Number Theory

Erzhuo Wang

January 20, 2025

Contents

Chapter 1

Global Field

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

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

of the K-vector space L :

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

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

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

is a basis of L/K.

Proposition 1.1.4. If L/K is a finite separable extension and $\sigma : L \to \bar{K}$ 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) $\mathrm{Tr}_{L|K}(x) = \sum_\sigma \sigma x$,

(3) $N_{L|K}(x) = \prod_\sigma \sigma x$.

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

$$d\left(\alpha_1, \ldots, \alpha_n\right) = \det\left(\left(\sigma_i \alpha_j\right)\right)^2$$

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

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

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

$$d\left(\alpha_1, \ldots, \alpha_n\right) = \det\left(\mathrm{Tr}_{L|K}\left(\alpha_i \alpha_j\right)\right).$$

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

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

where $\theta_i = \sigma_i \theta$.

Remark 1.1.6. Consider a finite separable extenison L/K, $(x, y) = \mathrm{Tr}_{L/K}(xy)$ 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 $\{\alpha_1, \ldots, \alpha_n\}$,

$$d\left(\alpha_1, \ldots, \alpha_n\right) \neq 0$$

Lemma 1.1.7. Let $\alpha_1, \ldots, \alpha_n$ be a basis of L/K which is contained in $\mathcal{O}_L$, of discriminant $d = d\left(\alpha_1, \ldots, \alpha_n\right)$. Then one has

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

More generally, if O_K be an integral domain, K be its fraction field,L/K be a separable extension and 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

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

Definition 1.1.8 (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 $\omega_1, \omega_2, \ldots, \omega_n$ for $K/\mathbb{Q}$ such that $w_i, i = 1, \ldots, n \in \mathcal{O}_K$ 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 O_K as free abelian group integral basis of $\mathcal{O}_K$

Definition 1.1.9 (discriminant of number field)**.** Define $d_K = d(\omega_1, \omega_2, \ldots, \omega_n)$, where $\omega_1, \ldots, \omega_n$ is an integral basis of $\mathcal{O}_K$.

Proposition 1.1.10. Let $L/\mathbb{Q}$ and $L'/\mathbb{Q}$ be two Galois extensions of degree n, resp. n', such that $L \cap L' = K$. Let $\omega_1, \ldots, \omega_n$, resp. $\omega_1', \ldots, \omega_{n'}'$, be an integral basis of $L \mid \mathbb{Q}$, resp. $L' \mid \mathbb{Q}$, 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 1.1.11. 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

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

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

Theorem 1.1.12. 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 $\mathbb{Q}(\theta)/\mathbb{Q}$,

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

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

Proposition 1.1.13. 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 $y \in \mathfrak{p}, y \neq 0$, 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 $a_n \in \mathfrak{p} \cap \mathbb{Z}$. The integral domain $\overline{\mathcal{O}} = \mathcal{O}_K/\mathfrak{p}$ is a field also follows from above equation.

Proposition 1.1.14. K is a algebraic number field. For a non-zero ideal $\mathfrak{A}$ of $\mathcal{O}_K$, define $\mathfrak{N}(\mathfrak{A}) = |\mathcal{O}_K/\mathfrak{A}|$

(1)

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

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

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

Definition 1.1.15 (relative norm)**.** Assume L/K be an extension of number field, and $\mathfrak{P}$ be a prime ideal in $\mathcal{O}_L$ and $\mathfrak{p}=\mathfrak{P}\cap\mathcal{O}_K$, define

$$N_{L/K}(\mathfrak{P})=(\mathfrak{p})^{[\mathcal{O}_L/\mathfrak{P}:\mathcal{O}_K/\mathfrak{p}]}$$

and for non-zero ideal of $\mathcal{O}_K$ in general, $N_{L/K}$ is defined by unqiue factorization.

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 $v_1,\ldots,v_m$ of V. The m-tuple $(v_1,\ldots,v_m)$ 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 $e_1,\ldots,e_n$ has volume 1 , and more generally, the parallelepiped spanned by n linearly independent vectors $v_1,\ldots,v_n$,

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

has volume

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

where $A=(a_{ij})$ is the unique matrix satisfying

$$[v_1,\ldots,v_n]=A[e_1,\ldots,e_n]$$

Proposition 1.2.3.

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

Definition 1.2.4. Let Γ be the lattice spanned by $v_1,\ldots,v_n$. Then Φ is a fundamental mesh of Γ, and we write for short

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

Theorem 1.2.5 (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

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

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

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

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

Example 1.2.6 (Minkowski's Theorem on Linear Forms)**.** Let

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

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

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

Definition 1.2.7 (Minkowski space)**.** Minkowski space $K_{\mathbb{R}}$ can be given in the following manner. Some of the embeddings $\tau : K \to \mathbb{C}$ are real in that they land already in $\mathbb{R}$, and others are complex, i.e., not real. Let

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

be the real embeddings. The complex ones come in pairs

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

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

$$f : K \to K_{\mathbb{R}} \quad x \mapsto (\rho_1(x), \ldots, \rho_{r_1}(x), \sigma_1(x), \bar{\sigma}_1(x), \ldots, \sigma_s(x), \bar{\sigma}_s(x))$$

Definition 1.2.8. $K_{\mathbb{C}}$ 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 $K_{\mathbb{R}} \times K_{\mathbb{R}} \to \mathbb{R}$.

Proposition 1.2.9. 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

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

Remark 1.2.10. Consider n-dimensional vector space $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ with a linear isomorphism

$$K_{\mathbb{R}} \to \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}, (x_1, \ldots, x_{r_1}, z_1, \overline{z_1}, \ldots, z_{r_2}, \overline{z_{r_2}}) \mapsto (x_1, \ldots, x_{r_1}, z_1, \ldots, z_{r_2})$$

Define Haar measure on $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ by product measure of Lebesgue measure on $\mathbb{R}$ and twice of Lebesgue measure on $\mathbb{C}$. Notice that above isomorphism preserves Haar measure: consider

$$[\alpha_1, \ldots, \alpha_{r_1}, \beta_1, \ldots, \beta_{r_2}] = \begin{vmatrix} 1 & & & & & \\ & \ddots & & & & \\ & & 1 & & & \\ & & & 1 & i & \\ & & & 1 & -i & \\ & & & & & \ddots \end{vmatrix}$$

We have the volume of fundamental domain generated by $[\alpha, \ldots, \alpha_{r_1}, \beta_1, \ldots, \beta_{r_2}]$ is 2^{r_2}. Meanwhile, the image of the fundamental domain in $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ has volume 2^{r_2}.

Proposition 1.2.11. Let $\mathfrak{a} \neq 0$ be an integral ideal of K, and let $c_\tau > 0$, for $\tau \in \operatorname{Hom}(K, \mathbb{C})$, be real numbers such that $c_\tau = c_{\bar{\tau}}$ and

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

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

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

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

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

given by $x_\rho = z_\rho, x_\sigma = \operatorname{Re}(z_\sigma), x_{\bar{\sigma}} = \operatorname{Im}(z_\sigma)$. 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

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

Lemma 1.2.12. In Minkowski space $K_{\mathbb{R}}$, the domain

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

has volume

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

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

$$x_1 + \cdots + x_r + w_1 + \cdots + w_s \leq t$$

$$\begin{aligned} I_{r,s}(1) &= \int_0^1 I_{r-1,s}\left(1 - x_1\right) dx_1 = \int_0^1 \left(1 - x_1\right)^{n-1} dx_1 \cdot I_{r-1,s}(1) \\ &= \frac{1}{n} I_{r-1,s}(1) \end{aligned}$$

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

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

and, doing the integration, induction shows that

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

Proposition 1.2.13. Show that in every ideal $\mathfrak{a} \neq 0$ of $\mathcal{O}_K$, there exists an $a \neq 0$ such that

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

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 1.2.12.

Remark 1.2.14. 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

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

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

Proposition 1.2.15. 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.

Corollary 1.2.16. 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 1.2.17. The $\mathbb{R}$-vector space $[\prod_\tau \mathbb{R}]^+$is explicitly given as follows. Separate as before the embeddings $\tau : K \to \mathbb{C}$ into real ones, $\rho_1, \ldots, \rho_r$, and pairs of complex conjugate ones, $\sigma_1, \bar{\sigma}_1, \ldots, \sigma_s, \bar{\sigma}_s$. Define

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

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 1.2.18. Consider a commutative diagram as follow:

$$\begin{tikzcd}
K^* \arrow[r, "j"] \arrow[d, "N_{K/\mathbb{Q}}"'] & K_{\mathbb{R}}^* \arrow[r, "l"] \arrow[d, "N"'] & {[\prod_\tau \mathbb{R}]^+} \arrow[d, "\mathrm{Tr}"] \\
\mathbb{Q}^* \arrow[r] & \mathbb{R}^* \arrow[r, "\log|\cdot|"'] & \mathbb{R}
\end{tikzcd}$$

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

In the upper part of the diagram we consider the subgroups

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

We obtain the homomorphisms

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

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

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

Proposition 1.2.19 (roots of unit)**.** The sequence

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

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

Definition 1.2.20 (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 1.2.21 (regulator)**.** Identifying $\left[\prod_\tau \mathbb{R}\right]^+ = \mathbb{R}^{r+s}$, 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 $\operatorname{vol}\left(\lambda\left(\mathcal{O}_K^*\right)\right)$ of the unit lattice $\Gamma = \lambda\left(\mathcal{O}_K^*\right) \subseteq H$, and will now compute it. Let $\varepsilon_1, \ldots, \varepsilon_t, t = r+s-1$, be a system of fundamental units and Φ the fundamental mesh of the unit lattice $\lambda\left(\mathcal{O}_K^*\right)$, spanned by the vectors $\lambda\left(\varepsilon_1\right), \ldots, \lambda\left(\varepsilon_t\right) \in H$. The vector

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

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 $\lambda_0, \lambda\left(\varepsilon_1\right), \ldots, \lambda\left(\varepsilon_t\right)$ in $\mathbb{R}^{t+1}$. But this has volume

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

where $[\lambda_1(\varepsilon_i), \ldots, \lambda_{t+1}(\varepsilon_i)] = \lambda(\varepsilon_i) \in \mathbb{R}^{r+s}$. 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 $\lambda\left(\mathcal{O}_K^*\right)$ in H is

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

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

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

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

Definition 1.2.22 (cyclotomic units)**.** Let ζ be a primitive m-th root of unity, $m \geq 3$. Show that the numbers $\dfrac{1-\zeta^k}{1-\zeta}$ 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.

Example 1.2.23 (fundamental unit of real quadratic field)**.** Consider real quadratic field $\mathbb{Q}(\sqrt{d})$. There's unique fundamental unit $a+b\sqrt{d}$ such that $a>0, b>0$ and we denote it by ϵ.

(1) If $d \equiv 2,3 (\bmod 4)$. Take $y=1,2,\ldots,$ one by one and check whether $dy^2 \pm 1$ is perfect square. Take $y=y_0$ be the minimal positive integer such that dy^2+1 or dy^2-1 be perfect square. If $dy^2-1=x_0^2, x_0>0$ is perfect square, then $\epsilon = x_0+y_0\sqrt{d}$ with $N_{K/\mathbb{Q}}(\epsilon)=-1$ and if $dy^2+1=x_0^2, x_0>0$ is perfect square, then $\epsilon=x_0+y_0\sqrt{d}$ with $N_{K/\mathbb{Q}}(\epsilon)=1$.

(2) $d=5$, the fundamental unit is $\dfrac{1+\sqrt{5}}{2}$.

(3) If $d \equiv 1 (\bmod 4)$ and $d \neq 5$, take $n=1,2,\ldots,$ one by one and check whether $n^2d \pm 4$ is a perfect square. Since $d \neq 5$, it's impossible for both of them to be perfect square. Take $n=n_0$ be the minimal positive integer such that $dn^2 \pm 4$ be perfect square and take $m_0>0$ such that $m_0^2 = dy_0^2 \pm 4$. If $m_0^2-dy_0^2=4$, $\epsilon = \dfrac{m_0+n_0\sqrt{d}}{2}$ with with $N_{K/\mathbb{Q}}(\epsilon)=1$. If $m_0^2-dy_0^2=-4$, $\epsilon=\dfrac{m_0+n_0\sqrt{d}}{2}$ with with $N_{K/\mathbb{Q}}(\epsilon)=-1$.

1.3 Ramification Theory

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

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

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,

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

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 1.1.7, we have

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

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

Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$ such that $\mathfrak{p}\mathcal{O}_L$ is relatively prime to the conductor $\mathfrak{F}$ and let

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

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

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

Remark 1.3.8. If $K = \mathbb{Q}$, then $p \nmid |\mathcal{O}_L/\mathcal{O}_K[\alpha]|$ 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

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

Remark 1.3.9. If $p(X)$ is separable module $\mathfrak{p}$, then $d(1, \theta, \dots, \theta^{n-1}) \notin \mathfrak{p}$, hence

$$(1) = d(1, \theta, \dots, \theta^{n-1})\mathcal{O}_L + \mathfrak{p}\mathcal{O}_L = \mathfrak{p}\mathcal{O}_L + \mathfrak{F}$$

Definition 1.3.10. The prime ideal $\mathfrak{p}$ is said to split completely (or to be totally split) in L, if in the decomposition

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

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 $\mathcal{O}_{\mathcal{K}}$ 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 1.3.11. p unramified over K if and only if p divides d_K.

Example 1.3.12. Let $K = \mathbb{Q}(\sqrt{-14})$ and $3\mathcal{O}_K = P_1P_2$ with $P_1 \neq P_2$, then $[P_1]$ is a generator of Cl_K and its order is 4.

Theorem 1.3.13. 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 $p \geqslant 3$, and $p \nmid d(K)$

(a) if $\left(\dfrac{d}{p}\right) = 1$, $pO_K = \mathfrak{p}_1\mathfrak{p}_2$, where $\mathfrak{p}_1 \neq \mathfrak{p}_2, N(\mathfrak{p}_1) = N(\mathfrak{p}_2) = p$.

(b) if $\left(\dfrac{d}{p}\right) = -1$, $pO_K = \mathfrak{p}, N(\mathfrak{p}) = p^2$.

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

(a) if $d \equiv 1 (\operatorname{mod} 8)$, $2\mathcal{O}_K$ is totally spilt.

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

Proposition 1.3.14. 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 $x \equiv 0 \bmod \mathfrak{P}'$ and $x \equiv 1 \bmod \sigma\mathfrak{P}$ 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 1.3.15. 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

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

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

Proposition 1.3.16. $[G : G_{\mathfrak{P}}]$ = the number of prime ideal over $\mathfrak{p}$. In particular, one has

$$G_{\mathfrak{P}} = 1 \Longleftrightarrow Z_{\mathfrak{P}} = L \Longleftrightarrow \mathfrak{p} \text{ is totally split,}$$
$$G_{\mathfrak{P}} = G \Longleftrightarrow Z_{\mathfrak{P}} = K \Longleftrightarrow \mathfrak{p} \text{ is nonsplit.}$$

Proposition 1.3.17. 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,

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

Proof: 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 $\sigma_i : \mathcal{O} \to \mathcal{O}$ induces an isomorphism

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

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

$$\mathfrak{P}^\nu \,|\mathfrak{p}\mathcal{O} \Longleftrightarrow \sigma_i\left(\mathfrak{P}^\nu\right)|\, \sigma_i(\mathfrak{p}\mathcal{O}) \Longleftrightarrow \left(\sigma_i\mathfrak{P}\right)^\nu \mid \mathfrak{p}\mathcal{O}$$

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 1.3.18. 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 1.3.19. Every $\sigma \in G_{\mathfrak{P}}$ induces an automorphism

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

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

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

is surjective.

Definition 1.3.20. The kernel $I_{\mathfrak{P}} \subseteq G_{\mathfrak{P}}$ of the homomorphism,

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

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

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

Proposition 1.3.21. One has

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

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

(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 1.3.22.

