : |x| < 1\}.$$

Theorem 2.2.11. For finite \mathbb{F}_q and $K = \mathbb{F}_q(t)$ the function field in one variable. The valuations $v_{\mathfrak{p}}$ associated to the prime ideals $\mathfrak{p} = (p(t))$ of $\mathbb{F}_q[t]$, together with the degree valuation

$$v_{\infty} : \frac{f}{g} \mapsto \deg g - \deg f$$

, are the only valuations of K , up to equivalence.

Proof: If \mathcal{O} (ring of integers) $\supset \mathbb{F}_q[t]$, we have $\mathfrak{p} \cap \mathbb{F}_q[t]$ is a prime ideal of $\mathbb{F}_q[t]$. Hence there's a monic irreducible polynomial $p(t)$ over $\mathbb{F}_q[t]$ such that $\mathfrak{p} \cap \mathbb{F}_q[t] = (p(t))$. Hence v is equivalent to $v_{\mathfrak{p}}$.

If $\mathbb{F}_q[t]$ is not a subset of \mathcal{O} . We have $v(t) < 0$. Hence v is equivalent to v_{∞} .

Theorem 2.2.12 (Product Formula). Consider $q > 1$ be a fixed real number and $\mathbb{F}_q(t)$, for irreducible polynomial $p(t)$, we put

$$|f|_p = q^{-\deg(p)v(f)}$$

and $|f|_{\infty} = q^{-v_{\infty}(f)}$. Then

$$\prod_p |f|_p = 1$$

where p varies over ∞ and irreducible polynomial of $\mathbb{F}_q(t)$.

Definition 2.2.13 (discrete valuation). An exponential valuation v is called discrete if it admits a smallest positive value s . In this case, one finds

$$v(K^*) = s\mathbb{Z}$$

It is called normalized if $s = 1$. Dividing by s we may always pass to a normalized valuation without changing the invariants $\mathcal{O}, \mathcal{O}^*, \mathfrak{p}$. Having done so, an element

$$\pi \in \mathcal{O} \text{ such that } v(\pi) = 1$$

is a prime element, and every element $x \in K^*$ admits a unique representation

$$x = u\pi^m$$

with $m \in \mathbb{Z}$ and $u \in \mathcal{O}^*$. For if $v(x) = m$, then $v(x\pi^{-m}) = 0$, hence $u = x\pi^{-m} \in \mathcal{O}^*$. If v is a discrete exponential valuation of K , then

$$\mathcal{O} = \{x \in K \mid v(x) \geq 0\}$$

is a principal ideal domain. Suppose v is normalized. Then the nonzero ideals of \mathcal{O} are given by

$$\mathfrak{p}^n = \pi^n \mathcal{O} = \{x \in K \mid v(x) \geq n\}, \quad n \geq 0$$

where π is a prime element, i.e., $v(\pi) = 1$. One has

$$\mathfrak{p}^n / \mathfrak{p}^{n+1} \cong \mathcal{O} / \mathfrak{p}$$

In a discretely valued field K the chain

$$\mathcal{O} \supseteq \mathfrak{p} \supseteq \mathfrak{p}^2 \supseteq \mathfrak{p}^3 \supseteq \dots$$

consisting of the ideals of the valuation ring \mathcal{O} forms a basis of neighbourhoods of the zero element. Indeed, if v is a normalized exponential valuation and $|\cdot| = q^{-v}$ ($q > 1$) an associated multiplicative valuation, then

$$\mathfrak{p}^n = \left\{ x \in K : |x| < \frac{1}{q^{n-1}} \right\}$$

As a basis of neighbourhoods of the element 1 of K^* , we obtain in the same way the descending chain

$$\mathcal{O}^* = U^{(0)} \supseteq U^{(1)} \supseteq U^{(2)} \supseteq \dots$$

of subgroups

$$U^{(n)} = 1 + \mathfrak{p}^n = \left\{ x \in K^* : |1 - x| < \frac{1}{q^{n-1}} \right\}, \quad n > 0$$

of \mathcal{O}^* .

Theorem 2.2.14. Let K be a field which is complete with respect to an archimedean valuation $|\cdot|$. Then there is an isomorphism σ from K onto \mathbb{R} or \mathbb{C} satisfying

$$|a| = |\sigma a|^s \quad \text{for all } a \in K$$

for some fixed $s \in (0, 1]$.

Proposition 2.2.15. Assume E/F be a field extension, P be a non-archimedean prime divisor on F and Q be an extension of P on E . Define

$$e = e(Q/P) = [v(E^\times) : v(F^\times)]$$

$$f = f(Q/P) = [\bar{E} : \bar{F}]$$

Proposition 2.2.16. Assume E/F be a field extension, and P be a non-archimedean prime divisor on F . Q be an extension of P on E . Denote ring of integers of E by O_E . If E/F is finite,

- (1) If $w_1, \dots, w_r \in O_E$, and $\bar{w}_1, \dots, \bar{w}_r \in \bar{E}$ are \bar{F} -linearly independent, then for $a_1, \dots, a_r \in F$, we have

$$v(a_1 w_1 + \dots + a_r w_r) = \min_{1 \leq i \leq r} \{v(a_i)\}$$

In particular, w_1, \dots, w_r are F -linearly independent. Hence $f(Q/P) \leq [E : F]$.

- (2) If $\pi_0, \dots, \pi_s \in E^\times$, and $v(\pi_j)$ ($0 \leq j \leq s$) are representatives for $v(F^\times)/v(E^\times)$, then for $b_0, \dots, b_s \in F$, we have

$$v(b_0 \pi_0 + \dots + b_s \pi_s) = \min_{0 \leq j \leq s} \{v(b_j \pi_j)\}$$

In particular, π_0, \dots, π_s are F -linearly independent. Hence, $e(Q/P) \leq [E : F]$.

Proposition 2.2.17. P is a non-archimedean prime divisor on K . $(K, P) \subset (\hat{K}, \hat{P})$ be the completion of (K, P) . Then $f(\hat{P}/P) = e(\hat{P}/P) = 1$ and the closure of ring of integers of K is the ring of integers of \hat{K} .

Theorem 2.2.18. For arbitrary discrete valuation v of the field K , let $R \subseteq \mathcal{O}$ be a system of representatives for $K = \mathcal{O}/\mathfrak{p}$ such that $0 \in R$, and let $\pi \in \mathcal{O}$ be a prime element. Then every $x \neq 0$ in \hat{K} admits a unique representation as a convergent series

$$x = \pi^m (a_0 + a_1 \pi + a_2 \pi^2 + \dots)$$

where $a_i \in R, a_0 \neq 0, m \in \mathbb{Z}$.

Example 2.2.19. Consider $\mathbb{F}_q((t))$ to be the ring of formal laurent series, and it can be shown that $\mathbb{F}_q((t))$ is a field. Define

$$v(a_r x^r + \dots) = r, \text{ where } a_r \neq 0$$

Then $\mathbb{F}_q((t))$ becomes a complete, discrete exponential valuation with finite residue field.

Lemma 2.2.20 (Hensel's Lemma). Let K again be a field which is complete with respect to a nonarchimedean valuation $|\cdot|$. Let \mathcal{O} be the corresponding valuation ring with maximal ideal \mathfrak{p} and residue class field $K = \mathcal{O}/\mathfrak{p}$. We call a polynomial $f(x) = a_0 + a_1 x + \dots + a_n x^n \in \mathcal{O}[x]$ primitive if $f(x) \not\equiv 0 \pmod{\mathfrak{p}}$, i.e., if

$$|f| = \max \{|a_0|, \dots, |a_n|\} = 1$$

If a primitive polynomial $f(x) \in \mathcal{O}[x]$ admits a factorization

$$f(x) \equiv \bar{g}(x) \bar{h}(x) \pmod{\mathfrak{p}}$$

into relatively prime polynomials $\bar{g}, \bar{h} \in \kappa[x]$, then $f(x)$ admits a factorization

$$f(x) = g(x)h(x)$$

into polynomials $g, h \in \mathcal{O}[x]$ such that $\deg(g) = \deg(\bar{g})$ and

$$g(x) \equiv \bar{g}(x) \pmod{\mathfrak{p}} \quad \text{and} \quad h(x) \equiv \bar{h}(x) \pmod{\mathfrak{p}}$$

Corollary 2.2.21. Let the field K be complete with respect to the nonarchimedean valuation $|\cdot|$ (e.g. \mathbb{C}_p or finite extension of \mathbb{Q}_p). Then, for every irreducible polynomial $f(x) = a_0 + a_1x + \cdots + a_nx^n \in K[x]$ such that $a_0a_n \neq 0$, one has

$$|f| = \max\{|a_0|, |a_n|\}$$

In particular, $a_n = 1$ and $a_0 \in \mathcal{O}$ imply that $f \in \mathcal{O}[x]$.

Theorem 2.2.22. Let K be complete with respect to the valuation $|\cdot|$. Then $|\cdot|$ may be extended in a unique way to a valuation of any given algebraic extension L/K . This extension is given by the formula

$$|\alpha| = \sqrt[n]{|N_{L/K}(\alpha)|}$$

when L/K has finite degree n . In this case L is again complete.

Definition 2.2.23. For a Global field, we mean finite extension of \mathbb{Q} or $\mathbb{F}_q(t)$. For a Local field, we mean a field with discrete, complete valuation such that the residue field is finite.

Proposition 2.2.24. A local field is locally compact and its valuation ring is compact.

Theorem 2.2.25. Let L be a local field. Then L is isomorphic to a finite extension of \mathbb{Q}_p or $\mathbb{F}_q((t))$.

Proposition 2.2.26. The multiplicative group of a local field K admits the decomposition

$$K^* = (\pi) \times \mu_{q-1} \times U^{(1)}$$

Here π is a prime element, $(\pi) = \{\pi^k \mid k \in \mathbb{Z}\}$, $q = \#\kappa$ is the number of elements in the residue class field $\kappa = \mathcal{O}/\mathfrak{p}$, μ_{q-1} be the group of $q-1$ -th roots of unit, and $U^{(1)} = 1 + \mathfrak{p}$ is the group of principal units.

Now we assume E/F is an extension of p -adic fields with $\mathcal{O}_E, \mathcal{O}_F, \bar{E}, \bar{F}$ their rings of integers and residue fields.

Theorem 2.2.27. If $\alpha_1, \alpha_2, \dots, \alpha_f \in \mathcal{O}_E$ are preimage of a basis for extension \bar{E}/\bar{F} , then elements

$$\begin{aligned} &\alpha_1, \alpha_2, \dots, \alpha_f \\ &\pi\alpha_1, \pi\alpha_2, \dots, \pi\alpha_f \\ &\pi^2\alpha_1, \pi^2\alpha_2, \dots, \pi^2\alpha_f \\ &\dots \\ &\pi^{e-1}\alpha_1, \pi^{e-1}\alpha_2, \dots, \pi^{e-1}\alpha_m \end{aligned}$$

form a basis of E/F . In particular, $ef = [E : F]$.

Proof: By Hensel's Lemma, we find that the order of group of $(q-1)$ -th roots of unit is $q-1$.

Proposition 2.2.28. $x \in O_E$ iff x is a root of polynomial with coefficients in O_K , i.e. O_K is the integral closure of O_E .

Proof: By the definition of absolute value on K and Proposition 1.1.3.

Proposition 2.2.29. O_E is a free O_K -module with rank n .

Proof: By structure of finitely generated module over PID and Lemma 1.1.8.

Proposition 2.2.30. E/F is unramified if $e=1, f=n$.

- (1) E/F 是不分歧扩张. 如果 $\bar{E} = \bar{F}(\alpha_0)$, 取元素 $\alpha \in O_E$, 使得 $\bar{\alpha} = \alpha_0$, 则 $E = F(\alpha)$, 并且若 $f(x)$ 是 α 在 F 上的极小多项式, 则 $\bar{f}(x)$ 是 $\bar{\alpha}$ 在 \bar{F} 上的极小多项式.
- (2) 若 $E = F(\alpha), \alpha \in O_E, g(x)$ 是 $O_F[x]$ 中首 1 多项式, $g(\alpha) = 0$. 如果 $\bar{g}(x)$ (在 \bar{F} 的代数闭包 $\bar{\Omega}$ 中) 没有重根, 则 E/F 是不分歧扩张.

Example 2.2.31. Consider all the (p^f-1) -th roots of unity in $\overline{\mathbb{Q}_p}$. ζ is a primitive (p^f-1) -th root of unity. Then $\mathbb{Q}_p(\zeta)$ is the unique unramified extension with degree f .

Proof: Let K be a finite extension of \mathbb{Q}_p with uniformizer π . By Hensel's Lemma, since $x^{p^f-1} - 1 \equiv 0 \pmod{\pi}$ have p^f-1 different solution on O_K/P , all the (p^f-1) -th root of unity lie in O_K . If ζ is a primitive (p^f-1) -th root of unity, notice that $\bar{\zeta}, \dots, \bar{\zeta}^{p^f-1}$ are all distinct in the residue field of $\mathbb{Q}_p(\zeta)$, we have $f = f(\mathbb{Q}_p(\zeta)/\mathbb{Q}_p)$.

Hence if we find an unramified extension K_1 of degree f , then $K_1 = \mathbb{Q}_p(\zeta)$ which shows that $\mathbb{Q}_p(\zeta)$ is the unique unramified subfield of algebraic closure of \mathbb{Q}_p .

Let

$$\bar{g}(X) = X^f + \bar{a}_{f-1}X^{f-1} + \dots + \bar{a}_1X + \bar{a}_0$$

be an irreducible polynomial over \mathbb{F}_p . Lifting $\bar{g}(X)$ to $g(X) \in \mathbb{Z}_p[X]$ any way we like, we get an irreducible polynomial over \mathbb{Q}_p . If α is a root of $g(X)$, then $K = \mathbb{Q}_p(\alpha)$ is an unramified extension of degree f .

Proposition 2.2.32. E/F finite extension of p -adic field.

- (1) 若 K/F 是 p -adic fields 的有限扩张, E/F 不分歧, 则 KE/K 不分歧.
- (2) 若 $E_1/F, E_2/F$ 均不分歧, 则 E_1E_2/F 不分歧.

Example 2.2.33. Let ζ_n be primitive n -th root of unit in algebraic closure of \mathbb{Q}_p , $p \nmid n$, then $\mathbb{Q}_p(\zeta_n) = \mathbb{Q}_p(\zeta_{p^m-1})$ where m is the order of p module n .

Proof: On the one hand, $\mathbb{Q}_p(\zeta_n) \subset \mathbb{Q}_p(\zeta_{p^m-1})$, hence $m \geq f(\mathbb{Q}_p(\zeta_n)/\mathbb{Q}_p)$

On the other hand, by Proposition 2.2.30, $\mathbb{Q}_p(\zeta_n)$ is unramified. Since $p \nmid n$, $x^n - 1 = (x - 1) \dots (x - \zeta_n^{n-1})$ shows that the order of $\bar{\zeta}_n$ is n . Then

$$m = [\mathbb{F}_p(\bar{\zeta}_n) : \mathbb{F}_p] \leq f(\mathbb{Q}_p(\zeta_n)/\mathbb{Q}_p) = [\mathbb{Q}_p(\zeta_n) : \mathbb{Q}_p]$$

The first equality holds because $x \mapsto x^p$ is a generator of the Galois group of $\mathbb{F}_p(\bar{\zeta}_n)/\mathbb{F}_p$.

Proposition 2.2.34. E/F finite extension of p -adic field.

- (1) 若 E/F 是完全分歧的, 则 $E = F(\pi)$, 并且 π 在 F 上的最小多项式为 Eisenstein 多项式.
- (2) 反之, 若 $E = F(\alpha)$ 并且 α 在 F 上的最小多项式是 Eisenstein 多项式, 则 E/F 是完全分歧扩张, 并且 α 是 E 的一个素元.

Proposition 2.2.35. Let ζ be a primitive p^m -th root of unity. Then one has:

- (1) $\mathbb{Q}_p(\zeta) \mid \mathbb{Q}_p$ is totally ramified of degree $\varphi(p^m) = (p-1)p^{m-1}$.
- (2) $\text{Gal}(\mathbb{Q}_p(\zeta) \mid \mathbb{Q}_p) \cong (\mathbb{Z}/p^m\mathbb{Z})^*$.
- (3) $\mathbb{Z}_p[\zeta]$ is the valuation ring of $\mathbb{Q}_p(\zeta)$.
- (4) $1 - \zeta$ is a prime element of $\mathbb{Z}_p[\zeta]$ with norm p .

Proposition 2.2.36. If $n = p^l m$, $(m, p) = 1$, then

$$f(\mathbb{Q}_p(\zeta_n)/\mathbb{Q}_p) = f(\mathbb{Q}_p(\zeta_m)/\mathbb{Q}_p) = \text{order of } p \text{ module } m$$

, and

$$e(\mathbb{Q}_p(\zeta_n)/\mathbb{Q}_p) = e(\mathbb{Q}_p(\zeta_{p^l})/\mathbb{Q}_p) = \varphi(p^l)$$

Theorem 2.2.37. Let K be a p -adic field and $q = p^f$ the number of elements in the residue class field. Then

$$K^* \cong \mathbb{Z} \oplus \mathbb{Z}/(q-1)\mathbb{Z} \oplus \mathbb{Z}/p^a\mathbb{Z} \oplus \mathbb{Z}_p^d$$

where

$$p^a = \# \bigcup_{n=1}^{\infty} \mu_{p^n} \cap K^*$$

and $d = [K : \mathbb{Q}_p]$. (μ_{p^n} is the group of all the p^n -th root of unity in algebraic closure of \mathbb{Q}_p)

Proof: Since

$$K^* = (\pi) \times \mu_{q-1} \times U^{(1)} \cong \mathbb{Z} \oplus \mathbb{Z}/(q-1)\mathbb{Z} \oplus U^{(1)}$$

This reduces us to the computation of the \mathbb{Z}_p -module $U^{(1)}$.

For n sufficiently big, \log and \exp gives us the isomorphism

$$\log : U^{(n)} \longrightarrow \mathfrak{p}^n = \pi^n \mathcal{O} \cong \mathcal{O}$$

Moreover, \mathcal{O} admits an integral basis $\alpha_1, \dots, \alpha_d$ over \mathbb{Z}_p , i.e., $\mathcal{O} = \mathbb{Z}_p\alpha_1 \oplus \dots \oplus \mathbb{Z}_p\alpha_d \cong \mathbb{Z}_p^d$. Therefore $U^{(n)} \cong \mathbb{Z}_p^d$. Since the index $(U^{(1)} : U^{(n)})$ is finite and $U^{(n)}$ is a finitely generated free \mathbb{Z}_p -module of rank d , so is free part of $U^{(1)}$. The torsion subgroup of $U^{(1)}$ is the group μ_{p^a} of roots of unity in K of p -power order. (consider the kernel of \log). By the main theorem on modules over principal ideal domains, there exists in $U^{(1)}$ a free, finitely generated \mathbb{Z}_p -submodule V of rank d such that

$$U^{(1)} = \mu_{p^a} \times V \cong \mathbb{Z}/p^a\mathbb{Z} \oplus \mathbb{Z}_p^d$$

Corollary 2.2.38.

$$(K^* : K^{*n}) = n(U : U^n) = n \times p^{dv_p(n)} \# \mu_n(K).$$

Theorem 2.2.39. Fix an algebraic closure of \mathbb{Q}_p ($p = \infty$ or a prime number). For a finite extension of \mathbb{Q} , if $\sigma : K \rightarrow \overline{\mathbb{Q}_p}$ is a \mathbb{Q} -embedding, define

$$v : K \mapsto \mathbb{R} = |\cdot|_p \circ \sigma$$

Then, v is an extension of $|\cdot|_p$ and for the completion (\hat{K}, \hat{v}) of (K, v) , there's unique way extends σ to \hat{K} continuously and preserves absolute value. Meanwhile, the image of the completion coincides with the completion of K and \mathbb{Q}_p which also be a finite extension of \mathbb{Q}_p .

$$\begin{array}{ccc} \hat{K} & \xrightarrow{\hat{\sigma}} & \overline{\mathbb{Q}_p} \\ & \nwarrow \sigma & \uparrow \\ & K & \mathbb{Q}_p \\ & \uparrow & \nearrow \\ \mathbb{Q} & & \end{array} \quad \hat{\sigma}(\hat{K}) = \mathbb{Q}_p K$$

Theorem 2.2.40. K is a algebraic number field, $|\cdot|_p$ (finite or infinite) is an absolute value on \mathbb{Q} . Fix an algebraic closure of \mathbb{Q}_p .