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

The following diagram demonstrates what we obtain

$$\begin{tikzcd}
 & L \arrow[dl, Rightarrow] & 1 \arrow[d, "\text{index}=e"] & \mathfrak{P} \\
\text{Galois} & T_{\mathfrak{P}} \arrow[u, "e"'] \arrow[dl, Rightarrow] & I_{\mathfrak{P}} \arrow[d, "\text{index}=f"] & \mathfrak{P}_T \arrow[u, "g_3=1,e_3=e,f_3=1"'] \\
\text{Galois} & Z_{\mathfrak{P}} \arrow[u, "f"'] & G_{\mathfrak{P}} \arrow[d, "\text{index}=g"] & \mathfrak{P}_Z \arrow[u, "g_2=1,e_2=1,f_2=f"'] \\
 & K \arrow[u, "g"'] & \mathrm{Gal}(L/K) & \mathfrak{p} \arrow[u, "e(\mathfrak{P}_Z/\mathfrak{p})=f(\mathfrak{P}_Z/\mathfrak{p})=1"']
\end{tikzcd}$$

Definition 1.3.23 (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

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

such that

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

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, we usually 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 1.3.24. *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 extenison. then*
$$\left.\left(\frac{L/K}{\mathfrak{P}}\right)\right|_E = \left(\frac{E/K}{\mathfrak{P}_E}\right)$$

Theorem 1.3.25. *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 $\mathfrak{P}_1 = \mathfrak{P} \cap E_1, \mathfrak{P}_2 = \mathfrak{P} \cap E_1$. 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

$$\varphi : \operatorname{Gal}(L/K) \to \operatorname{Gal}(E_1/K) \times \operatorname{Gal}(E_2/K), \sigma \mapsto \left(\sigma|_{E_1}, \sigma|_{E_2}\right)$$

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 1.3.24,

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

Corollary 1.3.26. If L/K is abelian, $Z_{\mathfrak{P}}$ is the maximal intermediate field such that $\mathfrak{p}$ is totally spilt and $T_{\mathfrak{P}}$ is the maximal intermediate field such that $\mathfrak{p}$ is unramified.

Example 1.3.27. The Lucas sequence

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

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

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

For prime number $p \neq 2, q$

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

Proposition 1.3.28. Let n be a prime power ℓ^ν and $K = \mathbb{Q}(\zeta_n)$. Put $\lambda = 1 - \zeta_n$. Then the principal ideal (λ) in the ring $\mathcal{O}$ of integers of $\mathbb{Q}(\zeta)$ is a prime ideal of in inertia degree, and we have

$$\ell \mathcal{O}_K = (\lambda)^d, \qquad \text{where } d = \varphi\left(\ell^\nu\right) = [\mathbb{Q}(\zeta_n) : \mathbb{Q}]$$

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

$$d\left(1, \zeta_n, \ldots, \zeta_n^{d-1}\right) = \pm \ell^s, \quad s = \ell^{\nu-1}(\nu\ell - \nu - 1)$$

Proposition 1.3.29. A $\mathbb{Z}$-basis of ring of integers of $\mathbb{Q}(\zeta_n)$ is given by $1, \zeta_n, \ldots, \zeta_n^{d-1}$, with $d = \varphi(n)$, in other words,

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

Proposition 1.3.30. 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

$$p^{f_p} \equiv 1 (\operatorname{mod} m), \text{ where } m = n/p^{\nu_p}$$

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

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

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

Proof: Consider the Frobenius Automorphism 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 1.3.28, we have $e = \varphi\left(p^{\nu_p}\right), f = f_p, g = \dfrac{\varphi(m)}{f_p}$.

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

Theorem 1.3.31. For distinct prime number p and q, we have

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}, \quad \left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{(p-1)/2\cdot(q-1)/2}$$

Proof: Notice that $(-1)^{(p^2-1)/8} = 1$ iff $p \equiv 1, 7 (\bmod 8)$ iff $\zeta_8 + \zeta_8^{-1} = \zeta_8^p + \zeta_8^{-p}$. And $\zeta_8 + \zeta^{-1} = \zeta^p + \zeta^{-p}$ if and only if $\left(\dfrac{\mathbb{Q}(\sqrt{2})/\mathbb{Q}}{p}\right)$ is trivial. This is equivalent to

$$\left(\frac{2}{p}\right) = 1$$

by Proposition 1.3.24.

For the second equation, consider the Gauss Sum

$$g(a,p) = \sum_{x=1}^{p-1} \zeta_p^{ax}\left(\frac{x}{p}\right), (a,p) = 1$$

We have

$$g(1,p)^2 = (-1)^{(p-1)/2}p$$

Then again consider Frobenius automorphism $\left(\dfrac{\mathbb{Q}(\sqrt{p})/\mathbb{Q}}{q}\right)$ is trivial or not.

Theorem 1.3.32 (Cubic Reciprocity)**.** Consider the ring $\mathbb{Z}[\omega] = \mathbb{Z}[\frac{-1+\sqrt{3}}{2}]$, prime number p factors in $\mathbb{Z}[\omega]$ as follow:

(1) If $p = 3$, then $1-\omega$ is prime in $\mathbb{Z}[\omega]$ and $3 = -\omega^2(1-\omega)^2$.

(2) If $p \equiv 1 \bmod 3$, then there is a prime $\pi \in \mathbb{Z}[\omega]$ such that $p = \pi\bar{\pi}$, and the primes π and $\bar{\pi}$ are nonassociate in $\mathbb{Z}[\omega]$.

(3) If $p \equiv 2 \bmod 3$, then p remains prime in $\mathbb{Z}[\omega]$.

Now we define the generalized Legendre symbol $(\alpha/\pi)_3$. Let π be a prime of $\mathbb{Z}[\omega]$ not dividing 3. It is straightforward to check that $3 \mid N(\pi) - 1$. Now suppose that $\alpha \in \mathbb{Z}[\omega]$ is not divisible by π. Then $x = \alpha^{(N(\pi)-1)/3}$ is a root of $x^3 \equiv 1 \bmod \pi$. Since

$$x^3 - 1 \equiv (x-1)(x-\omega)\left(x-\omega^2\right) \bmod \pi$$

and π is prime, it follows that

$$\alpha^{(N(\pi)-1)/3} \equiv 1, \omega, \omega^2 \bmod \pi.$$

Then we define the Legendre symbol $(\alpha/\pi)_3$ to be the unique cube root of unity such that

$$\alpha^{(N(\pi)-1)/3} \equiv \left(\frac{\alpha}{\pi}\right)_3 \bmod \pi$$

It's easy to check

$$\begin{aligned}\left(\frac{\alpha}{\pi}\right)_3 = 1 &\iff \alpha^{(N(\pi)-1)/3} \equiv 1 \bmod \pi \\ &\iff x^3 \equiv \alpha \bmod \pi \quad \text{ has a solution in } \mathbb{Z}[\omega]\end{aligned}$$

To state the law of cubic reciprocity, we need one final definition: a prime π is called primary if $\pi \equiv \pm 1 \bmod 3$. Given any prime π not dividing 3, one can show that exactly two of the six associates $\pm\pi, \pm\omega\pi$ and $\pm\omega^2\pi$ are primary.

Firstly, if $\pi = a + b\omega$ is a prime such that $a \equiv 1 (\bmod 3), b \equiv 2 (\bmod 3)$. Then $3 | N(\pi)$, we have $\pi | 3$, a contradiction. The case $\pi = a + b\omega$ when $a \equiv 2 (\bmod 3), b \equiv 1 (\bmod 3)$ is similar. Hence, it's easy to check that the coefficient pair (a, b) of $(\pi, \omega\pi, \omega^2\pi)$ always falls in one of the following circles module 3: $(3k+1, 3k+1) \to (3k+2, 3k) \to (3k, 3k+2)$ and $(3k+2, 3k+2) \to (3k+1, 3k) \to (3k, 3k+1)$.

Then the law of cubic reciprocity states the following: If π and θ are primary primes in $\mathbb{Z}[\omega]$ of unequal norm, then

$$\left(\frac{\theta}{\pi}\right)_3 = \left(\frac{\pi}{\theta}\right)_3.$$

Proposition 1.3.33. Let π be prime and not associate to $1-\omega$. Then we may assume that $\pi \equiv -1 \bmod 3$ (if π is primary, one of $\pm\pi$ satisfies this condition). Writing $\pi = -1 + 3m + 3n\omega$, then

$$\left(\frac{\omega}{\pi}\right)_3 = \omega^{m+n}$$
$$\left(\frac{1-\omega}{\pi}\right)_3 = \omega^{2m}$$

Theorem 1.3.34 (Biquadratic Reciprocity)**.** Let p be a prime in $\mathbb{Z}$. Then:

(1) If $p = 2$, then $1+i$ is prime in $\mathbb{Z}[i]$ and $2 = i^3(1+i)^2$.

(2) If $p \equiv 1 \bmod 4$, then there is a prime $\pi \in \mathbb{Z}[i]$ such that $p = \pi\bar{\pi}$ and the primes π and $\bar{\pi}$ are nonassociate in $\mathbb{Z}[i]$.

(3) If $p \equiv 3 \bmod 4$, then p remains prime in $\mathbb{Z}[i]$.

Furthermore, every prime in $\mathbb{Z}[i]$ is associate to one of the primes listed in (i)-(iii) above.

We also have the following version of Fermat's Little Theorem: if π is prime in $\mathbb{Z}[i]$ and doesn't divide $\alpha \in \mathbb{Z}[i]$, then

$$\alpha^{N(\pi)-1} \equiv 1 \bmod \pi$$

Then, for α not divisible by π, the Legendre symbol $(\alpha/\pi)_4$ is defined to be the unique fourth root of unity such that

$$\alpha^{(N(\pi)-1)/4} \equiv \left(\frac{\alpha}{\pi}\right)_4 \bmod \pi$$

A similar result:

$$\left(\frac{\alpha}{\pi}\right)_4 = 1 \Longleftrightarrow x^4 \equiv \alpha \bmod \pi \quad \text{is solvable in } \mathbb{Z}[i],$$

A prime π of $\mathbb{Z}[i]$ is primary if $\pi \equiv 1 \bmod 2+2i$. Any prime not associate to $1+i$ has a unique associate which is primary. With this normalization, the law of biquadratic reciprocity can be stated as follows:

If π and θ are distinct primary primes in $\mathbb{Z}[i]$, then

$$\left(\frac{\theta}{\pi}\right)_4 = \left(\frac{\pi}{\theta}\right)_4 (-1)^{(N(\theta)-1)(N(\pi)-1)/16}$$

There are also supplementary laws which state that

$$\left(\frac{i}{\pi}\right)_4 = i^{-(a-1)/2}$$
$$\left(\frac{1+i}{\pi}\right)_4 = i^{\left(a-b-1-b^2\right)/4}$$

where $\pi = a+bi$.

Example 1.3.35. Let $K = \mathbb{Q}(\sqrt{-3})$ and $L = K(\sqrt[3]{2})$. Notice that L is a Galois extension of K. Consider π be a prime such that $\pi \nmid 6$, then (π) is unramified over L. Now we show that

$$\left(\frac{L/K}{\pi}\right)(\sqrt[3]{2}) = \left(\frac{2}{\pi}\right)_3 \sqrt[3]{2}$$

To prove this, let $\mathfrak{P}$ be a prime of $\mathcal{O}_L$ containing π. Then,

$$\begin{aligned}\left(\frac{L/K}{\pi}\right)(\sqrt[3]{2}) &\equiv \sqrt[3]{2}^{N(\pi)} \bmod \mathfrak{P} \\ &\equiv 2^{(N(\pi)-1)/3} \cdot \sqrt[3]{2} \bmod \mathfrak{P}.\end{aligned}$$

Since,

$$2^{(N(\pi)-1)/3} \equiv \left(\frac{2}{\pi}\right)_3 \bmod \pi$$

we have

$$\left(\frac{L/K}{\pi}\right)(\sqrt[3]{2}) \equiv \left(\frac{2}{\pi}\right)_3 \sqrt[3]{2} \bmod \mathfrak{P}$$

Since $x^3 - 2$ is separable module $\mathfrak{P}$,

$$\left(\frac{L/K}{\pi}\right)(\sqrt[3]{2}) = \left(\frac{2}{\pi}\right)_3 \sqrt[3]{2}$$

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

Definition 1.3.36. Assume $\mathfrak{A}$ is a fractional ideal of L. Define

$$^*\mathfrak{A} = \left\{x \in L : \mathrm{Tr}_{L/K}(x\mathfrak{A}) \subset \mathcal{O}_K\right\}$$

Since $\mathfrak{A}$ is fractional ideal, $^*\mathfrak{A} \neq 0$. If $\alpha_1, \ldots, \alpha_n \in \mathcal{O}_L$ is a basis of L/K and $d = \det\left(\mathrm{Tr}\left(\alpha_i\alpha_j\right)\right)$ 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 $x = x_1\alpha_1 + \cdots + x_n\alpha_n \in {}^*\mathfrak{A}$, with $x_i \in K$, then the ax_i satisfy the system of linear equations $\sum_{i=1}^n ax_i \,\mathrm{Tr}\left(\alpha_i\alpha_j\right) = \mathrm{Tr}\left(xa\alpha_j\right) \in \mathcal{O}_K$. This implies $dx_ia \in \mathcal{O}_K$ and thus $dax \in \mathcal{O}_L$. Hence $^*\mathfrak{A}$ is also a fractional ideal.

Definition 1.3.37. The fractional ideal

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

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

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

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 1.3.38 (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 1.3.39. $f(X) = a_0 + a_1X + \cdots + a_nX^n \in F[X]$ with $a_n \neq 0$, F algebraiclly closed, and $\alpha_1, \ldots, \alpha_n$ be roots of $f(X)$. Suppose $\alpha_1, \ldots, \alpha_n$ are distinct, then

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

Proposition 1.3.40. If $\mathcal{O}_L = \mathcal{O}_K[\alpha]$, the different is the principal ideal

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

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

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

By above Lemma,

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

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

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

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

$$\mathfrak{C}_{\mathcal{O}_L|\mathcal{O}_K} = f'(\alpha)^{-1}\left(\mathcal{O}_Kb_0 + \cdots + \mathcal{O}_Kb_{n-1}\right) = f'(\alpha)^{-1}\mathcal{O}_L$$

Theorem 1.3.41. The different $\mathfrak{D}_{L|K}$ is the ideal generated by all differents of elements $\delta_{L|K}(\alpha)$ for $\alpha \in \mathcal{O}_L$.

Theorem 1.3.42. 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

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

Definition 1.3.43 (relative norm)**.** $\mathfrak{P}$ be a prime ideal in $\mathcal{O}_L$ and $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_K$, define

$$N_{L/K}(\mathfrak{P}) = (\mathfrak{p})^{[\mathcal{O}_L/\mathfrak{P}:\mathcal{O}_K/\mathfrak{p}]}$$

and for non-zero ideal of $\mathcal{O}_K$ in general, $N_{L/K}$ is defined by unqiue factorization.

Definition 1.3.44 (relative discriminant)**.** The discriminant $\mathfrak{d}_{L|K}$ is the ideal of $\mathcal{O}_L$ which is generated by the discriminants $d(\alpha_1, \ldots, \alpha_n)$ of all the bases $\alpha_1, \ldots, \alpha_n$ of $L \mid K$ which are contained in $\mathcal{O}_L$.

Theorem 1.3.45. The following relation exists between the discriminant and the different:

$$\mathfrak{d}_{L|K} = N_{L|K}\left(\mathfrak{D}_{L|K}\right).$$

Corollary 1.3.46. 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 1.3.47. If $\mathfrak{D}_{L/K} = \mathfrak{P}_1^{e_1} \ldots \mathfrak{P}_s^{e_s}$, then

$$\mathfrak{D}_{L_{\mathfrak{P}_i}|K_{\mathfrak{p}_i}} = \pi_{\mathfrak{P}_i}^{e_i} \mathcal{O}_{\mathfrak{P}_i}$$

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 $\mathfrak{o}_\nu$, 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 $\mathfrak{o}_\nu$ for all but finitely many places. Therefore, K embeds diagonally into $\mathbb{A}_K$:

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

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 $\mathbb{I}_K$:

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

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 $\mathbb{A}_\infty$ 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

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

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

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

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

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

(4): Take $x = (x_\nu) \in \mathbb{A}_K$, there's $0 \neq m \in \mathbb{Z}$ such that $mx_v \in \mathfrak{o}_\nu$ 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 $\nu \in S(\varepsilon$ sufficiently small). Then $x_v - y/m \in \mathfrak{o}_\nu$.

Proposition 1.4.3. K is a discrete subgroup of $\mathbb{A}_K$(hence closed by Proposition 2.1.14) 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 2.1.44, 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.

Remark 1.4.4. Assume $\alpha_1, \ldots, \alpha_n$ is an integral basis of $\mathcal{O}_K$, define

$$\lambda : K \to (\mathbb{R})^{r_1} \times (\mathbb{C})^{r_2}, \alpha \mapsto (\rho_1(\alpha), \ldots, \rho_{r_1}(\alpha), \sigma_{r_1}(\alpha), \ldots, \sigma_{r_2}(\alpha))$$

and

$$\Omega_\infty = \left\{ \sum_{i=1}^n k_i \sigma(\alpha_i) : 0 \leq k_i < 1, i = 1, \ldots, n \right\}$$

Then,

$$\Omega_\infty \times \prod_{\nu \text{ finite}} \mathcal{O}_\nu$$

forms a fundamental domain of $\mathbb{A}_K/K$.