- (1) every absolute value on K which extends $|\cdot|_p$ is given by \mathbb{Q} -embedding from K to $\overline{\mathbb{Q}_p}$.
- (2) σ_1 and σ_2 induce the same absolute value if and only if $\sigma_1 = \varphi \circ \sigma_2$ for some φ in absolute Galois group of \mathbb{Q}_p .

Theorem 2.2.41. Assume $p = \infty$ or a prime number. Suppose the extension K/\mathbb{Q} is generated by the zero α of the irreducible polynomial $f(X) \in \mathbb{Q}[X]$. Then the valuations w_1, \dots, w_r extending $|\cdot|_p$ to K correspond 1-1 to the irreducible factors f_1, \dots, f_r in the decomposition

$$f(X) = f_1(X) \cdots f_r(X)$$

of f over the completion \mathbb{Q}_p . Moreover, the completion of K at w_i is isomorphic to $\mathbb{Q}_p(\alpha_i)$ where α_i is a root of f_i .

Moreover, consider \mathbb{Q}_p -algebra $\prod_{i=1}^r \mathbb{Q}_p(\alpha_i)$ and $K \otimes_{\mathbb{Q}} \mathbb{Q}_p$, the map

$$\varphi : K \otimes_{\mathbb{Q}} \mathbb{Q}_p \rightarrow \prod_{i=1}^r \mathbb{Q}_p(\alpha_i), x \otimes \beta \mapsto (\beta \sigma_i(x))_i$$

gives an isomorphism between \mathbb{Q}_p -algebra. This is because, by previous theorem, the dimension of these two \mathbb{Q}_p -algebra are the same and to show $\text{Ker} \varphi = 0$, notice that $1 \otimes 1, \alpha \otimes 1, \dots, \alpha^{n-1} \otimes 1$ form a basis of $K \otimes_{\mathbb{Q}} \mathbb{Q}_p$. Then $\text{Ker} \varphi = 0$ follows from the determinant of Vandermonde matrix.

Therefore, consider the characteristic polynomial of $x \otimes 1 \in K \otimes_{\mathbb{Q}} \mathbb{Q}_p$ and $\sigma_i(x)$ in $\mathbb{Q}_p(\alpha_i)$, we have

$$\text{char. polynomial}_{K/\mathbb{Q}}(x) = \prod_{i=1}^r \text{char. polynomial}_{\mathbb{Q}_p(\alpha_i)/\mathbb{Q}_p}(\sigma_i(x)).$$

And we can obtain some basis corollary of this formula: for all $x \in K$,

$$N_{K/\mathbb{Q}}(x) = \prod_{i=1}^r N_{\mathbb{Q}_p(\alpha_i)/\mathbb{Q}_p}(\sigma_i(x)), \quad \text{Tr}_{K/\mathbb{Q}}(x) = \sum_{i=1}^r \text{Tr}_{\mathbb{Q}_p(\alpha_i)/\mathbb{Q}_p}(\sigma_i(x))$$

Corollary 2.2.42. K is an algebraic number field, assume

$$p\mathcal{O}_K = \mathfrak{P}_1^{e_1} \dots \mathfrak{P}_g^{e_g}$$

Then the valuation that extends $|\cdot|_p$ are precisely $v_{\mathfrak{P}_i}(\cdot), i = 1, \dots, g$. And $e(K_{\mathfrak{P}_i}/\mathbb{Q}_p) = e_i, f(K_{\mathfrak{P}_i}/\mathbb{Q}_p) = f_i$.

Lemma 2.2.43 (Krasner's Lemma). Let K be a non-archimedean complete valued field of characteristic zero, and let a and b be elements of the algebraic closure of K . Let $a_1 = a, a_2, \dots, a_n$ be the conjugates of a over K . Suppose that b is closer to a than any of conjugates of a , i.e.,

$$|b - a| < |a - a_i|$$

for $i = 2, 3, \dots, n$. Then $K(a) \subset K(b)$.

Theorem 2.2.44. Let K be a non-archimedean complete valued field of characteristic zero. Let

$$f(X) = X^n + a_{n-1}X^{n-1} + \dots + a_1X + a_0 \in K[X]$$

be a monic irreducible polynomial of degree n with coefficients in K , let λ be a root of $f(X)$, and let $L = K(\lambda)$ be the extension of K obtained by adjoining that root. Then there exists a real number $\varepsilon > 0$ such that the following holds: If $g(X) = X^n + b_{n-1}X^{n-1} + \dots + b_1X + b_0 \in K[X]$ is any monic polynomial of degree n for which we have

$$|a_i - b_i| < \varepsilon \quad \text{for all } i = 0, 1, \dots, n-1$$

then $g(X)$ is irreducible over K and has a root in L .

Definition 2.2.45 (\mathbb{C}_p). Let $\overline{\mathbb{Q}_p}$ be algebraic closure of \mathbb{Q}_p . Firstly we show that $\overline{\mathbb{Q}_p}$ is not complete.

Firstly, assume $\overline{\mathbb{Q}_p}$ is complete. Choose integers f_0, f_1, f_2, \dots such that $f_i < f_{i+1}$. For each i , let $m_i = p^{f_i} - 1$ and let ζ_i be a primitive m_i -th root of unity, so that $\mathbb{Q}_p(\zeta_i)$ is the unique unramified extension of degree f_i . Now construct the series

$$\sum_{i=0}^{\infty} \zeta_i p^i$$

The partial sums of this series clearly form a Cauchy sequence in $\overline{\mathbb{Q}_p}$. Define

$$c = \zeta_0 + \zeta_1 p + \zeta_2 p^2 + \dots$$

Assume $d = [\mathbb{Q}_p(c) : \mathbb{Q}_p]$, P be the set of non-unit elements of ring of integers of $\mathbb{Q}_p(c)$ and $p_i(x) \in \mathbb{Z}_p[x]$ is the minimal polynomial of ζ_i for $i = 0, 1, 2, \dots$. By Hensel's Lemma over $\mathbb{Q}_p(c)$, since $p_0(c) \equiv 0 \pmod{P}$, $\mathbb{Q}_p(c) \supset \mathbb{Q}_p(\zeta_0)$. Let $c_1 = (c - \zeta_0)/p$. Since $\zeta_0 \in \mathbb{Q}_p(c)$, we have $c_1 \in \mathbb{Q}_p(c)$ as well. Hence $\mathbb{Q}_p(c) \supset \mathbb{Q}_p(\zeta_1)$ as well. Hence we have $d \geq f_i$, a contradiction!

Definte \mathbb{C}_p be the completion of $\overline{\mathbb{Q}_p}$.

Proposition 2.2.46. \mathbb{C}_p is algebraic closed.

Proof: Take an irreducible polynomial $f(X)$ with coefficients in \mathbb{C}_p . Since $\overline{\mathbb{Q}_p}$ is dense in \mathbb{C}_p , we can find polynomials of the same degree and with coefficients in $\overline{\mathbb{Q}_p}$ whose coefficients are as close as we like to the coefficients of $f(X)$. By Theorem 2.2.44, if we choose such an $f_0(X)$ with coefficients close enough to those of $f(X)$, it will be irreducible over \mathbb{C}_p , and a fortiori also irreducible over $\overline{\mathbb{Q}_p}$. Since $\overline{\mathbb{Q}_p}$ is algebraically closed, this means that $f_0(X)$ will have degree one. Since $f(X)$ and $f_0(X)$ have the same degree, it follows that $f(X)$ has degree one.

Theorem 2.2.47 (Newton's Polygon). Fix a absolute value $|\cdot|$ and valuation v_p on \mathbb{C}_p such that it extends normal absolute value and valuation on \mathbb{Q} . Let $f(X) = 1 + a_1 X + a_2 X^2 + \dots + a_n X^n \in \mathbb{C}_p[X]$ be a polynomial, and let m_1, m_2, \dots, m_r be the slopes of its Newton polygon (in increasing order). Let i_1, i_2, \dots, i_r be the corresponding lengths. Then, for each $k, 1 \leq k \leq r$, $f(X)$ has exactly i_k roots (in \mathbb{C}_p , counting multiplicities) of absolute value p^{m_k} .

Lemma 2.2.48 (Lucas' Theorem). Let n, m be positive integers with $k < n$, written in base p as $n = b_0 + b_1 p + \dots + b_s p^s$ and $m = a_0 + a_1 p + \dots + a_s p^s$. (We add extra zeros to the base p expansion of m if necessary so that the two expansions have the same length.) Then

$$\binom{n}{m} \equiv \binom{b_0}{a_0} \binom{b_1}{a_1} \dots \binom{b_s}{a_s} \pmod{p}$$

Example 2.2.49. Exponential Taylor polynomials

$$E_n(x) = 1 + x + \frac{x^2}{2!} + \dots + \frac{x^n}{n!}$$

and the Laguerre polynomials

$$L_n(x) = \sum_{j=0}^n (-1)^j \binom{n}{j} \frac{x^j}{j!}$$

are irreducible over \mathbb{Q} for all n .

Proof: If we write $n = b_1 p^{n_1} + b_2 p^{n_2} + \cdots + b_s p^{n_s}$ with $n_1 > n_2 > \cdots > n_s$ and $0 < b_i < p$, then the vertices of the Newton polygon of $E_n(x)$ are $x_0 = (0, 0)$ and $(x_i, -\text{ord}_p(x_i!))$ for $1 \leq i \leq s$, where $x_i = b_1 p^{n_1} + \cdots + b_i p^{n_i}$, and the corresponding slopes of $E_n(x)$ are

$$m_i = \frac{-(p^{n_i} - 1)}{p^{n_i}(p - 1)}$$

Moreover, p -adic Newton polygon for $L_n(x)$ is equal to the Newton polygon for $E_n(x)$. Indeed, each coefficient of $L_n(x)$ has valuation at least as big as the corresponding coefficient of $E_n(x)$, and it follows from Lucas' theorem that $\binom{n}{x_i} \equiv 1 \pmod{p}$, so in particular $\text{ord}_p\left(\binom{n}{x_i}\right) = 0$.

Indeed, if p^m divides n then p^m divides the denominator of each m_i in lowest terms, hence the denominator of the valuation of each root of $f(x)$ in lowest terms. This implies that p^m divides the degree of every irreducible factor of $f(x)$ over \mathbb{Q}_p , hence over \mathbb{Q} as well. Thus every irreducible factor of $f(x)$ over \mathbb{Q} has degree divisible by $n = \prod_p p^{\text{ord}_p(n)}$.

2.3 p-adic analysis

Assume K is a finite extension of \mathbb{Q}_p with π a uniformizer.

Proposition 2.3.1. (1) A sequence (a_n) in K is Cauchy if and only if

$$\lim_{n \rightarrow \infty} |a_{n+1} - a_n| = 0$$

- (2) If a sequence (a_n) converges to a non-zero limit a , then we have $|a_n| = |a|$ for all sufficiently large n .
- (3) Let $b_{ij} \in K$, and suppose that for every i , $\lim_{j \rightarrow \infty} b_{ij} = 0$, and $\lim_{i \rightarrow \infty} b_{ij} = 0$ uniformly in j . Then both series

$$\sum_{i=0}^{\infty} \left(\sum_{j=0}^{\infty} b_{ij} \right) \quad \text{and} \quad \sum_{j=0}^{\infty} \left(\sum_{i=0}^{\infty} b_{ij} \right)$$

converge, and their sums are equal.

Proposition 2.3.2. Let $f(X) = \sum_{n=0}^{\infty} a_n X^n$, and define

$$\rho = \frac{1}{\limsup_{n \rightarrow \infty} \sqrt[n]{|a_n|}}$$

where we use the usual conventions when the limit is zero or infinity, so that $0 \leq \rho \leq \infty$.

- (1) If $\rho = 0$, then $f(x)$ converges only when $x = 0$.
- (2) If $\rho = \infty$, then $f(x)$ converges for every $x \in K$.
- (3) If $0 < \rho < \infty$ and $\lim_{n \rightarrow \infty} |a_n| \rho^n = 0$, then $f(x)$ converges if and only if $|x| \leq \rho$.
- (4) If $0 < \rho < \infty$ and $|a_n| \rho^n$ does not tend to zero as n goes to infinity, then $f(x)$ converges if and only if $|x| < \rho$.

Theorem 2.3.3 (uniqueness of coefficients). If $f(X) = \sum a_n X^n$ and $g(X) = \sum b_n X^n$ are power series with coefficients in K , x_m is a convergent sequence (since every open ball is closed, the limit still lies in the open ball) contained in the intersection of the disks of convergence of f and g , and we have $f(x_m) = g(x_m)$ for all m , then $a_n = b_n$ for all n .

Proposition 2.3.4. Let $f(X) = \sum a_n X^n$ and $g(X) = \sum b_n X^n$ be formal power series with $b_0 = 0$, and let $h(X) = f(g(X))$ be their formal composition. Suppose that

- (1) $g(x)$ converges,
- (2) $f(g(x))$ converges ,
- (3) for every n , we have $|b_n x^n| \leq |g(x)|$ (in other words, no term of the series converging to $g(x)$ is bigger than the sum).

Then $h(x)$ also converges, and $f(g(x)) = h(x)$.

Proposition 2.3.5. Let $f(X)$ and $g(X)$ be formal power series, and suppose $x \in \mathbb{Q}_p$. If $f(x)$ and $g(x)$ both converge, then:

- (1) $(f + g)(x)$ converges and is equal to $f(x) + g(x)$, and
- (2) $(fg)(x)$ converges and is equal to $f(x)g(x)$.

Proposition 2.3.6. Given a power series $f(X) = \sum_{n=0}^{\infty} a_n X^n$, we define its formal derivative to be $f'(X) = \sum_{n=1}^{\infty} n a_n X^{n-1}$. Show that this has the usual properties of a derivative:

- (1) $(f + g)'(X) = f'(X) + g'(X)$.
- (2) $(fg)'(X) = f'(X)g(X) + f(X)g'(X)$.
- (3) If $h(X) = f(g(X))$ where $g(X) = b_1 X + \dots$, then $h'(X) = f'(g(X))g'(X)$.

Proposition 2.3.7. Let $f(X) = \sum a_n X^n$ be a power series with non-zero radius of convergence and let $f'(X)$ be its formal derivative. Let $x \in K$. If $f(x)$ converges, then so does $f'(x)$.

Proposition 2.3.8. Suppose $f(X)$ and $g(X)$ are power series, and suppose that both series converge for $|x| < \rho$. If $f'(x) = g'(x)$ for all $|x| < \rho$, then there exists a constant $c \in K$ such that $f(X) = g(X) + c$ as power series.

Since every point in open ball is the center of the ball, we hope every power series has the same radius after a translation.

Proposition 2.3.9. Let $f(X) = \sum a_n X^n$ be a power series with coefficients in K , and let $\alpha \in K, \alpha \neq 0$, be a point for which $f(\alpha)$ converges. For each $m \geq 0$, define

$$b_m = \sum_{n \geq m} \binom{n}{m} a_n \alpha^{n-m}$$

and consider the power series

$$g(X) = \sum_{m=0}^{\infty} b_m (X - \alpha)^m$$

- (1) The series defining b_m converges for every m , so that the b_m are welldefined.
- (2) The power series $f(X)$ and $g(X)$ have the same region of convergence, that is, $f(\lambda)$ converges if and only if $g(\lambda)$ converges.
- (3) For any λ in the region of convergence, we have $g(\lambda) = f(\lambda)$.

Theorem 2.3.10 (Strassman). Let

$$f(X) = \sum_{n=0}^{\infty} a_n X^n = a_0 + a_1 X + a_2 X^2 + \dots$$

be a non-zero power series with coefficients in K , and suppose that we have $\lim_{n \rightarrow \infty} a_n = 0$, so that $f(x)$ converges for all $x \in O_K$. Let N be the integer defined by the two conditions

$$|a_N| = \max_n |a_n| \quad \text{and} \quad |a_n| < |a_N| \quad \text{for } n > N$$

Then the function $f : O_K \rightarrow K$ defined by $x \mapsto f(x)$ has at most N zeros.

Definition 2.3.11 (log on p-adic field). For a p-adic number field K there is a uniquely determined continuous homomorphism

$$\log : K^* \rightarrow K$$

such that $\log p = 0$ which on principal units $(1+x) \in U^{(1)}$ is given by the series

$$\log(1+x) = x - \frac{x^2}{2} + \frac{x^3}{3} - \dots$$

Proof: It's clear that \log is unique and by Proposition 2.3.1(4), \log is continuous.

It suffice to show \log is homomorphism. For $x \in \pi O_K$, we have

$$\sum_{n=1}^{\infty} x^n = \frac{1}{1-x}$$

Hence by Proposition 2.3.5, for all $\alpha \in \mathbb{Z}$,

$$(1+x)^\alpha = 1 + \sum_{k=1}^{\infty} \binom{\alpha}{k} x^k$$

Since

$$a_{n,k} = \frac{(-1)^{n-1}}{n} \binom{n}{k} x^k (1+y)^k y^{n-k} \rightarrow 0 \text{ as } n \rightarrow \infty$$

and

$$a_{n,k} = \frac{(-1)^{n-1}}{n} \binom{n}{k} x^k (1+y)^k y^{n-k} \rightarrow 0 \text{ as } k \rightarrow \infty \text{ uniformly,}$$

we have

$$\begin{aligned} \log((1+x)(1+y)) &= \sum_{n=1}^{\infty} (-1)^{n-1} \frac{(y + (1+y)x)^n}{n} \\ &= \sum_{n=1}^{\infty} \sum_{k=0}^n \frac{(-1)^{n-1}}{n} \binom{n}{k} x^k (1+y)^k y^{n-k} \\ &= \log(1+y) + \sum_{k=1}^{\infty} \sum_{n=k}^{\infty} \frac{(-1)^{n-1}}{n} \binom{n}{k} x^k (1+y)^k y^{n-k} \\ &= \log(1+y) + \log(1+x) \end{aligned}$$

Theorem 2.3.12. Let K/\mathbb{Q}_p be a p -adic number field with valuation ring O_K and maximal ideal πO_K , and let $pO_K = \pi^e O_K$. Then the power series

$$\exp(x) = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \cdots$$

and

$$\log(1+z) = z - \frac{z^2}{2} + \frac{z^3}{3} - \cdots$$

, yield, for $n > \frac{e}{p-1}$, two mutually inverse isomorphisms (and homeomorphisms)

$$(\mathfrak{p})^n \longleftrightarrow U^{(n)}.$$

Definition 2.3.13 (p-adic Interpolation). K is a p -adic field and $x \in U^{(1)}$, define

$$f : \mathbb{Z} \rightarrow K, n \mapsto x^n$$

Since f is uniformly continuous, by extension theorem, there's $\tilde{f} : \mathbb{Z}_p \rightarrow K$ extends f such that \tilde{f} is uniformly continuous.