Proposition 1.4.5. K^* is a discrete subgroup of $\mathbb{I}_K$(hence closed by Proposition 2.1.14) 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 1.4.6. 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 1.4.7. Now we will fix a Haar measure for each completion of K.

(1) If $F = \mathbb{R}$, then let dx be the standard Lesbesgue 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 $\mathrm{Vol}\left(\mathfrak{o}_F, dx\right) = N\left(\mathfrak{D}_F\right)^{-1/2}$, where $\mathfrak{D}_F$ denotes the different of F, which is an integral ideal of $\mathfrak{o}_F$.

Remark 1.4.8. By Theorem 1.3.42, for all the completion K_ν, there are only finite many finite places such that $\mathrm{Vol}\left(\mathfrak{o}_F, dx\right) \neq 1$.

Theorem 1.4.9. 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 1.4.10. Define

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

to be the absolute value on $\mathbb{I}_K$.By Proposition 2.1.51, $|\cdot|_{\mathbb{I}_K}$ is continous and surjective. Hence, $\mathbb{I}_K/K^*$ cannot be compact.

Theorem 1.4.11 (Artin's product formula)**.** For all $x \in K^*$, $|x|_{\mathbb{I}_K} = 1$ and $|\cdot|_{\mathbb{I}_K}$ is surjective.

Proof: By Theorem 2.3.41, 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 1.4.12. Define Ker $|\cdot|_{\mathbb{I}_K} = \mathbb{I}_K^1$ and we call it ideles of norm one.

Proposition 1.4.13. 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 2.1.51.

Proposition 1.4.14. LCHA $C_K^1 = \mathbb{I}_K^1 / K^*$ is compact.

Definition 1.4.15. For $\xi = (\xi_v) \in \mathbb{A}_K^\times = \mathbb{I}_K$, define the closed subset

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

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 $\mathbb{A}_K$ that is adapted to counting measure on the discrete subgroup K and the volume-1 measure on the compact quotient $\mathbb{A}_K/K$. Let $Z \subseteq \mathbb{A}_K$ 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 $\mathbb{A}_K/K$, which is to say that the projection map $\pi : \xi Z \to \mathbb{A}_K/K$ has some fiber with size at least 2 . Indeed, if χ on $\mathbb{A}_K$ is the characteristic function of the subset ξZ, then by Theorem 2.1.39(we need to find $f_n \in C_c(\mathbb{A}_K), n = 1, \ldots$ such that $f_n \to \chi$ pointwise and $f_n \leq f_{n+1}$ for all $n \geq 1$)

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

with $\bar{\mu}$ the volume-1 Haar measure on $\mathbb{A}_K/K$, and so if all fibers of π have size at most 1 then we get $\mu(\xi Z) \leq \int_{\mathbb{A}_K/K} \mathrm{d}\bar{\mu} = 1$, 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 1.4.16 (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 1.4.17. 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 $\mathfrak{o}_\nu$. A function $f \in S(\mathbb{A}_K)$ is called an adelic Schwartz-Bruhat function.

Proposition 1.4.18. For each place ν of K, let ψ_ν be the standard unitary character on K_ν. Then the restriction of ψ_ν to $\mathfrak{o}_\nu$ 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:

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

Proposition 1.4.19. Let K be a number field with the standard character ψ_K, as defined above. Then the following assertions hold:

(1) The map $\alpha_{\psi_K} : \mathbb{A}_K \to \widehat{\mathbb{A}_K}$, defined by $y \mapsto \psi_{K,y}$, where $\psi_{K,y}(x) = \psi_K(xy)$, is an isomorphism(as topological groups).

(2) The map $\beta_{\psi_K} : K \to \widehat{\mathbb{A}_K/K}$, 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-defind K-vector space structure on $K^\perp/K$. Hence $K^\perp = K$.

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

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

Proof: Fix a self-dual Haar measure on $\mathbb{A}_K$ and a suitable measure on $\mathbb{A}_K/K$ such that Theorem 2.1.39 holds.(Haar measure on K is counting measure). Then, we define

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

Hence,

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

Then by Fourier Inversion Formula, we have

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

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

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

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 conuting measure on K) and Theorem 2.1.39 hold simultaneously. Moreover, under this measure , the volume of the entire group $\mathbb{A}_K/K$ is 1.

Proof: Notice that the measure working on $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$(Recall that for $\mathbb{C}$, we use the twice of the Lebesgue measure) is the same as the measure induced by the inner product on $\mathbb{K}_{\mathbb{R}}$.

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

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

Notice that

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

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

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

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 is a continuous homomorphism $\chi : \mathbb{I}_K \to \mathbb{C}^\times$ such that $\chi|_{K^\times} = 1$.

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

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 Dirchlet character $(\operatorname{mod} p^n)$ for sufficiently large n. Hence, by Lemma 2.1.46, Each quasi-character of $\hat{\mathbb{Z}}^\times$ is induced by a primitive Dirchlet character.

Theorem 1.4.27. For any Dirchlet character $\chi : \hat{\mathbb{Z}}^\times \to \mathbb{S}^1$, it induces an idèle-class character by the canonical isomorphism

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

Moreover, if χ is a primitive Dirchlet character module m, then $L(s, \chi^{-1})$ identifies with the Hecke L-function of the idèle class character $\tilde{\chi}$ induced by χ. Moreover, the infinite factor of $\tilde{\chi}$ is sgn if and only if χ is an odd character.

Proof: Step 1: for all $p|m$, $\tilde{\chi}_p$ is ramified.

Step 2: for all $p \nmid m$, $\tilde{\chi}_p$ is unramified and $\tilde{\chi}_p(p) = \chi^{-1}(p)$

Step 3: $\tilde{\chi}_\infty(-1) = \chi(-1)$.

Chapter 2

Local Field

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. Morover, 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.

Definition 2.1.4. A homomorphism $G \to H$ between topological groups is a continous group homomorphism $\varphi : G \to H$.

Proposition 2.1.5. G, H are topological groups. $\varphi : G \to H$ is a group homomorphism, then φ is continous if and only if φ is continous at identity.

Definition 2.1.6. 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 $\|\|_u$ 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 2.1.7. Let G be a topological group. Every function $f \in C_c(G)$ is both left and right uniformly continuous.

Proposition 2.1.8. 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 2.1.9. X is a topological space, G is a topological group. If a topological group action is a group $G \times S \to S$ which is also continuous. If in addition the action is transitive, we call it transitive topological group action.

Example 2.1.10. 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 $\rho : G \times G/H \to G/H : (g, aH) \mapsto gaH$ is a transtive topological group action.

Proof: If U open in G/H, let

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

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

Proposition 2.1.11. Let G be a topological group and let H be a subgroup of G. Then the following assertions hold:

(1) The canonical projection $\rho : G \to G/H$ 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 2.1.12. 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 $\rho : G \to G/H$ is a closed map.

Proposition 2.1.13. 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 2.1.14 (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 2.1.15 (LCHG quotient group)**.** If G is LCHG and H is a closed subgroup, then G/H is a locally compact and Hausdorff space.

Theorem 2.1.16. Inverse limit exists in category of topological group.

Proof:

Example 2.1.17 (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 2.1.18 (pro-finite group)**.** A topological group is pro-finite if it is isomorphic to a inverse limit of finite discrete topological group.

Proposition 2.1.19. 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 $\prod_i G_i - \lim G_i$ 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 2.1.20 (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 2.1.21. G is discrete, then $\hat{G}$ is compact.

Proof: G is compact, then by Tychonoff'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 2.1.22. G is comact, then $\hat{G}$ is discrete.

Proposition 2.1.23. 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 2.1.24. G is a LCHA, then $\hat{G}$ is also LCHA.

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

Hausdorff: if $\chi_1 \neq \chi_2$, there's $g \in G$ such that $\chi_1(g) \neq \chi_2$. 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 $\chi_1 U(K, N(\varepsilon_0)) \cap \chi_2 U(K, N(\varepsilon_0)) = \varnothing$.

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 2.1.25. 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 2.1.26. A left Haar measure is a non-zero Radon measure on a LCHG such that it is left-invariant.

Proposition 2.1.27. 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 $\widetilde{\mu}(E) = \mu(E^{-1})$ 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 2.1.28. Every LCHG group G possesses a left Haar measure and it is unique up to a constant.

Example 2.1.29 (Haar measure on $\mathbb{T}^n$.)**.** Define $\varphi : Q = [0,1)^n \to \mathbb{T}^n : x \mapsto x + \mathbb{Z}^n$ a bijection map. and notive that $\mu : E \in B_{\mathbb{T}^n} \mapsto m(\varphi^{-1}(E)$ is a left invariant Radon measure.

And by Risez 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 2.1.30 (Pontrjagin Duality)**.** G LCHA. Then the map $G \to \hat{\hat{G}} : g \mapsto (\chi \mapsto \chi(g))$ is an isomorphic between topological group.

Definition 2.1.31 (Fourier Transform)**.** Let $f \in L_1(G)$. Then we define $\hat{f} : \hat{G} \to \mathbb{C}$, 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 continous function vanishes at infty.($\in C_0(G)$).

Theorem 2.1.32 (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 $L^2(\widehat{G})$.

Theorem 2.1.33 (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 2.1.34 (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 $\Delta : G \to (0, \infty)$ thus defined. It is called the modular function of G.

Proposition 2.1.35. 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

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

Proposition 2.1.36. 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 2.1.37. Let G be a LCHG, S a LCH space, $\rho : G \times S \to S$ a transitive G-action on S. Take $s_0 \in S$, define $\varphi : G \to S, g \mapsto gs_0$. Let H be the stabilizer at s_0, a closed subgroup of G. It induces a continous bijection $\Phi : G/H \to S$.

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

Definition 2.1.38. G is a LCHG with left Haar measure dx, H is a closed subgroup of G with left Haar measure $d\xi, q : G \to G/H$ 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 $P : C_c(G) \to C_c(G/H)$ by

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

Theorem 2.1.39. 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 2.1.40. G a LCHA. Suppose H is a closed subgroup of G. Then $H^\perp$ is a closed subgroup of $\widehat{G}$. We have

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

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

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

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

Definition 2.1.41 (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_v with respect to H_v 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 2.1.42 (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 2.1.43. G itself is a LCHG.

Proposition 2.1.44. A subset Y of G has compact closure if and only if $Y \subseteq \prod K_\nu$, for some family of compact subsets $K_\nu \subseteq G_v$, such that $K_\nu = H_\nu$ for all but finitely many indices ν.

Proposition 2.1.45. There exists a topological embedding of $G_\nu \longrightarrow G$ given by

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

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

Lemma 2.1.46. Let $\chi \in \mathrm{Hom}_{\mathrm{Cont}}(G, \mathbb{C}^\times)$ (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 2.1.47. For each ν let $\chi_\nu \in \mathrm{Hom}_{\mathrm{Cont}}\ (G_\nu, \mathbb{C}^\times)$and $\chi_\nu|_{H_\nu} = 1$ for all but finitely many indices ν. Then we have that $\chi = \prod_\nu \chi_\nu \in \mathrm{Hom}_{\mathrm{Cont}}\ (G, \mathbb{C}^\times)$.

Theorem 2.1.48. 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 $H_\nu^\perp$.

Proof: We will begin by showing that $K(G_\nu, H_\nu)$ is a compact-open subgroup of $\hat{G}_\nu$. 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 $\hat{G}_\nu$. By Proposition 2.1.11 and 2.1.40, $K(G_\nu, H_\nu)$ is a compact open subgroup.

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

Definition 2.1.49 (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 2.7.19, hence also Haar measure on G_S). We will write $dg = \prod_\nu dg_\nu$ for this measure.

Proposition 2.1.50. 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

$$\int_G f(g) = \lim_{n\to\infty} \int_{G_{S_n}} f(g_s)\, dg_S$$

Proposition 2.1.51. Let S_0 denote the finite set of indices containing both J_∞ and the set of indices for which $\operatorname{Vol}(H_\nu, dg_\nu) \neq 1$. 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_v are all abelian group.

Proposition 2.1.52. 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

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

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

Theorem 2.1.53. 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

$$\hat{\hat{f}}_\nu\left(g_\nu\right) = \mathrm{Vol}\left(H_\nu, dg_\nu\right) \int_{\hat{G}_\nu} \mathbf{1}_{H_\nu^\perp}\left(\chi_\nu\right) \chi_\nu\left(g_\nu\right) d\chi_\nu =$$

$$\mathrm{Vol}\left(H_\nu, dg_\nu\right) \int_{H_\nu^\perp} \chi_\nu\left(g_\nu\right) d\chi_\nu = \mathrm{Vol}\left(H_\nu, dg_\nu\right) \mathrm{Vol}\left(H_\nu^\perp, d\chi_\nu\right) 1_{\left(H_\nu^\perp\right)^\perp}$$

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

2.2 Infinite Galois Theory

Definition 2.2.1. Consider field extensions $F \subset E \subset F_{sep} \subset \bar{F}$, E/F is called (infinite) Galois extension if E/F is normal.

Definition 2.2.2. $(L_i)_{i\in I}$ are all finite Galois extenison of F contained in E, notice that $\mathrm{Gal}(E/L_1L_1) = \mathrm{Gal}(E/L_1) \cap \mathrm{Gal}(E/L_1)$ for $i, j \in I$ and for all $\sigma \in \mathrm{Gal}(E/F)$, $\sigma^{-1}\mathrm{Gal}(E/L_i)\sigma = \mathrm{Gal}(E/L_i)$. Hence $(\mathrm{Gal}(E/L_i)_{i\in I}$ induce a topological group structure on $\mathrm{Gal}(E/F)$ such that $(\mathrm{Gal}(E/L_i))_{i\in I}$ form a neighborhood at id of $G = \mathrm{Gal}(E/F)$ by Theorem 2.1.2. We call it Krull topology.

Proposition 2.2.3. *E/F is a Galois extenison, $G = \mathrm{Gal}(E/F)$ be the Galois group with Krull topology.*

(1) *$\mathrm{Gal}(E/L_j)_{j\in J}$, where $(L_i)_j$ are all the finite extenison of F such that $E \supset L_i$, also defines the Krull topology.*

(2) *If K/F is a field extension contained in E which is not necessarily finite, then $\mathrm{Gal}(K/E)$ is closed.*

(3) *The following map*

$$\varphi : \mathrm{Gal}(E/F) \to \mathrm{Gal}(K/F), \tau \mapsto \tau|_K$$

is continuous and surjective.

Proof: (1): Let L'_j be the Galois closure of L_j under $\bar{F}$. Notice that $L'_j \subset E$, we have for all $\sigma \in G$, $\sigma^{-1}\mathrm{Gal}(E/L'_j)\sigma \subset \mathrm{Gal}(E/L_i)$. By uniqueness, this neighborhood basis also defines Krull topology.

(2): Since open subgroup is closed and $\mathrm{Gal}(E/F)$ equals to the intersection of all the $\mathrm{Gal}(E/L)$ such that L is finite subfield of F.

(3):φ is well-defined by Theorem 1.4.37 in Algebra and surjective by Lemma 1.4.15 in Algebra and Theoerm 1.4.37. More Specifically, by Lemma 1.4.15, for all $\sigma \in \mathrm{Gal}(K/F)$, we may find σ_1 such that $\sigma_1|_F = \sigma$ and $\sigma_1 \in \mathrm{Hom}_F(E, E)$. And Theoerm 1.4.37 implies $\sigma_1 \in \mathrm{Gal}(E/F)$.

Theorem 2.2.4. *E/F Galois extenison and $\mathrm{Gal}(E/F)$ be the Galois group with Krull topology, then the map*

$$\iota = \prod \varphi : \mathrm{Gal}(E/F) \longrightarrow \prod_{K/F \text{ is finite Galois}} \mathrm{Gal}(K/F)$$

is injective, continous, homomorphism. Morover, its image $\varprojlim \mathrm{Gal}(K/F)$ as a pro-finite group is isomorphic to $\mathrm{Gal}(E/F)$.

Proof: We only need to check that $l' : \mathrm{Gal}(E/F) \to \varprojlim \mathrm{Gal}(K/F)$ is open. Notice that

$$\iota' \left(\mathrm{Gal}\left(E/K_j\right)\right) = \left(\{1\} \times \prod_{K_i \neq K_j} \mathrm{Gal}\left(K_i/F\right)\right) \cap \varprojlim \mathrm{Gal}\left(K_i/F\right)$$

Remark 2.2.5. In above isomorphism, we only need to take $(K_i)_{i\in I}$ such that K_i/F finite Galois and union of all K_i is E since $\mathrm{Gal}(E/K_i)$ form a neighborhood basis of $\mathrm{Gal}(E/F)$.