Hence there's a natural \mathbb{Z}_p -module structure on $U^{(1)}$.

Proposition 2.3.14. Let K/\mathbb{Q}_p be a p -adic number field. For $1+x \in U^{(1)}$ and $z \in \mathbb{Z}_p$ one has

$$(1+x)^z = \sum_{\nu=0}^{\infty} \binom{z}{\nu} x^\nu$$

and series on the right hand converges even for $x \in \pi^n O_K$ where $n > \frac{e}{p-1}$.

Proposition 2.3.15. For $1 + x \in U^{(1)}$ and $z \in \mathbb{Z}_p$

$$(1 + x)^z = \exp(z \log(1 + x)) \text{ and } \log(1 + x)^z = z \log(1 + x)$$

Proof: It suffices to show the case when $z \in \mathbb{Z}$.

Chapter 3

Tate's Thesis

$F = \mathbb{R}, \mathbb{C}$ or finite extension of \mathbb{Q}_p . Denote the ring of integers by \mathcal{O}_F if F is a p-adic field. μ is the Haar measure we have already defined on F .

3.1 Local characters and Haar Measure

Definition 3.1.1. A $\chi \in \text{Hom}_{\text{cont}}(F^\times, \mathbb{C}^\times)$ is unramified if it is trivial on norm-one subgroup u of F . That is, χ is trivial on

$$u = \begin{cases} \{\pm 1\}, & F = \mathbb{R} \\ \mathbb{S}^1, & F = \mathbb{C} \\ \mathcal{O}_F^\times, & F \text{ be p-adic field} \end{cases}$$

It's obvious that all the quasi-character factor through

$$V(F) := \{y \in \mathbb{R}_+^\times : y = |x|_F, \text{ for some } x \in F^\times\} = \begin{cases} \mathbb{R}_{>0}^*, & F = \mathbb{R} \\ \mathbb{R}_{>0}^*, & F = \mathbb{C} \\ q^\mathbb{Z}, & F \text{ be p-adic field} \end{cases}$$

continuously. Hence we only need to classify quasi-character on $V(F)$.

Proposition 3.1.2. For every unramified quasi-character χ of F^\times there exists a complex number s such that $\chi(\alpha) = |\alpha|_F^s$ for $\alpha \in F^\times$.

Proof: Notice that $\mathbb{C} \rightarrow \mathbb{C}^*, z \mapsto \exp(z)$ is an universal covering. Hence every quasi-character on $\mathbb{R}_{>0}^*$ factors through \exp . By functional equation of log,

$$t \mapsto t^s, s \in \mathbb{C}$$

are all the unramified quasi-character on $\mathbb{R}_{>0}^*$.

Proposition 3.1.3. Every quasi-character χ of F^\times has the form

$$\chi(x) = \chi_0 |x|_F^s$$

where χ_0 is a (unitary) character of F^\times and $s \in \mathbb{C}$. The real part of s and the value of χ_0 on u are uniquely determined by the quasi-character, but the imaginary part of s is not. We denote by σ the real part of s and call it the exponent of χ .

Remark 3.1.4. We can visualize quasi-characters of F^\times as follow:

- (1) Let $F = \mathbb{R}$. A quasi-character of \mathbb{R}^\times is either of the form $|\cdot|^s$ or $\text{sgn}|\cdot|^s$.
- (2) Let $F = \mathbb{C}$. Every quasi-character of \mathbb{C}^\times takes the form

$$\chi_{s,n} : re^{i\theta} \mapsto r^s e^{in\theta}, s \in \mathbb{C}, n \in \mathbb{Z}$$

- (3) Let F be non-Archimedean and \mathfrak{p} be the unique prime ideal in F . There exists an $n \in \mathbb{N}$ such that $\chi_0(1 + \mathfrak{p}^n) = \{1\}$. For the smallest n with this property, we call \mathfrak{p}^n the conductor of χ_0 . If χ_0 is trivial ($n = 0$), then we say the conductor is $\mathfrak{p}^0 = \mathfrak{o}_F^\times$. Consequently, χ_0 is induced by a character on the finite group $\mathfrak{o}_F^\times / (1 + \mathfrak{p}^n)$.

In addition, if we fix π_F a generator \mathfrak{p} , we can find a unique unitary character χ_0 with $\chi_0(\pi_F) = 1$ and a unique $s \in \mathbb{C} / \frac{2\pi i}{\log q} \mathbb{Z}$ such that $\chi = \chi_0 |\cdot|^s$.

Definition 3.1.5. We will now construct the standard non-trivial additive characters for each of the local fields.

- (1) ($F = \mathbb{R}$). Let $\psi(x) = e^{-2\pi i x}$.
- (2) ($F = \mathbb{C}$). Set $\psi(x) = e^{-2\pi i \text{Tr}_{\mathbb{C}/\mathbb{R}}(x)}$.
- (3) (F non-Archimedean). First, we will define a non-trivial character on \mathbb{Q}_p . Recall that every $x \in \mathbb{Q}_p$ can be represented in the form

$$x = x_{-r}p^{-r} + x_{1-r}p^{1-r} + \cdots + x_{-1}p^{-1} + x_0 + x_1p + \cdots$$

Define $\lambda(x) = x_{-r}p^{-r} + x_{1-r}p^{1-r} + \cdots + x_{-1}p^{-1}$. Then ψ_p is defined to be

$$\psi_p : \mathbb{Q}_p \rightarrow S^1, x \mapsto e^{2\pi i \lambda(x)}.$$

Now, for finite extension F of \mathbb{Q}_p , we define $\psi(x) = \psi_p(\text{Tr}_{F/\mathbb{Q}_p}(x))$.

Proposition 3.1.6. The conductor of an additive-character of a non-Archimedean local field is defined to be \mathfrak{p}^m where \mathfrak{p} is the unique prime ideal of F and

$$m = \inf \left\{ r \in \mathbb{Z} : \psi|_{\mathfrak{p}^r} = 1 \right\}$$

Then \mathfrak{p}^{-m} is the different of F/\mathbb{Q}_p .

Proof:

$$\psi|_{\mathfrak{p}^m} \equiv 1 \text{ iff } \text{Tr}_{F/\mathbb{Q}_p}(\mathfrak{p}^m) \subset \mathbb{Z}_p \text{ iff } \mathfrak{p}^m \subset \text{inverse different}$$

Theorem 3.1.7. If ψ is a non-trivial character on F , for each $a \in F$, define $\psi_a : F \rightarrow \mathbb{S}^1$ by $\psi_a(x) = \psi(ax)$. Then the map $\alpha_\psi : F \rightarrow \hat{F}$ given by $a \mapsto \psi_a$ is a topological group isomorphism. For example,

$$\mathbb{R} \rightarrow \hat{\mathbb{R}}, a \mapsto (x \mapsto e^{-2\pi i a x})$$

and

$$\mathbb{C} \rightarrow \hat{\mathbb{C}}, a \mapsto (x \mapsto e^{-2\pi i \operatorname{Tr}_{\mathbb{C}/\mathbb{R}}(ax)})$$

are topological group isomorphisms.

Theorem 3.1.8. By Theorem 3.1.7, we can give a Haar measure on \hat{F} , and under this Haar measure, Fourier Inverse Theorem holds.

Proof: We only show the case when F is non-archimedean. Let $f(x)$ be the characteristic function of \mathfrak{o}_F . Let ψ be the standard non-trivial character. Then,

$$\hat{f}(y) = \int_F f(x)\psi(xy)dx = \int_{\mathfrak{o}_F} \psi(xy)dx$$

We see that for all $x \in \mathfrak{o}_F$, $\psi(xy) = 1$ if and only if $y \in \mathfrak{D}_F^{-1}$. Otherwise, if there's $a \in \mathfrak{o}_F$ such that $\psi(ay) \neq 1$, we have

$$\hat{f}(y) = \int_{\mathfrak{o}_F} \psi((x+a)y)dx = \psi(ay) \int_{\mathfrak{o}_F} \psi(xy)dx$$

Hence

$$\int_{\mathfrak{o}_F} \psi(xy)dx = 0$$

To sum up,

$$\hat{f}(y) = \chi_{\mathfrak{D}_F^{-1}}\mu(\mathfrak{o}_F)$$

Hence

$$\hat{\hat{f}}(x) = \int_{\mathfrak{D}_F^{-1}} N(\mathfrak{D}_F)^{-1/2} \chi(yx)dy = N(\mathfrak{D}_F)^{-1/2} \mu(\mathfrak{D}_F)\chi_{\mathfrak{o}_F}(x) = \chi_{\mathfrak{o}_F}(x)$$

Definition 3.1.9 (Haar measure on multiplicative group of F). Define a constant

$$c_F = \begin{cases} 1, & F = \mathbb{R}, \mathbb{C} \\ \frac{q}{q-1}, & F = \text{p-adic field} \end{cases}$$

If $E \in B_{F^\times}$, define

$$\mu(E) = c_F \int_{F-\{0\}} \chi_E \frac{dx}{|x|_F}$$

Since F^* is a open subspace of F , by Analysis 2.6.11, μ is a Haar measure on F^\times . We denote it by d^*x .