Corollary 2.2.6. Fix the prime p and assume ξ_{p^n} is the p^n-th primitive root of unity. Let $K := \cup\mathbb{Q}(\xi_{p^n})$. Since $K/\mathbb{Q}$ is the union of finite Galois extensions $\mathbb{Q}(\xi_{p^n})/\mathbb{Q}$, $K/\mathbb{Q}$ is Galois such that

$$\mathrm{Gal}(K/\mathbb{Q}) \cong \varprojlim (\mathbb{Z}/p^n\mathbb{Z})^\times = \mathbb{Z}_p^\times$$

Corollary 2.2.7. The absolute Galois group of $\mathbb{F}_p$ is

$$\mathrm{Gal}\left(\overline{\mathbb{F}}_p/\mathbb{F}_p\right) \cong \varprojlim \mathbb{Z}/n\mathbb{Z} = \widehat{\mathbb{Z}}$$

Theorem 2.2.8 (infinite Galois correspondence)**.** E/F Galois extension and $G = \mathrm{Gal}(E/F)$ be the Galois group with Krull Topology, we have

(1) $E^G = F$.

(2) H be a subgroup of G, $\bar{H} = \mathrm{Gal}(E/E^H)$.

(3) By (1),(2), there's one-to-one correspondence between closed subgroup of G and subfield of E containing F.

(4) H is open iff E^H is finite over F.

(5) H is normal iff E^H is Galois over E

Proof: (1): By Proposition 2.2.3.

(2): It clear that $\bar{H} \subset \mathrm{Gal}(E/E^H)$, and for all $\sigma \in \mathrm{Gal}(E/E^H)$, there's K/F finite Galois extenison such that $\sigma\mathrm{Gal}(K/F) \cap H = \varnothing$. Let φ be the restriction from G to $\mathrm{Gal}(K/F)$. We have $\varphi(\sigma) \in \varphi(H)$ since for all $x \in K^{\varphi(H)}$, $x \in K \cap E^H$ be definition. Hence $\sigma(x) = x$, then $\varphi(\sigma) \in \varphi(H)$.

Notice that $\varphi^{-1}(\varphi(\sigma)) = \sigma\mathrm{Gal}(K/F)$, a contradiction!

(3): Assume H is a closed subgroup. There's one-to-one correspondence between G/H and $\mathrm{Hom}_F(E^H, \bar{F})$. H open iff finite indexed iff $\mathrm{Hom}_F(E^H, \bar{F})$ is finite iff $[E^H : F]$ is finite.

(4): Notice that $\sigma\mathrm{Gal}(E/K)\sigma^{-1} = \mathrm{Gal}(E/\sigma(K))$, then it follows from the equivalent definition of normal extenison.

2.3 Valuations

Definition 2.3.1. A valuation of a field K is a non-trivial function

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

enjoying the properties

(1) $|x| \geq 0$, and $|x| = 0 \Longleftrightarrow x = 0$,

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

(3) $|x + y| \leq |x| + |y|$

Definition 2.3.2. 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)

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

Definition 2.3.3. The valuation $|\cdot|$ is called nonarchimedean if $|n|$ stays bounded, for all $n \in \mathbb{N}$. Otherwise it is called archimedean.

Proposition 2.3.4. The valuation $|\cdot|$ is nonarchimedean if and only if it satisfies the strong triangle inequality

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

Proposition 2.3.5. 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 $a_1 + \cdots + a_n = 0$, at least two of them take the maximal valuation.

Definition 2.3.6 (prime divisor)**.**

Theorem 2.3.7 (Weak Approximation Theorem)**.** Let $|\cdot|_1, \ldots, |\cdot|_n$ be pairwise inequivalent valuations of the field K and let $a_1, \ldots, a_n \in K$ be given elements. Then for every $\varepsilon > 0$ there exists an $x \in K$ such that

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

Theorem 2.3.8. Every valuation of $\mathbb{Q}$ is equivalent to one of the valuations $|\cdot|_p$ or $|\cdot|_\infty$.

Definition 2.3.9. 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) $v(x) = \infty \Longleftrightarrow x = 0$,

(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 and equivalence class of exponential valuation.

Definition 2.3.10. 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 2.3.11. For finite finite $\mathbb{F}_q$ and $K = \mathbb{F}_q(t)$ the function field in one variable. The valuations $v_{\mathfrak{q}}$ 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 2.3.12 (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 2.3.13 (discrete valuation)**.** An exponential valuation v is called discrete if it admits a smallest positive value s. In this case, one finds

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

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 $v\left(x\pi^{-m}\right)=0$, 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

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

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 $|\cdot|=q^{-\nu}(q>1)$ 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

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

of subgroups

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

of $\mathcal{O}^*$.

Theorem 2.3.14. Let K be a field which is complete with respect to an archimedean valuation $|\ |$. Then there is an isomorphism σ from K onto $\mathbb{R}$ or $\mathbb{C}$ satisfying

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

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

Proposition 2.3.15. 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

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

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

Proposition 2.3.16. 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 $w_1, \cdots, w_r \in O_E$, and $\bar{w}_1, \cdots, \bar{w}_r \in \bar{E}$ are $\bar{F}-$ linearly independent, then for $a_1, \cdots, a_r \in F$, we have
$$v\left(a_1 w_1 + \cdots + a_r w_r\right) = \min_{1 \leqslant i \leq r} \left\{v\left(a_i\right)\right\}$$
In particular , $w_1, \cdots, w_r$ are $F-$ linealy independent. Hence $f(Q/P) \leqslant [E : F]$.

(2) If $\pi_0, \cdots, \pi_s \in E^{\times}$, and $v\left(\pi_j\right) (0 \leqslant j \leqslant s)$ are representatives for $v\left(F^{\times}\right)/v\left(E^{\times}\right)$, then for $b_0, \cdots, b_s \in F$, we have

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

In particular, $\pi_0, \cdots, \pi_s$ are F-linearly independent. Hence, $e(Q/P) \leqslant [E : F]$.

Proposition 2.3.17. 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 2.3.18. 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 $\widehat{K}$ admits a unique representation as a convergent series

$$x = \pi^m \left(a_0 + a_1 \pi + a_2 \pi^2 + \cdots\right)$$

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

Example 2.3.19. 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 2.3.20 (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 $f(x) = a_0 + a_1x + \cdots + a_nx^n \in \mathcal{O}[x]$ primitive if $f(x) \not\equiv 0 \bmod \mathfrak{p}$, i.e., if

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

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

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

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

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

Corollary 2.3.21. 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 2.3.22. Let K be complete with respect to the valuation $|\ |$. Then $|\ |$ may be extended in a unique way to a valuation of any given algebraic extension L/K. This extension is given by the formula

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

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

Definition 2.3.23. For a Global field, we mean finite extenison 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 2.3.24. A local field is locally compact and its valuation ring is compact.

Theorem 2.3.25. Let L be a local field. Then L is isomorphic to a finite extension of $\mathbb{Q}_p$ or $\mathbb{F}_q((t))$.

Proposition 2.3.26. 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, $(\pi) = \left\{\pi^k \mid k \in \mathbb{Z}\right\}$, $q = \#\kappa$ 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 finite extension of p-adic fields with $O_E, O_F, \bar{E}, \bar{F}$ their rings of integers and residue fields.

Theorem 2.3.27. 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 2.3.28. $x \in O_E$ 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 2.3.29. O_E is a free O_K-module with rank n.

Proof: By structure of finitely generated module over PID and Lemma 1.1.7.

Proposition 2.3.30. E/F is unramified if $e = 1, f = n$.

(1) E/F is unramified extension. If $\bar{E} = \bar{F}(\alpha_0)$ for some $\alpha_0 \in \bar{E}$, take $\alpha \in \mathcal{O}_E$ such that $\bar{\alpha} = \alpha_0$, then $E = F(\alpha)$. Moreover, if $f(x)$ is the minimal polynomial of α over F,we have $\bar{f}(x)$ is the minimal polynomial of $\bar{\alpha}$ over $\bar{F}$.

(2) Assume $E = F(\alpha), \alpha \in \mathcal{O}_E$ and $g(x)$ is a monic polynomial in $O_F[x]$. If $\bar{g}(x)$ doesn't have multiple roots in the algebraic closure of $\bar{F}$, E/F is unramified.

Example 2.3.31. 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 finte extenison of $\mathbb{Q}_p$ with uniformlizer π. By Hensel's Lemma, since $x^{p^f-1} - 1 \equiv 0 (\bmod \pi)$ have $p^{f-1} - 1$ 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 extenison 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
$$\bar{g}(X)=X^f+\bar{a}_{f-1}X^{f-1}+\cdots+\bar{a}_1X+\bar{a}_0$$
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 2.3.32. E/F fintie extension of p-adic field.

(1) If K/F is a finite extension of p-adic field and E/F is unramified, then KE/K is unramified.

(2) If $E_1/F, E_2/F$ are unramified, E_1E_2/F is unramified.

Example 2.3.33. 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 2.3.30, $\mathbb{Q}_p(\zeta_n)$ 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 2.3.34. E/F fintie extension of p-adic field.

(1) If E/F totally ramified and $E=F(\pi)$, the minimal polynomial of π over F is Eisenstein polynomial.

(2) If $E=F(\alpha)$ and the minimal polynomial of α over F is Eisenstein polynomial, we have E/F totally ramified and α is a prime in $\mathcal{O}_E$.

Proposition 2.3.35. 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 $\varphi\left(p^m\right)=(p-1)p^{m-1}$.

(2) $\operatorname{Gal}\left(\mathbb{Q}_p(\zeta)\mid\mathbb{Q}_p\right)\cong(\mathbb{Z}/p^m\mathbb{Z})^*$.

(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 2.3.36. If $n=p^lm$, $(m,p)=1$, 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 2.3.37. 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 $\alpha_1, \ldots, \alpha_d$ over $\mathbb{Z}_p$, i.e., $\mathcal{O} = \mathbb{Z}_p\alpha_1 \oplus \cdots \oplus \mathbb{Z}_p\alpha_d \cong \mathbb{Z}_p^d$. Therefore $U^{(n)} \cong \mathbb{Z}_p^d$. Since the index $\left(U^{(1)} : U^{(n)}\right)$ 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 2.3.38.

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

Theorem 2.3.39. Fix an algebraic closure of $\mathbb{Q}_p$($p = \infty$ or a prime number). For a finite extenison of $\mathbb{Q}$, if $\sigma : K \to \overline{\mathbb{Q}_p}$ 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 $\hat{K}$ continously and preserves absolute value. Meanwhile, the image of the completion coincides with the composition of K and $\mathbb{Q}_p$ which also be a fintie extension of $\mathbb{Q}_p$.

$$\begin{tikzcd}
\hat{K} \arrow[rr, "\hat{\sigma}"] & & \overline{\mathbb{Q}_p} \\
& K \arrow[ul] \arrow[ur, "\sigma"] & \mathbb{Q}_p \arrow[u] \\
& \mathbb{Q} \arrow[u] \arrow[ur] &
\end{tikzcd}
\qquad \hat{\sigma}(\hat{K}) = \mathbb{Q}_p K$$

Theorem 2.3.40. 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 2.3.41. 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 the $\mathbb{Q}_p$-vector space linear transform

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

We claim that this gives an isomorphism of $\mathbb{Q}_p$ vector space. Notice that, by previous theorem, the dimension of these two $\mathbb{Q}_p$-algebra are the same. Hence, it suffices to show $\mathrm{Ker}\varphi = 0$. 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 $\mathrm{Ker}\varphi = 0$ follows from the determinant of Vandermonde matrix.

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

$$f_x(t) = \prod_{i=1}^{r} f^i_{\sigma_i(x)}(t) \text{ in } \mathbb{Q}_p[t]$$

And we can obtain two direct Corollaries from this formula if we view $\mathbb{Q}$ as a subfield of $\mathbb{Q}_p$: for all $x \in K$,

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

Corollary 2.3.42. K is an algebraic number field, assume

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

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

Remark 2.3.43. We may replace $\mathbb{Q}$ in above theormes by an arbitrary fixed algebraic number field F and consider a finite number field extension K/F.

Lemma 2.3.44 (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 2.3.45. 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 2.3.46 ($\mathbb{C}_p$)**.** 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 $p_0(c) \equiv 0(\mathrm{mod} P)$, $\mathbb{Q}_p(c) \supset \mathbb{Q}_p(\zeta_0)$. 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 2.3.47. $\mathbb{C}_p$ 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 2.3.45, 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 2.3.48 (Newton's Polygon)**.** Fix a absolute value $|\cdot|$ and valuation v_p on $\mathbb{C}_p$ such that it extends normal absoulte value and valuation on $\mathbb{Q}_p$. Let $f(X) = 1+a_1X+a_2X^2+\cdots+a_nX^n \in \mathbb{C}_p[X]$ be a polynomial, and let $m_1, m_2, \ldots, m_r$ be the slopes of its Newton polygon (in increasing order). Let $i_1, i_2, \ldots, i_r$ be the corresponding lengths. Then, for each $k, 1 \le k \le r, f(X)$ has exactly i_k roots (in $\mathbb{C}_p$, counting multiplicities) of absolute value p^{m_k}.

Lemma 2.3.49 (Lucas' Theorem)**.** Let n, m be positive integers with $k < n$, written in base p as $n = b_0 + b_1p + \cdots + b_sp^s$ and $m = a_0 + a_1p + \cdots + a_sp^s$. (We add extra zeros to the base p expansion of m if necessary so that the two expansions have the same length.) Then

$$\binom{n}{m} \equiv \binom{b_0}{a_0}\binom{b_1}{a_1}\cdots\binom{b_s}{a_s}(\mathrm{mod} p)$$

Example 2.3.50. Exponential Taylor polynomials

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

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 $n = b_1p^{n_1} + b_2p^{n_2} + \cdots + b_sp^{n_s}$ 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 $(x_i, -\mathrm{ord}_p(x_i!))$ for $1 \le i \le s$, where $x_i = b_1p^{n_1} + \cdots + b_ip^{n_i}$, 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 $\binom{n}{x_i} \equiv 1(\mathrm{mod} p)$, so in particular $\mathrm{ord}_p\left(\binom{n}{x_i}\right) = 0$.

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 $n = \prod_p p^{\mathrm{ord}_p(n)}$.

2.4 p-adic analysis

Assume K is a finite extenison of $\mathbb{Q}_p$ with π an uniformlizer.

Proposition 2.4.1. (1) A sequence (a_n) in K is Cauchy if and only if

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

(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 $i, \lim_{j\to\infty} b_{ij} = 0$, and and $\lim_{i\to\infty} b_{ij} = 0$ 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 2.4.2. Let $f(X) = \sum_{n=0}^{\infty} a_n X^n$, and define

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

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

(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 $\lim_{n\to\infty} |a_n| \rho^n = 0$, then $f(x)$ converges if and only if $|x| \le \rho$.

(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 2.4.3 (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 2.4.4. 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 $|b_n x^n| \le |g(x)|$ (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 2.4.5. 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 2.4.6. 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 2.4.7. 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 2.4.8. 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 2.4.9. 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 2.4.10 (Strassman)**.** Let

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

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

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

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

Definition 2.4.11 (log on p-adic field)**.** For a p-adic number field K there is a uniquely determined continuous homomorphism

$$\log : K^* \to K$$

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

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

Proof: It's clear that log is unique and by Proposition 2.4.1(4), log is continous.

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 2.4.5, for all $\alpha \in \mathbb{Z}$,

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

Since

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

and

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

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 2.4.12. 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 2.4.13 (p-aid Interpolation)**.** K is a p-adic field and $x \in U^{(1)}$, define

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

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

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

Proposition 2.4.14. 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

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

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

Proposition 2.4.15. For $1+x \in U^{(1)}$ and $z \in \mathbb{Z}_p$

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

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

Chapter 3

Tate's Thesis

Setting: $F = \mathbb{R}$, $\mathbb{C}$ 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. Fourier Transform is defined to be

$$\hat{f}(\chi) = \int_G f(y)\chi(y)dg.$$

3.1 Local characters and Haar Measure

Definition 3.1.1. A $\chi \in \mathrm{Hom}_{\mathrm{cont}}(F^\times, \mathbb{C}^\times)$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

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

continously. 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 $\mathbb{C} \to \mathbb{C}^*, z \mapsto \exp(z)$ 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 classify 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 $\mathrm{sgn}|\cdot|^s$.

(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 $s \in \mathbb{C}/\dfrac{2\pi i}{\log q}\mathbb{Z}$ 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) ($F = \mathbb{C}$). Let $\psi(x) = e^{-2\pi i \operatorname{Tr}_{\mathbb{C}/\mathbb{R}}(x)}$.

(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

$$x = x_{-r}p^{-r} + x_{1-r}p^{1-r} + \cdots + x_{-1}p^{-1} + x_0 + x_1 p + \cdots$$

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

$$\psi_p : \mathbb{Q}_p \to S^1, x \mapsto e^{2\pi i \lambda(x)}.$$

Now, for finite extension F of $\mathbb{Q}_p$, we define $\psi(x) = \psi_p(\operatorname{Tr}_{F/\mathbb{Q}_p}(x))$.

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:
$$\psi|_{\mathfrak{p}^m} \equiv 1 \text{ iff } \mathrm{Tr}_{F/\mathbb{Q}_p}(\mathfrak{p}^m) \subset \mathbb{Z}_p \text{ iff } \mathfrak{p}^m \subset \text{ inverse different}$$

Theorem 3.1.7. If ψ is a non-trivial character on F, for each $a \in F$, define $\psi_a : F \to \mathbb{S}^1$ by $\psi_a(x) = \psi(ax)$. Then the map $\alpha_\psi : F \to \hat{F}$ given by $a \mapsto \psi_a$ is a topological group isomorphism. For example,
$$\mathbb{R} \to \hat{\mathbb{R}}, a \mapsto (x \mapsto e^{-2\pi iax})$$
and
$$\mathbb{C} \to \hat{\mathbb{C}}, a \mapsto (x \mapsto e^{-2\pi i \,\mathrm{Tr}_{\mathbb{C}/\mathbb{R}}(ax)})$$
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,
$$\hat{\hat{f}}(x) = \int_{\mathfrak{D}_F^{-1}} N\left(\mathfrak{D}_F\right)^{-1/2}\chi(yx)dy = N\left(\mathfrak{D}_F\right)^{-1/2}\mu(\mathfrak{D}_F^{-1})\chi_{\mathfrak{o}_F}(x) = \chi_{\mathfrak{o}_F}(x)$$
In the last equality, we use $\mu(\mathfrak{D}_F^{-1}) = N(\mathfrak{D}_F)\mu(\mathfrak{o}_F)$

Definition 3.1.9 (Haar measure on multiplicative group of F)**.** Define a constant
$$c_F = \begin{cases} 1, & F = \mathbb{R}, \mathbb{C} \\ \dfrac{q}{q-1}, & F = \text{ p-adic field} \end{cases}$$
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 2.7.12, μ is a Haar measure on $F^\times$. We denote it by d^*x.

Then, there is a one-to-one correspondence of $L^1\left(F^\times\right)$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

$$\operatorname{Vol}\left(\mathfrak{o}_F^\times, d^*x\right) = \frac{q}{q-1}\int_{\mathfrak{o}_F^\times} dx = \operatorname{Vol}\left(\mathfrak{o}_F, dx\right) - \operatorname{Vol}\left(\pi_F\mathfrak{o}_F, dx\right))q/(q-1) = \operatorname{Vol}\left(\mathfrak{o}_F, dx\right)$$

3.2 Global Functional Equation

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 $f = 1_{a+p^l}$, the characteristic function of the set $a + \mathfrak{p}^\ell$, is

$$\hat{f}(y) = \psi(ay)N(\mathfrak{D}_F)^{-\frac{1}{2}}N(\mathfrak{p})^{-l}1_{\mathfrak{p}^{-l}\mathfrak{D}_F^{-1}}(y)$$

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 $\chi \in \operatorname{Hom}_{\text{cont}}\left(F^\times, \mathbb{C}^\times\right)$.

(1) If $F = \mathbb{C}$, then let

$$L\left(\chi_{s,n}\right) = \Gamma_{\mathbb{C}}\left(s + \frac{|n|}{2}\right) = (2\pi)^{-\left(s+\frac{|n|}{2}\right)}\Gamma\left(s + \frac{|n|}{2}\right)$$

(2) If $F = \mathbb{R}$ and $\chi = |\cdot|^s$ or $\chi = \operatorname{sgn}|\cdot|^s$, then let

$$L(\chi) = \begin{cases} \Gamma_{\mathbb{R}}(s) = \pi^{-s/2}\Gamma(s/2) & \text{if } \chi = |\cdot|^s \\ \Gamma_{\mathbb{R}}(s+1) & \text{if } \chi = \operatorname{sgn}|\cdot|^s \end{cases}$$

(3) If F is non-Archimedean, then let

$$L(\chi)=\begin{cases}\left(1-\chi\left(\pi_F\right)\right)^{-1} & \text{if } \chi \text{ is unramified}\\ 1 & \text{otherwise}\end{cases}$$

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 $L\left(\chi|\cdot|_F^s\right)$. We define the shifted dual of χ to be

$$\check{\chi}=\chi^{-1}|\cdot|_F$$

so that

$$L((\chi|\cdot|^s)^\vee)=L(1-s,\chi^{-1})$$

Definition 3.2.7 (local zeta function)**.** For $f\in S(F)$ and $\chi\in\operatorname{Hom}_{\text{cont}}\left(F^\times,\mathbb{C}^\times\right)$, 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 $\omega:\mathcal{O}_F^\times\to\mathbb{C}^\times$ and $\psi:\mathcal{O}_F\to\mathbb{C}^\times$, 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 $|g(\omega,\psi)|^2=c_F^2q^{-m}N(\mathfrak{D}_F)^{-1}$.

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

$$\begin{aligned}|g(\omega,\psi)|^2&=\int_{\mathcal{O}_F^\times}\omega(x)\psi(x)d^\times x\overline{\int_{\mathcal{O}_F^\times}\omega(y)\psi(y)d^\times y}\\&=\int_{\mathcal{O}_F^\times}\int_{\mathcal{O}_F^\times}\omega\left(xy^{-1}\right)\psi(x-y)d^\times xd^\times y\\&=\int_{\mathcal{O}_F^\times}\int_{\mathcal{O}_F^\times}\omega(z)\psi(yz-y)d^\times yd^\times z\\&=\int_{\mathcal{O}_F^\times}\omega(z)h(z)d^\times z\end{aligned}$$

where

$$\begin{aligned}
h(z) &= \int_{\mathcal{O}_F^\times} \psi(yz-y)d^\times y \\
&= \int_{\mathcal{O}_F^\times} \psi(y(z-1))dy \quad \big(\text{ since } |y|=1 \text{ on } \mathcal{O}_F^\times\big) \\
&= c_F \int_{\mathcal{O}_F} \psi(y(z-1))dy - c_F \int_{1+\mathfrak{p}} \psi(y(z-1))dy \\
&= c_F \times \mathrm{Vol}(\mathcal{O}_F, dx) \times \begin{cases} 1-q^{-1} & \text{if } v(z-1) \geq m \quad \text{(both integrands are 1)} \\ -q^{-1} & \text{if } v(z-1) = m-1 \quad \text{(second integrand is 1)} \\ 0 & \text{if } v(z-1) < m-1 \quad \text{(neither integrand is constant)} \end{cases}
\end{aligned}$$

Thus

$$|g(\omega,\psi)|^2 = c_F \times \mathrm{Vol}(\mathcal{O}_F, dx)(\int_{1+\mathfrak{p}^m} \omega(z)d^\times z - q^{-1}\int_{1+\mathfrak{p}^{m-1}} \omega(z)d^\times z) = c_F^2 q^{-m} N(\mathfrak{D}_F)^{-1}$$

Proposition 3.2.9. For all $\chi = \chi_0|\cdot|^s$ with $0 < \mathrm{Re}(s) < 1$, we have

$$Z(f,\chi)Z(\hat{g},\check{\chi}) = Z(\hat{f},\check{\chi})Z(g,\chi)$$

Proposition 3.2.10. 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 $\epsilon(\chi)$ such that

$$\frac{Z(\hat{f},\chi^\vee)}{L(\chi^\vee)} = \epsilon(\chi)\frac{Z(f,\chi)}{L(\chi)}$$

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

$$\pi_F^n \mathfrak{o}_F - \{0\} = \bigcup_n^\infty \pi_F^k \mathfrak{o}_F^\times$$

and the translation invariance of the multiplicative measure, it follows that

$$|Z(f,\chi)| \leq c_F \int_{F-\{0\}} |f(x)||x|_F^{\sigma-1}dx = c_F \int_{F-\{0\}} \chi_{(\pi_F^n)}|x|_F^{\sigma-1}dx = \sum_{k=n}^\infty \int_{\pi_F^k\mathfrak{o}_F^\times} |x|_F^\sigma d^*x =$$

$$= \sum_{k=n}^\infty \int_{\mathfrak{o}_F^\times} \left|\pi_F^k x\right|_F^\sigma d^*x = \sum_{k=n}^\infty q^{-k\sigma}\int_{\mathfrak{o}_F^\times} d^*x = \frac{q^{-n\sigma}}{1-q^{-\sigma}}\,\mathrm{Vol}\left(\mathfrak{o}_F, dx\right)$$

(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 $F=\mathbb{R}$, $\chi=\operatorname{sgn}\cdot|\cdot|^s$, 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 uniformlizer 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

$$\begin{aligned}Z(f_0,\chi_{s,0})&=\int_{F^\times}f_0(x)\chi_{s,0}(x)d^*x=\int_{\pi_F^{-d}-\{0\}}|x|_F^s d^*x=\\&=\sum_{k=-d}\int_{\pi_F^k\mathfrak{o}_F^\times}|x|_F^s d^*x=\sum_{k=-d}^{\infty}q^{-ks}\operatorname{Vol}\left(\mathfrak{o}_F^\times,d^*x\right)=\\&=\operatorname{Vol}\left(\mathfrak{o}_F^\times,d^*x\right)\frac{q^{ds}}{1-q^{-s}}=q^{ds}\operatorname{Vol}\left(\mathfrak{o}_F^\times,d^*x\right)\left(1-|\pi_F|_F^s\right)^{-1}\\&=q^{ds}\operatorname{Vol}\left(\mathfrak{o}_F,dx\right)L\left(\chi_{s,0}\right)\end{aligned}$$

(e): If χ is ramified, i.e. $n\geq 1$, we have

$$\begin{aligned}Z(f_n,\chi_{s,n})&=\int_{F^\times}f_n(x)\chi_{s,n}(x)d^*x=\int_{\pi_F^{-d-n}\mathfrak{o}_F-\{0\}}\psi(x)\chi_0(x)|x|_F^s d^*x=\\&=\sum_{k=-d-n}^{\infty}\int_{\mathfrak{o}_F^\times}\psi\left(\pi_F^k u\right)\chi_0(u)\left|\pi_F^k u\right|_F^s d^*u=\sum_{k=-d-n}^{-d}q^{-ks}\int_{\mathfrak{o}_F^\times}\psi\left(\pi_F^k u\right)\chi_0(u)d^*u\end{aligned}$$

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 $\hat{f}_0(y)=\operatorname{Vol}\left(\mathfrak{p}^{-d},dx\right)\mathbf{1}_{\mathfrak{o}_F}(y)$, where $\mathbf{1}_{\mathfrak{o}_F}(y)$ is the characteristic function of $\mathfrak{o}_F$.

For $n > 0$ we have $\hat{f}_n(y) = \mathrm{Vol}\left(\mathfrak{p}^{-d-n}, dx\right) \mathbf{1}_{\mathfrak{p}^n-1}(y)$, where $\mathbf{1}_{\mathfrak{p}^n-1}(y)$ is the characteristic function of $\mathfrak{p}^n - 1$.

Hence,

$$Z(\hat{f}_0, \chi_{s,0}^\vee) = q^d \mathrm{Vol}\left(\mathfrak{o}_F, dx\right)^2 L(\chi_{s,0}^\vee) = L(\chi_{s,0}^\vee)$$

and

$$\epsilon\left(\chi_{s,0}, \psi, dx\right) = q^{-d(s-1)}\, \mathrm{Vol}\left(\mathfrak{o}_F, dx\right) = \left(\frac{q^{d\cdot s/2}}{q^{d(1-s)/2}}\right)^{-1}$$

If $n \geq 1$, we have

$$Z\left(\hat{f}_n, \chi_{s,n}^\vee\right) = c_F q^d \mathrm{Vol}\left(\mathfrak{o}_F, dx\right)^2 \chi_0(-1) L(\chi_{s,n}^\vee)$$

and

$$\epsilon\left(\chi_{s,n}, \psi, dx\right) = \frac{c_F q^d q^{-(d+n)s}\, \mathrm{Vol}^2\left(\mathfrak{o}_F, dx\right) \chi_0(-1)}{g\left(\chi_0, \psi_{\pi_F^{-d-n}}\right)} = C_\nu \cdot \left(\frac{q^{d\cdot s/2}}{q^{d(1-s)/2}}\right)^{-1} \left(\frac{q^{n\cdot s/2}}{q^{n(1-s)/2}}\right)^{-1}$$

where the conductor for each character in the p-adic Gauss sum is $\mathfrak{p}^n$ and $C_\nu \in \mathbb{C}$ is a constant with $|C_\nu| = 1$.

Corollary 3.2.11. If we choose standard non-trivial character(then conductor = inverse different), self-dual measure($\mathrm{Vol}(\mathcal{O}_F, dx) = q^{-d/2}$) and $s = 1/2$, $|\epsilon(\chi)| = 1$.

Definition 3.2.12. Let $\chi \in \mathrm{Hom}_{\mathrm{cont}}\left(\mathbb{I}_K/K^*, \mathbb{C}^\times\right)$. For $f \in S\left(\mathbb{A}_K\right)$, define the global zeta function by

$$Z(f, \chi) = \int_{\mathbb{I}_K} f(x)\chi(x) d^*x$$

Theorem 3.2.13. For all idele-class characters $\chi = \chi_0|\cdot|^s$ and $f \in S\left(\mathbb{A}_K\right)$, 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

$$-\mathrm{Vol}\left(C_K^1\right) f(0) \quad \text{and} \quad \mathrm{Vol}\left(C_K^1\right) \hat{f}(0)$$

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 unqiue Haar measure on $\mathbb{I}_K^1$ such that Theorem 2.1.39 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 2.1.39 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

$$\begin{aligned}
\int_{C_K^1}\left(\sum_{a\in K} f(atx)\right)\chi(tx)d^*x &= \int_{C_K^1}\left(\sum_{a\in K}\hat{f}\left(at^{-1}x^{-1}\right)\right)\frac{\chi(tx)}{|tx|_{\mathbb{I}_K}}d^*x \\
&= \int_{C_K^1}\left(\sum_{a\in K}\hat{f}\left(at^{-1}x\right)\right)\left|t^{-1}x\right|_{\mathbb{I}_K}\chi\left(tx^{-1}\right)d^*x \\
&= \int_{C_K^1}\left(\sum_{a\in K^*}\hat{f}\left(at^{-1}x\right)\right)\check{\chi}(x/t)d^*x + \hat{f}(0)\int_{C_K^1}\check{\chi}(x/t)d^*x \\
&= Z_{t^{-1}}(\hat{f},\check{\chi}) + \hat{f}(0)\int_{C_K^1}\check{\chi}(x/t)d^*x
\end{aligned}$$

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

$$\int_1^\infty Z_t(f,\chi)\frac{1}{t}dt = \int_{\left\{x\in\mathbb{I}_K : |x|_{\mathbb{I}_K}\geq 1\right\}} f(x)\chi(x)d^*x$$

Since f_v are supported on a compact subset for all finite place ν and $|f_\nu|$ decrease rapidly for all infinite place ν, we have

$\int_1^\infty Z_t(f,\chi)$ is an entire function.

$$\int_0^1 Z_t(f,\chi)\frac{1}{t}dt = \int_0^1 \left(Z_{t^{-1}}(\hat{f},\check{\chi}) + \hat{f}(0)\check{\chi}\left(t^{-1}\right)\int_{C_K^1}\check{\chi}(x)d^*x - f(0)\chi(t)\int_{C_K^1}\chi(x)d^*x \right)\frac{1}{t}dt$$

Applying the change of variable $t \mapsto t^{-1}$ to the first integral in the sum, we obtain

$$\int_0^1 Z_{t^{-1}}(\hat{f},\check{\chi})\frac{1}{t}dt = \int_1^\infty Z_t(\hat{f},\check{\chi})\frac{1}{t}dt$$

$$R(f,\chi) := \int_0^1 \hat{f}(0)\check{\chi}\left(t^{-1}\right)\int_{C_K^1}\check{\chi}(x)d^*x\frac{1}{t}dt - \int_0^1 f(0)\chi(t)\int_{C_K^1}\chi(x)d^*x\frac{1}{t}dt$$