Then, there is a one-to-one correspondence of $L^1(F^\times)$ and $L^1(F - \{0\})$ given by $g(x) \mapsto g(x)|x|_F^{-1}$, and for these functions we have

$$\int_{F^\times} g(x)d^*x = c_F \int_{F-\{0\}} g(x) \frac{dx}{|x|_F}.$$

If F is non-archimedean, have

$$\text{Vol}(\mathfrak{o}_F^\times, d^*x) = \frac{q}{q-1} \int_{\mathfrak{o}_F^\times} dx = \text{Vol}(\mathfrak{o}_F, dx) - \text{Vol}(\pi_F \mathfrak{o}_F, dx) q/(q-1) = \text{Vol}(\mathfrak{o}_F, dx)$$

3.2 Fourier Transform

Definition 3.2.1 (Schwarz-Bruhat Function for F). Now we define Schwarz-Bruhat Function for F , recall $\mathcal{S}(\mathbb{R}^n)$ is the Schwartz space for n -dimension euclidean space.

$$S(F) = \begin{cases} \mathcal{S}(\mathbb{R}), & F = \mathbb{R} \\ \mathcal{S}(\mathbb{R}^2), & F = \mathbb{C} \\ \text{locally constant and compactly supported,} & F = \text{p-adic field} \end{cases}$$

Proposition 3.2.2. For every $f \in S(F)$, F non-Archimedean, there exist integers m and n , $-m \leq n$, such that $f(x) = 0$ for $x \notin \mathfrak{p}^{-m}$, and for $x \in \mathfrak{p}^{-m}$, $f(y) = f(x)$ for all $y \in x + \mathfrak{p}^n$.

Lemma 3.2.3. Assume F is non-archimedean. The local Fourier transform of $f = 1_{a+\mathfrak{p}^\ell}$, the characteristic function of the set $a + \mathfrak{p}^\ell$, is

$$\hat{f}(y) = \psi(ay) N(\mathfrak{D}_F)^{-\frac{1}{2}} N(\mathfrak{p})^{-\ell} 1_{\mathfrak{p}^{-\ell} \mathfrak{D}_F^{-1}}(y)$$

Corollary 3.2.4. By Lemma 3.2.3, and Proposition 3.1.6, Fourier Transform gives a linear isomorphism between $S(F)$.

Definition 3.2.5 (local L-function). Let $\chi \in \text{Hom}_{\text{cont}}(F^\times, \mathbb{C}^\times)$.

(1) If $F = \mathbb{C}$, then let

$$L(\chi_{s,n}) = \Gamma_{\mathbb{C}}\left(s + \frac{|n|}{2}\right) = (2\pi)^{-(s + \frac{|n|}{2})} \Gamma\left(s + \frac{|n|}{2}\right)$$

(2) If $F = \mathbb{R}$ and $\chi = |\cdot|^s$ or $\chi = \text{sgn}|\cdot|^s$, then let

$$L(\chi) = \begin{cases} \Gamma_{\mathbb{R}}(s) = \pi^{-s/2} \Gamma(s/2) & \text{if } \chi = |\cdot|^s \\ \Gamma_{\mathbb{R}}(s+1) & \text{if } \chi = \text{sgn}|\cdot|^s \end{cases}$$

(3) If F is non-Archimedean, then let

$$L(\chi) = \begin{cases} (1 - \chi(\pi_F))^{-1} & \text{if } \chi \text{ is unramified} \\ 1 & \text{otherwise} \end{cases}$$

Then $L(\chi)$ be a meromorphic function on \mathbb{C} .

Proposition 3.2.6. Given any quasi-character χ of F^\times and a complex number s , the product $\chi| \cdot |_F^s$ is also a character. And we write $L(s, \chi)$ for $L(\chi| \cdot |_F^s)$. We define the shifted dual of χ to be

$$\check{\chi} = \chi^{-1}| \cdot |_F$$

so that

$$L((\chi| \cdot |_F^s)^\vee) = L(1 - s, \chi^{-1})$$

Definition 3.2.7 (local zeta function). For $f \in S(F)$ and $\chi \in \text{Hom}_{\text{cont}}(F^\times, \mathbb{C}^\times)$, we define the associated local zeta function to be

$$Z(f, \chi) = \int_{F^\times} f(x) \chi(x) d^*x$$

Note that $Z(f, \chi)$ is dependent on the multiplicative measure d^*x . If we fix an additive measure dx and choose $d^*x = c_F dx / |x|_F$, then $Z(f, \chi)$ is dependent on dx .

Lemma 3.2.8 (Gauss sum). Assume F is non-archimedean. Given characters $\omega : \mathcal{O}_F^\times \rightarrow \mathbb{C}^\times$ and $\psi : \mathcal{O}_F \rightarrow \mathbb{C}^\times$, define the Gauss sum

$$g(\omega, \psi) := \int_{\mathcal{O}_F^\times} \omega(x) \psi(x) d^\times x.$$

Suppose ω is of conductor \mathfrak{p}^n with $n > 0$, and ψ is of conductor \mathfrak{p}^m with $m \geq 0$.

(1) If $m \neq n$, then $g(\omega, \psi) = 0$.

(2) If $m = n$, then $|g(\omega, \psi)|^2 = c_F^2 q^{-m} \text{Vol}(\mathcal{O}_F, dx)^2$.

Proof: (1): If $m > n$, then the integral over each coset of $1 + \mathfrak{p}^n$ is 0 since ω is constant and ψ is a nontrivial character on \mathfrak{p}^n . If $m < n$, then the integral over each coset of $1 + \mathfrak{p}^m$ is 0 since ψ is constant and ω is a nontrivial character on $1 + \mathfrak{p}^m$.

(2): If $m = n > 0$, then

$$\begin{aligned} |g(\omega, \psi)|^2 &= \int_{\mathcal{O}_F^\times} \omega(x) \psi(x) d^\times x \overline{\int_{\mathcal{O}_F^\times} \omega(y) \psi(y) d^\times y} \\ &= \int_{\mathcal{O}_F^\times} \int_{\mathcal{O}_F^\times} \omega(xy^{-1}) \psi(x - y) d^\times x d^\times y \\ &= \int_{\mathcal{O}_F^\times} \int_{\mathcal{O}_F^\times} \omega(z) \psi(yz - y) d^\times y d^\times z \\ &= \int_{\mathcal{O}_F^\times} \omega(z) h(z) d^\times z \end{aligned}$$

where

$$\begin{aligned}
h(z) &= \int_{\mathcal{O}_F^\times} \psi(yz - y) d^\times y \\
&= \int_{\mathcal{O}_F^\times} \psi(y(z - 1)) dy \quad (\text{since } |y| = 1 \text{ on } \mathcal{O}_F^\times) \\
&= c_F \int_{\mathcal{O}_F} \psi(y(z - 1)) dy - c_F \int_{1+\mathfrak{p}} \psi(y(z - 1)) dy \\
&= c_F \times \text{Vol}(\mathcal{O}_F, dx) \times \begin{cases} 1 - q^{-1} & \text{if } v(z - 1) \geq m \quad (\text{both integrands are 1}) \\ -q^{-1} & \text{if } v(z - 1) = m - 1 \quad (\text{second integrand is 1}) \\ 0 & \text{if } v(z - 1) < m - 1 \quad (\text{neither integrand is constant}) \end{cases}
\end{aligned}$$

Thus

$$|g(\omega, \psi)|^2 = c_F \times \text{Vol}(\mathcal{O}_F, dx) \left(\int_{1+\mathfrak{p}^m} \omega(z) d^\times z - q^{-1} \int_{1+\mathfrak{p}^{m-1}} \omega(z) d^\times z \right) = c_F^2 q^{-m} \text{Vol}(\mathcal{O}_F, dx)^2$$

Proposition 3.2.9. Let $f \in S(F)$, and $\chi = \chi_0 |\cdot|^s$ where χ_0 is the unitary part of the quasicharacter χ . Let $\sigma = \Re(s)$. Then the following statements hold:

- (1) $Z(f, \chi)$ is holomorphic and absolutely convergent if $\sigma > 0$.
- (2) There exists a nonvanishing holomorphic function $\epsilon(\chi, \psi, dx)$ such that

$$\frac{Z(\hat{f}, \chi^\vee)}{L(\chi^\vee)} = \epsilon(\chi, \psi, dx) \frac{Z(f, \chi)}{L(\chi)}$$

for all $f \in S(F)$. Hence $Z(f, \chi)$ has a meromorphic continuation to the whole complex plane.

Proof: (1): Since $f \in S(F)$, f factors through the finite quotient group $\mathfrak{p}^{-m}/\mathfrak{p}^n, m, n \in \mathbb{Z}, -m \leq n$. Hence, we only need to consider $f = \chi_{\mathfrak{p}^n}$. Let π_F be a uniformizing parameter of \mathfrak{p} . From

$$\pi_F^n \mathfrak{o}_F - \{0\} = \bigcup_n \pi_F^k \mathfrak{o}_F^\times$$

and the translation invariance of the multiplicative measure, it follows that

$$\begin{aligned}
|Z(f, \chi)| &\leq c_F \int_{F-\{0\}} |f(x)| |x|_F^{\sigma-1} dx = c_F \int_{F-\{0\}} \chi(\pi_F^n) |x|_F^{\sigma-1} dx = \sum_{k=n}^{\infty} \int_{\pi_F^k \mathfrak{o}_F^\times} |x|_F^{\sigma} d^*x = \\
&= \sum_{k=n}^{\infty} \int_{\mathfrak{o}_F^\times} |\pi_F^k x|_F^{\sigma} d^*x = \sum_{k=n}^{\infty} q^{-k\sigma} \int_{\mathfrak{o}_F^\times} d^*x = \frac{q^{-n\sigma}}{1 - q^{-\sigma}} \text{Vol}(\mathfrak{o}_F, dx)
\end{aligned}$$

- (2): Choose dx, ψ to be standard Haar measure and additive character on F , we have:

(a): If $F = \mathbb{R}$, $\chi = |\cdot|^s$, take $f = e^{-\pi x^2}$, we have

$$Z(f, \chi) = L(\chi), Z(\hat{f}, \chi^\vee) = L(\chi^\vee)$$

Hence, $\epsilon = 1$.

(b): If $F = \mathbb{R}$, $\chi = \text{sgn} \cdot |\cdot|^s$, take $f = xe^{-\pi x^2}$, we have

$$Z(f, \chi) = L(\chi), Z(\hat{f}, \chi^\vee) = -iL(\chi^\vee)$$

Hence, $\epsilon = -i$.

(c): If $F = \mathbb{C}$, $\chi = \chi_{s,n}$, take

$$f_n(z) = \begin{cases} (2\pi)^{-1} \bar{z}^{|n|} e^{-2\pi z \bar{z}} & \text{for } n \geq 0 \\ (2\pi)^{-1} z^{|n|} e^{-2\pi z \bar{z}} & \text{for } n < 0 \end{cases}$$

, we have $\hat{f}_n = (-i)^{|n|} f_{-n}$ and

$$Z(f_n, \chi_{s,n}) = L(\chi_{s,n}), Z(\hat{f}_n, \chi^\vee) = (-i)^{|n|} L(\chi^\vee) = (-i)^{|n|} L(\chi_{-n,1-s})$$

Hence, $\epsilon = (-i)^{|n|}$.

(d): If F is non-archimedean and $\chi = \chi_{s,n} = \chi_0 |\cdot|^s$ with $\mathfrak{p}^n, n \geq 1$ to be the conductor of χ_0 . Fix a uniformizer π_F , assume $\mathfrak{p}^{-d}, d \geq 0$ be the conductor of ψ and $\chi_0(\pi_F) = 1$. Define

$$f_n(x) = \psi(x) \mathbf{1}_{\mathfrak{p}^{-d-n}}(x)$$

If χ is unramified, i.e χ_0 is trivial, we have

$$\begin{aligned} Z(f_0, \chi_{s,0}) &= \int_{F^\times} f_0(x) \chi_{s,0}(x) d^*x = \int_{\pi_F^{-d} - \{0\}} |x|_F^s d^*x = \\ &= \sum_{k=-d}^{\infty} |x|_F^s d^*x = \sum_{k=-d}^{\infty} q^{-ks} \text{Vol}(\mathfrak{o}_F^\times, d^*x) = \\ &= \text{Vol}(\mathfrak{o}_F^\times, d^*x) \frac{q^{ds}}{1 - q^{-s}} = q^{ds} \text{Vol}(\mathfrak{o}_F^\times, d^*x) (1 - |\pi_F|_F^s)^{-1} = \\ &= q^{ds} \text{Vol}(\mathfrak{o}_F, dx) L(\chi_{s,0}) \end{aligned}$$

(e): If χ is ramified, i.e. $n \geq 1$, we have

$$\begin{aligned} Z(f_n, \chi_{s,n}) &= \int_{F^\times} f_n(x) \chi_{s,n}(x) d^*x = \int_{\pi_F^{-d-n} \mathfrak{o}_F - \{0\}} \psi(x) \chi_0(x) |x|_F^s d^*x = \\ &= \sum_{k=-d-n}^{\infty} \int_{\mathfrak{o}_F^\times} \psi(\pi_F^k u) \chi_0(u) |\pi_F^k u|_F^s d^*u = \sum_{k=-d-n}^{-d} q^{-ks} \int_{\mathfrak{o}_F^\times} \psi(\pi_F^k u) \chi_0(u) d^*u \end{aligned}$$

By Proposition 3.2.8, $Z(f_n, \chi_{s,n}) = q^{(-d-n)s} g(\chi_0, \psi_{\pi_F^{-d-n}})$.

Now we want to calculate the Fourier Transform of f_n . Notice that for $n = 0$, we have $\hat{f}_0(y) = \text{Vol}(\mathfrak{p}^{-d}, dx) \mathbf{1}_{\mathfrak{o}_F}(y)$, where $\mathbf{1}_{\mathfrak{o}_F}(y)$ is the characteristic function of \mathfrak{o}_F . For $n > 0$ we have $\hat{f}_n(y) = \text{Vol}(\mathfrak{p}^{-d-n}, dx) \mathbf{1}_{\mathfrak{p}^{n-1}}(y)$, where $\mathbf{1}_{\mathfrak{p}^{n-1}}(y)$ is the characteristic function of $\mathfrak{p}^n - 1$.

Hence,

$$Z(\hat{f}_0, \chi_{s,0}^\vee) = q^d \text{Vol}(\mathfrak{D}_F, dx)^2 L(\chi_{s,0}^\vee)$$

and

$$\epsilon(\chi_{s,0}, \psi, dx) = q^{-d(s-1)} \text{Vol}(\mathfrak{o}_F, dx)$$

If $n \geq 1$, we have

$$Z(\hat{f}_n, \chi_{s,n}^\vee) = c_F q^d \text{Vol}(\mathfrak{o}_F, dx)^2 \chi_0(-1) L(\chi_{s,n}^\vee)$$

and

$$\epsilon(\chi_{s,n}, \psi, dx) = \frac{c_F q^d q^{-(d+n)s} \text{Vol}^2(\mathfrak{o}_F, dx) \chi_0(-1)}{g(\chi_0, \psi_{\pi_F^{-d-n}})}$$

where the conductor of characters in the p-adic Gauss sum are all \mathfrak{p}^n .

Corollary 3.2.10. If we choose standard non-trivial character (then conductor = inverse different), self-dual measure ($\text{Vol}(\mathcal{O}_F, dx) = q^{-d/2}$) and $s = 1/2$, $|\epsilon(\chi)| = 1$.

Theorem 3.2.11. For all idele-class characters $\chi = \chi_0 |\cdot|^s$ and $f \in S(\mathbb{A}_K)$, the global zeta function $Z(f, \chi)$ is uniformly convergent in every compact subset of $\sigma = \Re(s) > 1$, hence holomorphic in $\sigma = \Re(s) > 1$. Furthermore, $Z(f, \chi)$ extends to a meromorphic function of s and satisfies the functional equation

$$Z(f, \chi) = Z(\hat{f}, \chi^\vee)$$

For $\chi = \chi_0 |\cdot|^s$, if χ_0 is non-trivial, the continuation of $Z(f, \chi)$ is entire. If χ_0 is trivial, the continuation of $Z(f, \chi)$ has simple poles at $s = 0$ and $s = 1$, with corresponding residues given by

$$-\text{Vol}(C_K^1) f(0) \quad \text{and} \quad \text{Vol}(C_K^1) \hat{f}(0)$$

respectively. The volume of C_K^1 is taken with respect to the quotient measure on C_K defined by both d^*x and the counting measure on K^* .

Proof: If we fix an infinite place of K , then $\mathbb{I}_K \simeq \mathbb{R}_+^\times \times \mathbb{I}_K^1$. Haar measure on $\mathbb{I}_K/\mathbb{I}_K^1 \cong \mathbb{R}_{>0}^\times$ is defined to be dt/t , then there's unique Haar measure on \mathbb{I}_K^1 such that Theorem 2.1.38 holds for $G = \mathbb{I}_K$ and $H = \mathbb{I}_K^1$. And we also denote this Haar measure on \mathbb{I}_K^1 by d^*x .

Hence for $\sigma > 1$ and $f \in S(\mathbb{A}_K)$,

$$Z(f, \chi) = \int_{\mathbb{I}_K} f(x) \chi(x) d^*x = \int_0^\infty \int_{\mathbb{I}_K^1} f(tx) \chi(tx) d^*x \frac{dt}{t}$$

Define

$$Z_t(f, \chi) = \int_{\mathbb{I}_K^1} f(tx) \chi(tx) d^*x$$

We will now apply Poisson Summation Formula to establish a functional equation for $Z_t(f, \chi)$.

We claim that The function $Z_t(f, \chi)$ satisfies the relation

$$Z_t(f, \chi) = Z_{t^{-1}}(\hat{f}, \chi^\vee) + \hat{f}(0) \int_{C_K^1} \check{\chi}(x/t) d^*x - f(0) \int_{C_K^1} \chi(tx) d^*x$$

Now we give a proof of the proposition. Fix a Haar measure on \mathbb{I}^1/K^* such that Theorem 2.1.38 holds for counting measure on K^* . Then

$$Z_t(f, \chi) = \int_{C_K^1} \left(\sum_{a \in K^*} f(atx) \chi(atx) \right) d^*x = \int_{C_K^1} \left(\sum_{a \in K^*} f(atx) \right) \chi(tx) d^*x$$

since $\chi|_{K^*} = 1$, by hypothesis. To apply the Poisson Summation Formula, we need to sum over K , not K^* . In order to do this, we add $f(0) \int_{C_K^1} \chi(tx) d^*x$ to $Z_t(f, \chi)$. That is,

$$Z_t(f, \chi) + f(0) \int_{C_K^1} \chi(tx) d^*x = \int_{C_K^1} \left(\sum_{a \in K} f(atx) \right) \chi(tx) d^*x$$

Applying the Poisson Summation Formula to the sum on the right-hand side and then using the change of variable $x \mapsto x^{-1}$, we obtain

$$\begin{aligned} \int_{C_K^1} \left(\sum_{a \in K} f(atx) \right) \chi(tx) d^*x &= \int_{C_K^1} \left(\sum_{a \in K} \hat{f}(at^{-1}x^{-1}) \right) \frac{\chi(tx)}{|tx|_{\mathbb{I}_K}} d^*x \\ &= \int_{C_K^1} \left(\sum_{a \in K} \hat{f}(at^{-1}x) \right) |t^{-1}x|_{\mathbb{I}_K} \chi(tx^{-1}) d^*x \\ &= \int_{C_K^1} \left(\sum_{a \in K^*} \hat{f}(at^{-1}x) \right) \check{\chi}(x/t) d^*x + \hat{f}(0) \int_{C_K^1} \check{\chi}(x/t) d^*x \\ &= Z_{t^{-1}}(\hat{f}, \check{\chi}) + \hat{f}(0) \int_{C_K^1} \check{\chi}(x/t) d^*x \end{aligned}$$

We may break up $Z(f, \chi)$ as follows:

$$Z(f, \chi) = \int_0^1 Z_t(f, \chi) \frac{1}{t} dt + \int_1^\infty Z_t(f, \chi) \frac{1}{t} dt$$

We see that

$$\int_1^\infty Z_t(f, \chi) \frac{1}{t} dt = \int_{\{x \in \mathbb{I}_K : |x|_{\mathbb{I}_K} \geq 1\}} f(x) \chi(x) d^*x$$

The integral on the right-hand side is uniformly convergent on every compact subset of \mathbb{C} . This is because, f_ν are supported on a compact subset for all finite place ν and $|f_\nu|$ decrease rapidly for all infinite place ν . Hence, $\int_1^\infty Z_t(f, \chi)$ is an entire function.

$$\int_0^1 Z_t(f, \chi) \frac{1}{t} dt = \int_0^1 \left(Z_{t^{-1}}(\hat{f}, \check{\chi}) + \hat{f}(0) \check{\chi}(t^{-1}) \int_{C_K^1} \check{\chi}(x) d^*x - f(0) \chi(t) \int_{C_K^1} \chi(x) d^*x \right) \frac{1}{t} dt$$

Applying the change of variable $t \mapsto t^{-1}$ to the first integral in the sum, we obtain

$$\int_0^1 Z_{t^{-1}}(\hat{f}, \check{\chi}) \frac{1}{t} dt = \int_1^\infty Z_t(\hat{f}, \check{\chi}) \frac{1}{t} dt$$

$$R(f, \chi) := \int_0^1 \hat{f}(0) \check{\chi}(t^{-1}) \int_{C_K^1} \check{\chi}(x) d^*x \frac{1}{t} dt - \int_0^1 f(0) \chi(t) \int_{C_K^1} \chi(x) d^*x \frac{1}{t} dt$$

There are two cases to consider.