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

$$\begin{aligned} R(f,\chi) &= \hat{f}(0)\operatorname{Vol}\left(C_K^1\right)\int_0^1 t^{s-2}dt - f(0)\operatorname{Vol}\left(C_K^1\right)\int_0^1 t^{s-1}dt \\ &= \frac{\hat{f}(0)\operatorname{Vol}\left(C_K^1\right)}{s-1} - \frac{f(0)\operatorname{Vol}\left(C_K^1\right)}{s} \end{aligned}$$

Consequently,

$$\int_0^1 Z_t(f,\chi)\frac{1}{t}dt = \int_1^\infty Z_t(\hat{f},\check{\chi})\frac{1}{t}dt + \frac{\hat{f}(0)\operatorname{Vol}\left(C_K^1\right)}{s-1} - \frac{f(0)\operatorname{Vol}\left(C_K^1\right)}{s}$$

, and hence

$$Z(f,\chi) = \int_1^\infty Z_t(f,\chi)\frac{1}{t}dt + \int_1^\infty Z_t(\hat{f},\check{\chi})\frac{1}{t}dt + \frac{\hat{f}(0)\operatorname{Vol}\left(C_K^1\right)}{s-1} - \frac{f(0)\operatorname{Vol}\left(C_K^1\right)}{s}$$

Definition 3.2.14. We define the global L-function of χ in terms of its local versions by the product expansion

$$L(\chi) = \prod_\nu L\left(\chi_\nu\right)$$

It' clear that $L(\chi)$ uniformly converges on all compact subsets of $\operatorname{Re}(s) > 1$ and holomorphic in $\operatorname{Re}(s) > 1$

Definition 3.2.15 (Hecke L-function)**.** Let $\chi \in \mathrm{Hom}_{\mathrm{cont}}\ (\mathbb{I}_K/K^*, \mathbb{C}^\times)$(an idele-class character). For complex s, define the Hecke L-function $L(s,\chi)$ by

$$L(s,\chi) = L\left(\chi|\cdot|^s\right)$$

If $\chi = \otimes' \chi_\nu$, define

$$L\left(s, \chi_f\right) = \prod_{\nu \text{ finite}} L\left(s, \chi_\nu\right)$$

and

$$L\left(s, \chi_\infty\right) = \prod_{\nu | \infty} L\left(s, \chi_\nu\right)$$

respectively. Then

$$L(s,\chi) = L(s,\chi_f) L(s,\chi_\infty)$$

Example 3.2.16. For χ equals to identity character 1 on $\mathrm{Hom}_{\mathrm{cont}}\ (\mathbb{I}_K/K^*, \mathbb{C}^\times)$, 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 3.2.17 (Analytic Class Number Formula)**.**

$$\mathrm{Vol}\left(C_K^1\right) = \frac{2^{r_1} (2\pi)^{r_2} h_K R_K}{\omega_K \sqrt{|d_K|}}$$

Proof: Assume F is an algebraic number field. Firstly, we need to understand the structure of $\mathbb{I}_F$. Consider a surjective homomorphism

$$f : \mathbb{I}_F \to \mathcal{I}_F/\mathcal{P}_F, (\alpha_{\mathfrak{p}}) \mapsto \prod \mathfrak{p}^{\mathrm{ord}_{\mathfrak{p}}(\alpha_{\mathfrak{p}})}$$

The kernel of f equals to

$$((\mathbb{R}^\times)^{r_1} \times (\mathbb{C}^\times)^{r_2} \times \prod_{\mathfrak{p}} \mathcal{O}_{\mathfrak{p}}^*) F^\times$$

Hence,

$$\mathbb{I}_F/((\mathbb{R}^\times)^{r_1} \times (\mathbb{C}^\times)^{r_2} \times \prod_{\mathfrak{p}} \mathcal{O}_{\mathfrak{p}}^*) F^\times \simeq \mathcal{C}_F$$

which is a finite group. Take $H = \{a_1, \dots, a_{h_K}\} \subset \mathbb{I}_F^1$ be a system of representatives of the quotient group and we will use it later.

Notice that

$$((\mathbb{R}^\times)^{r_1} \times (\mathbb{C}^\times)^{r_2} \times \prod_{\mathfrak{p}} \mathcal{O}_{\mathfrak{p}}^*) \cap F^\times = \mathcal{O}_F^\times$$

Consider the following maps

$$U = \{\pm 1\}^{r_1} \times (S^1)^{r_2} \xrightarrow{\subset} (\mathbb{R}^\times)^{r_1} \times (\mathbb{C}^\times)^{r_2} \xrightarrow{|\cdot|} (\mathbb{R}^\times_{>0})^{r_1} \times (\mathbb{R}^\times_{>0})^{r_2} \xrightarrow{\mathrm{Log}} \mathbb{R}^{r_1+r_2}$$

where $|\cdot|$ be the pointwise usual absolute value on $\mathbb{R}$ and $\mathbb{C}$ and Log is defined to be

$$\mathrm{Log} : (x_1, \dots, x_{r_1}, y_1, \dots, y_{r_2}) \mapsto (\log(x_1), \dots, \log(x_{r_1}), 2\log(y_1), \dots, 2\log(y_{r_2}))$$

In above diagram, Log is an isomorphism and the kernel of the second arrow is exactly the first object. Take $\varepsilon_1, \dots, \varepsilon_{r_1+r_2-1}$ be a system of fundamental units. In addition, define

$$\gamma = (\exp(1/(r_1+r_2)), \dots, \exp(1/2(r_1+r_2)), \dots, \exp(1/2(r_1+r_2))) \in (\mathbb{R}^\times_{>0})^{r_1} \times (\mathbb{R}^\times_{>0})^{r_2}$$

. We have $|\gamma|_{\mathbb{I}_F} = e$.

Define

$$\lambda : \mathcal{O}_F^\times \to (\mathbb{R}^\times)^{r_1} \times (\mathbb{C}^\times)^{r_2}, \alpha \mapsto (\rho_1(\alpha), \dots, \rho_{r_1}(\alpha), \sigma_{r_1}(\alpha), \dots, \sigma_{r_2}(\alpha))$$

Then, by Dirchlet unit theorem, $\mathrm{Log}(\gamma), \mathrm{Log}(|\lambda(\varepsilon_1)|), \dots, \mathrm{Log}(|\lambda(\varepsilon_{r_1+r_2-1})|)$ forms a basis of $\mathbb{R}^{r_1+r_2}$. Hence, there's a

$$(\mathbb{R}^\times_{>0})^{r_1} \times (\mathbb{R}^\times_{>0})^{r_2} \simeq \gamma^{\mathbb{R}} |\lambda(\varepsilon_1)|^{\mathbb{R}} \dots |\lambda(\varepsilon_{r_1+r_2-1})|^{\mathbb{R}}$$

Then, idèle can be factored as

$$\mathbb{I}_F = H \times \{\pm 1\}^{r_1} \times (S^1)^{r_2} \times \gamma^{\mathbb{R}} |\lambda(\varepsilon_1)|^{[0,1)} \dots |\lambda(\varepsilon_{r_1+r_2-1})|^{[0,1)} \times \prod_{\mathfrak{p}} \mathcal{O}_{\mathfrak{p}}^* \times F^\times.$$

And this factorization is unique up to a multiple of roots of unit in F.

Hence, take

$$M = (\{\pm 1\}^{r_1} \times (S^1)^{r_2}) \times \gamma^{[0,\log(m))} |\lambda(\varepsilon_1)|^{[0,1)} \dots |\lambda(\varepsilon_{r_1+r_2-1})|^{[0,1)} \times \prod_{\mathfrak{p}} \mathcal{O}_{\mathfrak{p}}^*$$

for some $m > 1$.

Then,

$$\begin{aligned}\int_{\mathbb{I}_F} \chi_M &= \int_{\mathbb{I}_F/\mathbb{I}_F^1} \int_{\mathbb{I}_F^1} \chi_M = \int_{\mathbb{I}_F/\mathbb{I}_F^1} \int_{\mathbb{I}_F^1/F^\times} \int_{F^\times} \chi_M \\ &= \int_1^m \frac{\omega_F}{h_F} \mathrm{Vol}(C_F^1) \frac{\mathrm{d}t}{t} \\ &= \log(m) \frac{\omega_F}{h_F} \mathrm{Vol}(C_F^1)\end{aligned}$$

On the other hand, consider the topological group isomorphism

$$(\mathbb{R}^\times)^{r_1} \times (\mathbb{C}^\times)^{r_2} \xrightarrow{\simeq} \{\pm 1\}^{r_1} \times (S^1)^{r_2} \times (\mathbb{R}^\times_{>0})^{r_1} \times (\mathbb{R}^\times_{>0})^{r_2} \xrightarrow{\mathrm{id}\times\mathrm{Log}} \{\pm 1\}^{r_1} \times (S^1)^{r_2} \times \mathbb{R}^{r_1+r_2}$$

Fix Haar measure on each component of the right hand side: $\{\pm 1\}$ with counting measure, S^1 with $\mathrm{Vol}(S^1) = 2\pi$ and Lebesgue measure on $\mathbb{R}$. Then it's easy to check Haar measures on both sides match with respect to above isomorphism! Hence,

$$\begin{aligned}\int_{\mathbb{I}_F} \chi_M =&|d_F|^{-1/2} \int_{(\mathbb{R}^\times)^{r_1}\times(\mathbb{C}^\times)^{r_2}} (\{\pm 1\}^{r_1} \times (S^1)^{r_2}) \times \gamma^{[0,\log(m))} |\lambda(\varepsilon_1)|^{[0,1)} \dots |\lambda(\varepsilon_{r_1+r_2-1})|^{[0,1)} \\ =&|d_F|^{-1/2} 2^{r_1} (2\pi)^{r_2} |\det \begin{pmatrix} \log(m)/(r_1+r_2) & \log|\rho_1(\varepsilon_1)| & \cdots & \log|\rho_1(\varepsilon_{r_1+r_2-1})| \\ \vdots & \vdots & & \vdots \\ \log(m)/(r_1+r_2) & 2\log|\sigma_{r_2}(\varepsilon_1)| & \cdots & 2\log|\sigma_{r_2}(\varepsilon_{r_1+r_2-1})| \end{pmatrix} | \\ =&|d_F|^{-1/2} 2^{r_1} (2\pi)^{r_2} R_F \log(m)\end{aligned}$$

Theorem 3.2.18. 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

$$\epsilon(s,\chi) = \prod_\nu \epsilon\left(\chi_\nu |\cdot|^s, \psi_\nu, dx_\nu\right) \in \mathbb{C}^\times$$

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

$$-|d_K|^{1/2}(2\pi)^{-r_2} \mathrm{Vol}\left(C_K^1\right), \quad (2\pi)^{-r_2} \mathrm{Vol}\left(C_K^1\right)$$

respectively.

Hence, Dedekind zeta function $\zeta_K(s)$ can be extended to a meromorphic function with only simple pole at $s = 1$ with residue

$$\mathrm{Vol}\left(C_K^1\right) = \frac{2^{r_1}(2\pi)^{r_2} h_K R_K}{\omega_K \sqrt{|d_K|}}$$

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_v for all ν as the form in Theoerm 3.2.10, 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

$$-|d_K|^{1/2}(2\pi)^{-r_2} \mathrm{Vol}\left(C_K^1\right), \quad (2\pi)^{-r_2} \mathrm{Vol}\left(C_K^1\right)$$

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 $\mathrm{Vol}(C_K^1)$ 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 3.2.19. For an arbitrary unitary idèle class character $\chi_0 = \otimes'_\nu \chi_\nu$, define

$$C_{\chi_0} = \prod_{\nu \text{ finite}} q_\nu^{n_v}$$

where n_ν be the positive integer such that $\mathfrak{p}_\nu{}^{n_\nu}$ be the conductor of χ_ν. Then

$$L(s, \chi_0)(|d_K| C_{\chi_0})^{s/2} = C L(1-s, \chi_0^{-1})(|d_K| C_{\chi_0})^{(1-s)/2}$$

for some C with $|C| = 1$.

Proposition 3.2.20. For all unitary, ramified, idèle-class character χ, $L(1, \chi) \neq 0$. In particular, $L(1 + it, \chi) \neq 0$ for all unitary, ramified, idèle-class character.

Proof:

Ideas in thesis:

(1) conductor of arbitrary Hecke L-fucntion

(2) recover weber l function by Hecke l function

(3) orthogonal-invariant measure on upper-half plane and sphere.

(4) Artin l function and hecke L function relation

(5) Converse Theorem, higher dimension automorphic L function.

(6) decomposition of idèle

(7) proof of conductor formula

Chapter 4

Class Field Theory and L-functions

4.1 Quadratic Forms

Definition 4.1.1. An integral quadratic form is $f(x, y) = ax^2 + bxy + cy^2$ where $a, b, c \in \mathbb{Z}$.

Definition 4.1.2. A form $ax^2 + bxy + cy^2$ is primitive if its coefficients a, b and c are coprime.

Definition 4.1.3. An integer m is represented by $f(x, y)$ if there's $x, y \in \mathbb{Z}$ such that $f(x, y) = m$. m is properly represented if it can by represented by x, y with $(x, y) = 1$.

Proposition 4.1.4. Next, we say that two forms $f(x, y)$ and $g(x, y)$ are equivalent if there are integers p, q, r and s such that

$$f(x, y) = g(px + qy, rx + sy) \quad \text{and} \quad ps - qr = \pm 1$$

Since $\det \begin{bmatrix} p & q \\ r & s \end{bmatrix} = ps - qr = \pm 1$, this means that $\begin{bmatrix} p & q \\ r & s \end{bmatrix}$ is in the group of 2×2 invertible integer matrices $\mathrm{GL}(2, \mathbb{Z})$, and it follows easily that the equivalence of forms is an equivalence relation. An equivalence is proper equivalence if $\begin{bmatrix} p & q \\ r & s \end{bmatrix} \in \mathrm{SL}(2, \mathbb{Z})$.

An important observation is that equivalent forms represent the same numbers, and the same is true for proper representations.

Proof: It suffice to check $(a, b) = 1$ implies $(px+qy, rx+sy) = 1$. Assume $d = (px+qy, rx+sy)$, notice that $x = s(px + qy) - q(rx + sy)$, we have $d|x$. Similarly, we have $d|y$. Hence $d = 1$.

Proposition 4.1.5. Any form equivalent to a primitive form is itself primitive.

Proof: If $\begin{bmatrix} p & q \\ r & s \end{bmatrix} (ax^2 + bxy + cy^2) = d(mx^2 + nxy + ry^2)$ with $d > 1$. Then, if $d \nmid a$, take $x = 1, y = d$(the case $d \nmid c$ is the same), and if $d \nmid b$ but $d \mid a, b$, take $x = y = 1$. A contradiction!

Definition 4.1.6. A form $f(x, y)$ properly represents an integer m if and only if $f(x, y)$ is properly equivalent to the form $mx^2 + Bxy + Cy^2$ for some $B, C \in \mathbb{Z}$.

Proof:

Definition 4.1.7. We define the discriminant of $ax^2 + bxy + cy^2$ to be $D = b^2 - 4ac$. To see how this definition relates to equivalence, suppose that the forms $f(x, y)$ and $g(x, y)$ have discriminants D and D' respectively, and that

$$f(x, y) = g(px + qy, rx + sy), \quad p, q, r, s \in \mathbb{Z}$$

Then a straightforward calculation shows that

$$D = (ps - qr)^2 D'$$

Definition 4.1.8. The sign of the discriminant D has a strong effect on the behavior of the form. If $f(x, y) = ax^2 + bxy + cy^2$, then we have the identity

$$4af(x, y) = (2ax + by)^2 - Dy^2$$

If $D > 0$, then $f(x, y)$ represents both positive and negative integers, and we call the form indefinite, while if $D < 0$, then the form represents only positive integers or only negative ones, depending on the sign of a, and $f(x, y)$ is accordingly called positive definite or negative definite. Note that all of these notions are invariant under equivalence.

Proposition 4.1.9. Let $D \equiv 0, 1 \bmod 4$ be an integer and m be an odd integer relatively prime to D. Then m is properly represented by a primitive form of discriminant D if and only if D is a quadratic residue modulo m.

Proof: If $f(x, y)$ properly represents m, then we may assume that $f(x, y) = mx^2 + bxy + cy^2$. Thus $D = b^2 - 4mc$, and $D \equiv b^2 \bmod m$ follows easily.

Conversely, suppose that $D \equiv b^2 \bmod m$. Since m is odd, we can assume that D and b have the same parity (replace b by $b + m$ if necessary), and then $D \equiv 0, 1 \text{mod } 4$ implies that $D \equiv b^2 \bmod 4m$. This means that $D = b^2 - 4mc$ for some c. Then $mx^2 + bxy + cy^2$ represents m properly and has discriminant D, and the coefficients are relatively prime since m is relatively prime to D.

Corollary 4.1.10. Let n be an integer and let p be an odd prime not dividing n. Then $(-n/p) = 1$ if and only if p is represented by a primitive form of discriminant $-4n$.

Theorem 4.1.11 (reduced form)**.** A primitive positive definite form $ax^2 + bxy + cy^2$ is said to be reduced if

$$|b| \leq a \leq c, \text{ and } b \geq 0 \text{ if either } |b| = a \text{ or } a = c$$

Every primitive positive definite form is properly equivalent to a unique reduced form.

We say that two forms are in the same class if they are properly equivalent. We will let $h(D)$ denote the number of classes of primitive positive definite forms of discriminant D, which is just the number of reduced forms.

D	$h(D)$	Reduced Forms of Discriminant D
-4	1	$x^2 + y^2$
-8	1	$x^2 + 2y^2$
-12	1	$x^2 + 3y^2$
-20	2	$x^2 + 5y^2, 2x^2 + 2xy + 3y^2$
-28	1	$x^2 + 7y^2$
-56	4	$x^2 + 14y^2, 2x^2 + 7y^2, 3x^2 \pm 2xy + 5y^2$
-108	3	$x^2 + 27y^2, 4x^2 \pm 2xy + 7y^2$
-256	4	$x^2 + 64y^2, 4x^2 + 4xy + 17y^2, 5x^2 \pm 2xy + 13y^2$

Definition 4.1.12. Denote $C(D)$ all the equivalence classes of primitive positive definite forms of discriminant D. There's an operation called Dirchlet composition such that $C(D)$ form an abelian group and the identiy is is the class containing the principal form

$$\begin{aligned} x^2 - D/4 \cdot y^2 \quad & \text{if } D \equiv 0 \bmod 4 \\ x^2 + xy + (1-D)/4 \cdot y^2 \quad & \text{if } D \equiv 1 \bmod 4 \end{aligned}$$

and the inverse of the class containing the form $ax^2 + bxy + cy^2$ is the class containing $ax^2 - bxy + cy^2$.

Now we introduce the Artin Reciprocity Theorem for the Hilbert Class Field.

Theorem 4.1.13 (Artin Reciprocity Theorem for the Hilbert Class Field)**.** Given a number field K, there is a finite Galois extension L of K such that:

(1) L is an unramified Abelian extension of K.

(2) Any unramified Abelian extension of K lies in L.

The field L of is called the Hilbert class field of K. It is the maximal unramified Abelian extension of K and is clearly unique.

If L is the Hilbert class field of a number field K, then the Artin map

$$\left(\frac{L/K}{\cdot}\right) : I_K \longrightarrow \mathrm{Gal}(L/K)$$

is surjective, and its kernel is exactly the subgroup P_K of principal fractional ideals. Thus the Artin map induces an isomorphism

$$\mathrm{Cl}_K \xrightarrow{\sim} \mathrm{Gal}(L/K).$$

Corollary 4.1.14. Let L be the Hilbert class field of a number field K, and let p be a prime ideal of K. Then $\mathfrak{p}$ splits completely in $L \Longleftrightarrow \mathfrak{p}$ is a principal ideal.

Proof: Since the order of Frobenius automorphism is f, then $f = 1 \Longleftrightarrow \mathfrak{p}$ spilts completely.

Corollary 4.1.15. Let L be the Hilbert class field of $K = \mathbb{Q}(\sqrt{-n})$. Assume that $-n \equiv 2, 3 (\bmod 4)$ is square-free, so that $\mathcal{O}_K = \mathbb{Z}[\sqrt{-n}]$. If p is an odd prime not dividing n, then

$$p = x^2 + ny^2 \Longleftrightarrow p \text{ splits completely in } L.$$

Corollary 4.1.16. Let L be the Hilbert class field of $K = \mathbb{Q}(\sqrt{-n})$. Assume that $-n \equiv 1 (\mathrm{mod}\, 4)$ is square-free, so that $\mathcal{O}_K = \mathbb{Z}[(1+\sqrt{-n})/2]$. If p is an odd prime not dividing n, then

$$p = x^2 + xy + (n+1)y^2/4 \iff p \text{ splits completely in } L.$$

Lemma 4.1.17. Let K be an imaginary quadratic field, and let $K \subset L$ be a Galois extension. As usual, τ will denote complex conjugation.

(1) Show that L is Galois over $\mathbb{Q}$ if and only if $\tau(L) = L$.

(2) If L is Galois over $\mathbb{Q}$, then prove that $[L \cap \mathbb{R} : \mathbb{Q}] = [L : K]$ and for $\alpha \in L \cap \mathbb{R}, L \cap \mathbb{R} = \mathbb{Q}(\alpha) \iff L = K(\alpha)$.

Proof: (1): Trivial

(2):

$$\begin{tikzcd}
 & L = \mathbb{Q}(\alpha) & \\
L \cap \mathbb{R} \arrow[ur, "2"] & & K \arrow[ul, "d"'] \\
\mathbb{Q}(\alpha + \bar{\alpha}) \arrow[u, "1"] \arrow[uur, "2"] & & \\
 & \mathbb{Q} \arrow[ul, "d"'] \arrow[uur, "2"'] &
\end{tikzcd}$$

Corollary 4.1.18. Hilbert class field of imaginary quadratic field is Galois over $\mathbb{Q}$.

Theorem 4.1.19. Let K be an imaginary quadratic field, and let L be a finite extension of K which is Galois over $\mathbb{Q}$. Then:

(1) There is a real algebraic integer α such that $L = K(\alpha)$.

(2) Given α as in (1), let $f(x) \in \mathbb{Z}[x]$ denote its monic minimal polynomial over $\mathbb{Q}$. If p is a prime not dividing the discriminant of $f(x)$, then

$$p \text{ splits completely in } L \iff \begin{cases} (d_K/p) = 1 \text{ and } f(x) \equiv 0 \bmod p \\ \text{has an integer solution.} \end{cases}$$

Proof:

(1): By Lemma 4.1.17.

(2): Notice that $f(x) \in \mathbb{Z}[x] \subset \mathcal{O}_K[x]$ is also the minimal polynomial of $\alpha \in L$ over K. Then (2) follows from Theorem 1.3.7 and the second following remark.

Corollary 4.1.20. Assume $-n \equiv 2,3 \pmod 4$ is square-free. Let $K = \mathbb{Q}(\sqrt{-n})$ be a imaginary quadratic field, L be its Hilbert class field, then there's an algebraic integer $\alpha \in \mathbb{R}$ such that $K(\alpha) = L$. Suppose $f_n(x) \in \mathbb{Z}[x]$ be its minimal polynomial, then

$$\begin{aligned} p = x^2 + ny^2 &\Longleftrightarrow p \text{ splits completely in } L \\ &\Longleftrightarrow \begin{cases} (-n/p) = 1 \text{ and } f_n(x) \equiv 0 \bmod p \\ \text{has an integer solution.} \end{cases} \end{aligned}$$

for all $p \nmid \operatorname{disc}(f_n)$. Moreover, we have $\deg f_n = [\mathbb{Q}(\alpha) : \mathbb{Q}] = [L : K] = h_{\mathbb{Q}(\sqrt{-n})} = h(-4n)$.

Corollary 4.1.21. Assume $-n \equiv 1 \pmod 4$ is square-free. Let $K = \mathbb{Q}(\sqrt{-n})$ be a imaginary quadratic field, L be its Hilbert class field, then there's an algebraic integer $\alpha \in \mathbb{R}$ such that $K(\alpha) = L$. Suppose $f_n(x) \in \mathbb{Z}[x]$ be its minimal polynomial, then

$$\begin{aligned} p = x^2 + xy + (n+1)y^2/4 &\Longleftrightarrow p \text{ splits completely in } L \\ &\Longleftrightarrow \begin{cases} (-n/p) = 1 \text{ and } f_n(x) \equiv 0 \bmod p \\ \text{has an integer solution.} \end{cases} \end{aligned}$$

for all $p \nmid \operatorname{disc}(f_n)$. Moreover, we have $\deg f_n = [\mathbb{Q}(\alpha) : \mathbb{Q}] = [L : K] = h_{\mathbb{Q}(\sqrt{-n})} = h(-n)$.

Theorem 4.1.22. Let K be an imaginary quadratic field of discriminant $d_K < 0$. Then:

(1) If $f(x,y) = ax^2 + bxy + cy^2$ is a primitive positive definite quadratic form of discriminant d_K, then
$$\left[a, \left(-b + \sqrt{d_K}\right)/2\right] = \left\{ma + n\left(-b + \sqrt{d_K}\right)/2 : m, n \in \mathbb{Z}\right\}$$
is an ideal of $\mathcal{O}_K$.

(2) The map sending $f(x,y)$ to $\left[a, \left(-b + \sqrt{d_K}\right)/2\right]$ induces an isomorphism between the form class group $C\left(d_K\right)$ and the ideal class group Cl_K. Hence the order of Cl_K is the class number $h\left(d_K\right)$.

Example 4.1.23. If $p \neq 7$ is an odd prime, then

$$p = x^2 + 14y^2 \Longleftrightarrow \begin{cases} (-14/p) = 1 \text{ and } \left(x^2+1\right)^2 \equiv 8 \bmod p \\ \text{has an integer solution.} \end{cases}$$

This is because $\alpha = \sqrt{2\sqrt{2} - 1}$ is a real integral primitive element of the Hilbert class field of $K = \mathbb{Q}(\sqrt{-14})$, its minimal polynomial $x^4 + 2x^2 - 7 = \left(x^2+1\right)^2 - 8$ can be chosen to be the polynomial $f_{14}(x)$. Its discriminant is $-2^{14} \cdot 7$.

4.2 Kronecker-Weber

Theorem 4.2.1. Let $K = \mathbb{Q}(\zeta_m)$, then

$$\zeta_K(s) = G(s) \prod_{\chi} L(\chi, s)$$

where χ varies over all Dirichlet characters mod$m$, and

$$G(s) = \prod_{\mathfrak{P}|m} \left(1 - \mathfrak{N}(\mathfrak{P})^{-s}\right)^{-1}$$

Proof: For $p \nmid m$, let f be the order of p module m and $g = \varphi(m)/f$. Then we have the follow diagram

$$\begin{tikzcd}
K & 1 \arrow[d, "f"] & \mathfrak{P} \arrow[d, dash] \\
Z_{\mathfrak{P}} \arrow[u] & D_p = \text{subgroup generated by } p \arrow[d, "g"] & \mathfrak{P}_Z \arrow[d, dash] \\
\mathbb{Q} \arrow[u] & G = (\mathbb{Z}/m\mathbb{Z})^{\times} & p
\end{tikzcd}$$

where D_p be the decomposition group. Notice that

$$\prod_{\chi \in \hat{G}} (1 - \chi(p)T) = \prod_{\chi \in \hat{G}/D_p^{\perp}} (1 - \chi(p)T)^g = (1 - T^f)^g$$

Then take $T = p^{-s}$.

Corollary 4.2.2. Let $K = \mathbb{Q}(\zeta_m)$,

$$\zeta_K(s) = \prod_{\chi} L(\chi, s)$$

where χ runs over primitive Dirchlet character module d with $d|m$.

Proof: It suffice to show that for $p|m$,

$$\prod_{\mathfrak{P}|p} (1 - N(\mathfrak{P})^{-s}) = \prod_{\chi'} (1 - \chi'(p)p^{-s})$$

where χ' runs over primitive Dirchlet character with conductor divides m.

Assume $m = p^{\alpha} n$, f be the order of p module n and $g = \varphi(n)/f$, then

$$\begin{aligned}
\prod_{\chi' \text{ primitive,cond}(\chi')|m} (1 - \chi'(p)p^{-s}) &= \prod_{\chi', \text{ primitive cond}(\chi')|n} (1 - \chi'(p)p^{-s}) \\
&= \prod_{\chi (\operatorname{mod} n)} (1 - \chi(p)p^{-s}) \\
&= (1 - p^{-fs})^g \\
&= \prod_{\mathfrak{P}|p} (1 - N(\mathfrak{P})^{-s})
\end{aligned}$$

Theorem 4.2.3 (Kronecker-Weber theorem)**.** Every finite abelian extension of $\mathbb{Q}$ is contained within some cyclotomic field.

Theorem 4.2.4. K is an abelian extension of $\mathbb{Q}$, take $\mathbb{Q}(\zeta_m)$ be the minimal cyclotomic field contains K. Then $H = \mathrm{Gal}(\mathbb{Q}(\zeta_m)/K)$ is a subgroup of $(\mathbb{Z}/m\mathbb{Z})^\times$. And there's a one-to-one correspondence between Dirchlet character trivial on H and the character of $\mathrm{Gal}(K/\mathbb{Q})$. We have

$$\prod_{\chi'} L(s,\chi') = \zeta_K(s)$$

where χ' runs over primiteive Dirchlet characters induced by character of $\mathrm{Gal}(K/\mathbb{Q}) = H^\perp$.

Proof: It suffices to show

$$\prod_{\mathfrak{P}|p}(1 - N(\mathfrak{P})^{-s}) = \prod_{\chi'}(1 - \chi'(p)p^{-s})$$

Assume p be a prime number, $m = p^\alpha n$, e, f, g be the ramification degree, residue field degree, spilt degree for the extension $K/\mathbb{Q}$ and Z_p, D_p, I_p are decomposition field, decomposition group and inertia group respectively with respect to the the extension $\mathbb{Q}(\zeta_m)/\mathbb{Q}$. From the following diagram, we obtain a visualization of informations of Galois correspondence:

$$\begin{tikzcd}
 & \mathbb{Q}(\zeta_m) \\
K \arrow[ur] & \mathbb{Q}(\zeta_n) \arrow[u, "\varphi(p^\alpha)"'] \\
\mathbb{Q}(\zeta_n)\cap K \arrow[u, "e"] \arrow[ur] & \\
Z_p \cap K \arrow[u, "f"] & Z_p \arrow[ul] \arrow[uu, "\mathrm{ord}_n(p)"'] \\
 & \mathbb{Q} \arrow[ul, "g"] \arrow[u, "\varphi(n)/\mathrm{ord}_n(p)"']
\end{tikzcd}
\qquad
\begin{tikzcd}
 & 1 \arrow[dl] \arrow[d] \\
H \arrow[d, "e"] & I_p = \{a : (a,p) = 1, a \equiv 1 (\mathrm{mod}\, n)\} \arrow[dl] \arrow[dd] \\
(H, I_p) \arrow[d, "f"] \arrow[dr] & \\
(H, D_p) \arrow[dr, "g"] & D_p = \left\{a : (a,p) = 1, a \equiv p^k (\mathrm{mod}\, n)\right\} \arrow[d] \\
 & (\mathbb{Z}/m\mathbb{Z})^\times
\end{tikzcd}$$

Hence,

$$\begin{aligned}
\prod_{\chi' \text{ induced by } \chi\in H^\perp}(1-\chi'(p)p^{-s}) &= \prod_{\chi' \text{ induced by } \chi\in (H,I_p)^\perp}(1-\chi'(p)p^{-s}) \\
&= \prod_{\chi'\text{induced by } \chi\in (H,I_p)^\perp/(H,D_p)^\perp}(1-\chi'(p)p^{-s})^g
\end{aligned}$$

where first equality follows from $\mathrm{cond}\chi'|m$. Since

$$(H,I_p)^\perp/(H,D_p)^\perp \simeq ((\mathbb{Z}/m\mathbb{Z})^\times/(H,I_p))^\wedge/((H,D_p)/(H,I_p)^\perp) \simeq \widehat{(H,D_p)/(H,I_p)} \simeq \mathbb{Z}/f\mathbb{Z}$$

,we have

$$\prod_{\chi'\text{induced by } \chi\in (H,I_p)^\perp/(H,D_p)^\perp}(1-\chi'(p)p^{-s})^g = (1-p^{-fs})^g$$

Lemma 4.2.5. K be an abelian extension of $\mathbb{Q}$ and $\mathbb{Q}(\zeta_m)$ be the minimal cyclotomic field contains K. $H = \mathrm{Gal}(\mathbb{Q}(\zeta_m)/K)$ be a subgroup of $(\mathbb{Z}/m\mathbb{Z})^\times$. We have

$$\widehat{\mathrm{Gal}(K/\mathbb{Q})} \simeq \left\{\chi \in \widehat{(\mathbb{Z}/m\mathbb{Z})}^\times : \chi \text{ is trivial on } H\right\}$$

Then K is totally real if and only if all the Dirchlet characters in $\widehat{\mathrm{Gal}(K/\mathbb{Q})}$ is even.