Firstly, if χ is nontrivial on \mathbb{I}_K^1 , then

$$\int_{C_K^1} \check{\chi}(x) d^*x \text{ and } \int_{C_K^1} \chi(x) d^*x$$

are both zero by orthogonality of characters ($R(f, \chi) = 0$). Therefore,

$$\int_0^1 Z_t(f, \chi) \frac{1}{t} dt = \int_1^\infty Z_t(\hat{f}, \check{\chi}) \frac{1}{t} dt$$

, and hence

$$Z(f, \chi) = \int_1^\infty Z_t(f, \chi) \frac{1}{t} dt + \int_1^\infty Z_t(\hat{f}, \check{\chi}) \frac{1}{t} dt$$

So, when χ is nontrivial on \mathbb{I}_K^1 , then $Z(f, \chi)$ extends to an entire function.

Secondly, if $\chi = |\cdot|^s$ is trivial on \mathbb{I}_K^1 , then

$$\begin{aligned} R(f, \chi) &= \hat{f}(0) \text{Vol}(C_K^1) \int_0^1 t^{s-2} dt - f(0) \text{Vol}(C_K^1) \int_0^1 t^{s-1} dt \\ &= \frac{\hat{f}(0) \text{Vol}(C_K^1)}{s-1} - \frac{f(0) \text{Vol}(C_K^1)}{s} \end{aligned}$$

Consequently,

$$\int_0^1 Z_t(f, \chi) \frac{1}{t} dt = \int_1^\infty Z_t(\hat{f}, \check{\chi}) \frac{1}{t} dt + \frac{\hat{f}(0) \text{Vol}(C_K^1)}{s-1} - \frac{f(0) \text{Vol}(C_K^1)}{s}$$

, and hence

$$Z(f, \chi) = \int_1^\infty Z_t(f, \chi) \frac{1}{t} dt + \int_1^\infty Z_t(\hat{f}, \check{\chi}) \frac{1}{t} dt + \frac{\hat{f}(0) \text{Vol}(C_K^1)}{s-1} - \frac{f(0) \text{Vol}(C_K^1)}{s}$$

Definition 3.2.12. We define the global L-function of χ in terms of its local versions by the product expansion

$$L(\chi) = \prod_{\nu} L(\chi_{\nu})$$

It's clear that $L(\chi)$ uniformly converges on all compact subsets of $\text{Re}(s) > 1$ and holomorphic in $\text{Re}(s) > 1$

Definition 3.2.13 (Hecke L-function). Let $\chi \in \text{Hom}_{\text{cont}}(\mathbb{I}_K/K^*, \mathbb{C}^\times)$ (an idele-class character). For complex s , define the Hecke L-function $L(s, \chi)$ by

$$L(s, \chi) = L(\chi | \cdot|^s)$$

Let $\chi \in \text{Hom}_{\text{cont}}(\mathbb{I}_K/K^*, \mathbb{C}^\times)$ (an idele-class character). For complex s , define the Hecke L-function $L(s, \chi)$ by

$$L(s, \chi) = L(\chi | \cdot|^s)$$

If $\chi = \otimes' \chi_\nu$, define

$$L(s, \chi_f) = \prod_{\nu \text{ finite}} L(s, \chi_\nu)$$

and

$$L(s, \chi_\infty) = \prod_{\nu|\infty} L(s, \chi_\nu)$$

respectively. Then

$$L(s, \chi) = L(s, \chi_f) L(s, \chi_\infty)$$

Example 3.2.14. For χ equals to identity character 1 on $\text{Hom}_{\text{cont}}(\mathbb{I}_K/K^*, \mathbb{C}^\times)$, we have

$$L(s, 1_f) = \prod_{\nu \text{ finite}} \frac{1}{1 - |\pi_\nu|^s} = \zeta_K(s)$$

which is so-call Dedekind zeta-function.

For a Dirchlet character $\chi : \mathbb{I}_\mathbb{Q} \xrightarrow{\pi} \widehat{\mathbb{Z}}^\times \xrightarrow{\chi_1} \mathbb{S}^1$, if χ correspondes to χ_0 , a primitive Dirchlet character module m , where $m = p_1^{e_1} \dots p_s^{e_s}$, we have

$$L(s, \chi_f) = \prod_{p \nmid m} \frac{1}{1 - \chi_p(p)p^{-s}} = \prod_{p \nmid m} \frac{1}{1 - \chi_0^{-1}(p)p^{-s}}$$

Theorem 3.2.15.

$$\text{Vol}(C_K^1) = \frac{2^{r_1}(2\pi)^{r_2} h_K R_K}{\omega_K \sqrt{|d_K|}}$$

Theorem 3.2.16. Let χ be a unitary idele-class character with factorization $\chi = \prod_\nu \chi_\nu$. ψ_ν be the standard unitary character on K_ν , then $\psi = \prod_\nu \psi_\nu$ be a non-trivial adelic character that is trivial on K . Then $L(s, \chi)$, which is holomorphic in $\{s \in \mathbb{C} : \Re(s) > 1\}$, admits a meromorphic continuation to the whole complex plane, and satisfies the functional equation

$$L(1-s, \chi^{-1}) = \epsilon(s, \chi) L(s, \chi)$$

where

$$\epsilon(s, \chi) = \prod_\nu \epsilon(\chi_\nu | \cdot |^s, \psi_\nu, dx_\nu) \in \mathbb{C}^\times$$

Furthermore, if χ is ramified, $L(s, \chi)$ is entire. If χ unramified, $L(s, \chi)$ is a meromorphic function with simple poles at 0 and 1. And residue at 0 and 1 are

$$-|d_K|^{1/2} (2\pi)^{-r_2} \text{Vol}(C_K^1), \quad (2\pi)^{-r_2} \text{Vol}(C_K^1)$$

respectively.

Hence, Dedekind zeta function $\zeta_K(s)$ can be extended to a meromorphic function with only simple pole at $s = 1$ with residue

$$\text{Vol}(C_K^1) = \frac{2^{r_1}(2\pi)^{r_2} h_K R_K}{\omega_K \sqrt{|d_K|}}$$

and the order of zeros at $s = 0$ equals to rank of unit group, that is $r_1 + r_2 - 1$.

Proof: Dedekind zeta function: Take f_ν for all ν as the form in Theorem 3.2.9, we have

$$Z(f, |\cdot|^s) = \prod_{\nu} \int_{K_{\nu}} Z(f_{\nu}, |\cdot|^s) = L(s, 1) |d_K|^{s-1/2}$$

Notice that

$$f(0) = (2\pi)^{-r_2} \quad \hat{f}(0) = (2\pi)^{-r_2} |d_K|^{1/2}$$

Hence, the residues at 0 and 1 for Hecke L-function $L(s, |\cdot|^s)$ are

$$-|d_K|^{1/2} (2\pi)^{-r_2} \text{Vol}(C_K^1), \quad (2\pi)^{-r_2} \text{Vol}(C_K^1)$$

Since

$$\zeta_K(s) \prod_{\nu \text{ infinite}} L(|\cdot|^s) |d_K|^{s-1/2} = Z(f, |\cdot|^s)$$

and Gamma function has simple pole at $s = 1$, the order of zero of $\zeta_K(s)$ at $s = 0$ is $r_1 + r_2 - 1$.

Moreover, the residue of $\zeta_K(s)$ at $s = 1$ is $\text{Vol}(C_K^1)$ because $\Gamma(1) = 1, \Gamma(1/2) = \sqrt{\pi}$.

To obtain functional equation, notice that

$$L(1-s, 1) = Z(\hat{f}, |\cdot|^{1-s}) = Z(f, |\cdot|^s) = \prod_{\nu} \int_{K_{\nu}} Z(f_{\nu}, |\cdot|^s) = L(s, 1) |d_K|^{s-1/2}$$

Hence,

$$|d_K|^{s/2} L(s, 1) = L(1-s, 1) |d_K|^{(1-s)/2}$$

Corollary 3.2.17. For an arbitrary unitary idèle class character $\chi_0 = \otimes'_{\nu} \chi_{\nu}$, define

$$C_{\chi_0} = \prod_{\nu \text{ finite}} q_{\nu}^{n_{\nu}}$$

where $\mathfrak{p}_{\nu}^{n_{\nu}}$ be the conductor of χ_{ν} . Then

$$L(s, \chi_0) (|d_K| C_{\chi_0})^{s/2} = CL(1-s, \chi_0^{-1}) (|d_K| C_{\chi_0})^{(1-s)/2}$$

for some C with $|C| = 1$.