If K is not totally real, denote K^+ be the maximal real subfield of K. We have $[K : K^+] = 2$ and the even character of $\mathrm{Gal}(K/\mathbb{Q})$ is exactly the character of $\mathrm{Gal}(K^+/\mathbb{Q})$.

Proof: K is totally real iff the automorphism $\zeta_m \mapsto \zeta_m^{-1}$ fixes K iff $(-1) \in H$ iff for all $\chi \in \widehat{\mathrm{Gal}(K/\mathbb{Q})}$, $\chi(-1) = 1$. The last equivalence follows from The Second Orthogonality Relation for Group Characters.

The second statement follows from the following Galois correspondence

$$\begin{array}{ccc}
\mathbb{Q}(\zeta_m) & & 1 \\
\uparrow & & \downarrow \\
K & & H \\
\uparrow{\scriptstyle 2} & & \downarrow{\scriptstyle 2} \\
K^+ & & (H, -1) \\
\uparrow & & \downarrow \\
\mathbb{Q} & & (\mathbb{Z}/m\mathbb{Z})^\times
\end{array}$$

Corollary 4.2.6. K is a number field. If K is totally reall with $[K : \mathbb{Q}] = n$,

$$R_K h_K \cdot \frac{2^{n-1}}{|d_K|^{1/2}} = \prod_{\substack{\chi \in \widehat{\mathrm{Gal}(K/\mathbb{Q})} \\ \chi \neq \chi_0}} L\left(1, \chi^*\right).$$

If K is not totally reall with $[K : \mathbb{Q}] = n$, we have

$$\zeta_{K_+}(s) = \prod_{\chi \in \widehat{\mathrm{Gal}(K^+/\mathbb{Q})}} L\left(s, \chi^*\right) = \prod_{\substack{\chi \in \widehat{\mathrm{Gal}(K/\mathbb{Q})} \\ \chi(-1)=1}} L\left(s, \chi^*\right)$$

In particular,

$$R_K h_K \frac{(2\pi)^{n/2}}{w_K |d_K|^{1/2}} = \prod_{\substack{\chi \in \widehat{\mathrm{Gal}(K/\mathbb{Q})} \\ \chi \neq \chi_0}} L\left(1, \chi^*\right).$$

and

$$R_{K_+} h_{K_+} \cdot \frac{2^{n/2-1}}{|d_{K^+}|^{1/2}} = \prod_{\substack{\chi_0 \neq \chi \in \widehat{\mathrm{Gal}(K/\mathbb{Q})} \\ \chi(-1)=1}} L\left(1, \chi^*\right).$$

Corollary 4.2.7 (Conductor Formula)**.**

$$\prod_{\chi \in \widehat{\mathrm{Gal}(K/\mathbb{Q})}} \mathrm{cond}(\chi) = |d_K|$$

Proof: Assume K is an abelian extension of $\mathbb{Q}$ and $[K:\mathbb{Q}] = n$. If K is totally real, then is $r_1 = n$. Hence, the meromorphic function

$$|d_K|^{s/2}\zeta_K(s)(\Gamma(s/2)\pi^{-s/2})^n$$

with simple pole at $s = 0$ and $s = 1$ is invariant under $s \mapsto 1-s$. On the other hand, by Tate's thesis or functional equation of Dirchlet L-functions,

$$(\prod_{\chi \in \widehat{\mathrm{Gal}(K/\mathbb{Q})}} \mathrm{cond}(\chi))^{s/2}(\Gamma(s/2)\pi^{-s/2})^n\zeta(s) \prod_{\substack{\chi \in \widehat{\mathrm{Gal}(K/\mathbb{Q})} \\ \chi \neq \chi_0}} L\left(s, \chi^*\right)$$

is meromorphic function with simple pole at $s = 0$ and $s = 1$ which is invariant under $s \mapsto (1-s)$. Then again consider the quotient of above function and Legendre duplication formula.

If K is not totally real, since $K/\mathbb{Q}$ is Galois, we have $r_1 = 0, r_2 = n/2$. Then,

$$|d_K|^{s/2}\zeta_K(s)((2\pi)^{-s}\Gamma(s))^{n/2}$$

is invariant under $s \mapsto 1-s$. On the other hand, by Tate's thesis or functional equation of Dirchlet L-functions,

$$(\prod_{\chi \in \widehat{\mathrm{Gal}(K/\mathbb{Q})}} \mathrm{cond}(\chi))^{s/2}(\Gamma(s/2)\pi^{-s/2})^{n/2}(\Gamma((s+1)/2)\pi^{-(s+1)/2})^{n/2}\zeta(s) \prod_{\substack{\chi \in \widehat{\mathrm{Gal}(K/\mathbb{Q})} \\ \chi \neq \chi_0}} L\left(s, \chi^*\right)$$

is meromorphic function with simple pole at $s = 0$ and $s = 1$ which is invariant under $s \mapsto (1-s)$. Consider the quotient of above two equation, we can obtain the result.

Lemma 4.2.8. Assume χ be a primitive Dirchlet character module m, $m \geqslant 3$, then if $\chi(-1) = 1$,

$$L(1, \chi) = -\frac{2G(1, \chi)}{m} \sum_{1 \leqslant k < m/2} \bar{\chi}(k) \log \sin \frac{k\pi}{m},$$

and if $\chi(-1) = -1$,

$$L(1, \chi) = \frac{\pi i G(1, \chi)}{m^2} \sum_{k=1}^{m-1} \bar{\chi}(k) k = \frac{\pi i G(1, \chi)}{m(\chi(2) - 2)} \sum_{1 \leqslant k < m/2} \bar{\chi}(k)$$

where

$$G(k, \chi) = \sum_{a \in (\mathbb{Z}/m\mathbb{Z})^\times} \chi(a)\zeta_m^{ak}$$

.

Remark 4.2.9. If χ is a primitive Dirchlet character module m, $|G(1,\chi)| = \sqrt{m}$ and if $(k,m) = 1$, we have $G(k,\chi) = \overline{\chi}(k)G(1,\chi)$.

Corollary 4.2.10 (Class number of quadratic field)**.** For $K = \mathbb{Q}(\sqrt{d})$, define $m = |d_K|$. By Theorem 4.2.4 and Conductor Formula, there's primitive Dirchlet character $\chi_{\mathbb{Q}(\sqrt{d})} = \chi$ module m such that

$$\zeta_{\mathbb{Q}(\sqrt{d})}(s) = L(s,\chi)\zeta(s)$$

If $d < 0$, by lemma 4.2.5, χ is odd character and if $d > 0$, χ is a even character.

For odd prime number $p \nmid m$, we claim that $\chi(p) = \left(\frac{d}{p}\right)$. Consider the following Galois correspondence

$$\begin{tikzcd}
\mathbb{Q}(\zeta_m) & 1 \arrow[d] & \left(\frac{\mathbb{Q}(\zeta_m)/\mathbb{Q}}{p}\right) \\
\mathbb{Q}(\sqrt{d}) \arrow[u] & H \arrow[d] & \left(\frac{\mathbb{Q}(\zeta_m)/\mathbb{Q}}{p}\right)\Big|_{\mathbb{Q}(\sqrt{d})} \arrow[u] \\
\mathbb{Q} \arrow[u] & (\mathbb{Z}/m\mathbb{Z})^\times & p \arrow[u]
\end{tikzcd}$$

Notice that

$$\left(\frac{d}{p}\right) = 1 \Leftrightarrow p \text{ totally spilt in } \mathcal{O}_{\mathbb{Q}(\sqrt{d})} \Leftrightarrow \left(\frac{\mathbb{Q}(\zeta_m)/\mathbb{Q}}{p}\right)\Big|_{\mathbb{Q}(\sqrt{d})} \text{ is non-trivial}$$
$$\Leftrightarrow \left(\frac{\mathbb{Q}(\zeta_m)/\mathbb{Q}}{p}\right) \notin H \Leftrightarrow \chi(p) = -1$$

On the other hand, we can show that

$$\chi(2) = \begin{cases} 1, \text{ if } d \equiv 1(\operatorname{mod} 8); \\ -1, \text{ if } d \equiv 5(\operatorname{mod} 8); \\ 0, \text{ otherwise} \end{cases}$$

It suffice to show that case when $d \equiv 1(\operatorname{mod} 4)$ by Example 1.1.11. This equation follows from the expression of the local factor at 2 and Theorem 1.3.13.

Hence, if K is an imaginary quadratic field with $K \neq \mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-3})$, we have

$$h_K = \frac{1}{m}\sum_{k=1}^{|d_k|-1} \chi_K(k)k = \frac{1}{2-\chi_K(2)}|\sum_{1\leq k<m/2} \chi_K(k)|$$

If K is a real quadratic field with $\epsilon > 1$ be the fundamental unit, then

$$h_K = \frac{1}{\log \epsilon}|\sum_{1\leq k<m/2} \chi_K(k) \log \sin \frac{\pi k}{m}|$$

4.3 Main Theorems of Class Field Theory

Definition 4.3.1. Assume K is a algebraic number field, $\alpha \neq 0$ is totally real if for all real embeddings σ, we have $\sigma(\alpha) > 0$.

Now we fix some notations. Assume F is a algebraic number field, $0 \neq \mathfrak{m}$ be an integral ideal of $\mathcal{O}_F$.

(1) $\mathcal{I}_F = \{\text{fractional ideals of } F\}$

(2) $\mathcal{P}_F = \{\text{principal fractional ideals of } F\}$

(3) $\mathcal{C}_F = \mathcal{I}_F / \mathcal{P}_F$ be the ideal class group.

(4) $\mathcal{P}_{F,\mathfrak{m}} = \{(\alpha) : \alpha \in F - \{0\}, v_{\mathfrak{p}}(\alpha - 1) \geq \operatorname{ord}_{\mathfrak{p}}(\mathfrak{m}) \text{ for all } \mathfrak{p}|\mathfrak{m}\}$

(5) $\mathcal{P}^+_{F,\mathfrak{m}} = \{(\alpha) : \alpha \in F - \{0\}, v_{\mathfrak{p}}(\alpha - 1) \geq \operatorname{ord}_{\mathfrak{p}}(\mathfrak{m}) \text{ for all } \mathfrak{p}|\mathfrak{m}, \alpha \text{ totally real}\}$

(6) $\mathcal{I}_F(\mathfrak{m}) = \{\mathfrak{a} \in \mathcal{I}_F : \operatorname{ord}_{\mathfrak{p}} \mathfrak{a} = 0 \text{ for all } \mathfrak{p} \mid \mathfrak{m}\}$

(7) $\mathcal{P}_F(\mathfrak{m}) = \mathcal{I}_F(\mathfrak{m}) \cap \mathcal{P}_F$

(8) $\mathcal{R}^+_{F,\mathfrak{m}} = \mathcal{I}_F(\mathfrak{m}) / \mathcal{P}^+_{F,\mathfrak{m}}$ be the narrow ray class group.

(9) $\mathcal{U}_F = \mathcal{O}_F^\times$

(10) $\mathcal{U}_{F,\mathfrak{m}} = \{\varepsilon \in \mathcal{U}_F : \varepsilon \equiv 1 (\operatorname{mod} \mathfrak{m})\}$

(11) $\mathcal{U}^+_{F,\mathfrak{m}} = \{\varepsilon \in \mathcal{U}_F : \varepsilon \equiv 1 (\operatorname{mod} \mathfrak{m}), \varepsilon \text{ totally real}\}$

(12) $F(\mathfrak{m}) = \{\alpha \in F^\times, (\alpha) \in \mathcal{I}_F(\mathfrak{m})\}$

(13) $F^+_{\mathfrak{m}} = \{\alpha \in F^\times, \alpha \text{ totally real }, v_{\mathfrak{p}}(\alpha - 1) \geq \operatorname{ord}_{\mathfrak{p}}(\mathfrak{m}) \text{ for all } \mathfrak{p}|\mathfrak{m}\}$

(14) $\mathfrak{m} = \prod \mathfrak{p}^{\operatorname{ord}_{\mathfrak{p}}(\mathfrak{m})}$, $K_{\mathfrak{p}}$ be the completion at $\mathfrak{p}$ and $\pi_{\mathfrak{p}}$ be an uniformlizer of ring of integers $\mathcal{O}_{\mathfrak{p}}$ of $K_{\mathfrak{p}}$.

$$U_{\mathfrak{p}}(\mathfrak{m}) = \begin{cases} 1 + \pi_{\mathfrak{p}}^{\operatorname{ord}_{\mathfrak{p}}(\mathfrak{m})} \mathcal{O}_{\mathfrak{p}}, & \text{if } \mathfrak{p} \notin S_\infty, \mathfrak{p} \mid \mathfrak{m}, \\ \mathcal{O}_{\mathfrak{p}}^\times, & \text{if } \mathfrak{p} \notin S_\infty, \mathfrak{p} \nmid \mathfrak{m}, \\ \mathbb{R}_+^\times, & \text{if } \mathfrak{p} \in S_r \\ \mathbb{C}^\times, & \text{if } \mathfrak{p} \in S_c \end{cases}$$

(15) $\mathbb{I}_F$ be idèle.

(16) $\mathbb{U}_F(\mathfrak{m}) = \prod_{\mathfrak{p}} U_{\mathfrak{p}}(\mathfrak{m})$

(17) $\mathbb{I}_F(\mathfrak{m}) := \{\alpha \in \mathbb{I}_F : \alpha_{\mathfrak{p}} \in U_{\mathfrak{p}}(\mathfrak{m}), \forall \mathfrak{p} \mid \mathfrak{m} \text{ or } \mathfrak{p} \mid \infty\}$

Proposition 4.3.2.

$$\mathcal{P}_{F,\mathfrak{m}} = \left\{ \left\langle \frac{\alpha}{\beta} \right\rangle : \alpha, \beta \in \mathcal{O}_F \text{ prime to } \mathfrak{m}; \alpha \equiv \beta \pmod{\mathfrak{m}} \right\}$$

and

$$\mathcal{P}^+_{F,\mathfrak{m}} = \left\{ \left\langle \frac{\alpha}{\beta} \right\rangle : \frac{\alpha}{\beta} \gg 0; \alpha, \beta \in \mathcal{O}_F \text{ prime to } \mathfrak{m}; \alpha \equiv \beta \pmod{\mathfrak{m}} \right\}$$

Proof: For $0 \neq \alpha \in F$, $(\alpha) = P_1^{e_1} \dots P_s^{e_s} / Q_1^{f_1} \dots Q_r^{f_r}$ with all P_i, Q_j coprime to $\mathfrak{m}$. By CRT, there's $\gamma \in \mathcal{O}_F$ such that

$$(\gamma) = Q_1^{f_1} \dots Q_r^{f_r} M_1^{w_1} \dots M_g^{w_g}$$

where $(M_i, \mathfrak{m}) = 1$ for all $i = 1, \dots, g$. Therefore, $(\alpha) = P_1^{e_1} \dots P_s^{e_s} M_1^{w_1} \dots M_g^{w_g}/(\gamma)$. Hence,

$$\alpha = \alpha\gamma/\gamma$$

with $\alpha\gamma$ and γ coprime to $\mathfrak{m}$.

Proposition 4.3.3 (recover Dirchlet character)**.** Let $F = \mathbb{Q}, \mathfrak{m} = m\mathbb{Z}$, where $m \geq 1$. If $\langle r \rangle \in \mathcal{I}(\mathfrak{m})$, then we may suppose $r > 0$ and $r = a/b$, where $(a, m) = (b, m) = 1$. The map

$$\mathcal{I}_{\mathbb{Q}}(\mathfrak{m}) \longrightarrow (\mathbb{Z}/m\mathbb{Z})^\times$$

given by $\langle r \rangle \mapsto ab^{-1}((\operatorname{mod} m))$ is then well-defined. It is clearly surjective and its kernel is $\{\langle r \rangle : r > 0, r = a/b, (a, m) = (b, m) = 1, a \equiv b (\operatorname{mod} m)\} = \mathcal{P}^+_{\mathbb{Q},\mathfrak{m}}$. Hence for $F = \mathbb{Q}, \mathfrak{m} = m\mathbb{Z}$, we have

$$\mathcal{I}_{\mathbb{Q}}(\mathfrak{m})/\mathcal{P}^+_{\mathbb{Q},\mathfrak{m}} \cong (\mathbb{Z}/m\mathbb{Z})^\times$$

Proposition 4.3.4. $\mathcal{R}^+_{F,\mathfrak{m}}$is a finite group, with

$$\#\mathcal{R}^+_{F,\mathfrak{m}} = \frac{h_F 2^{r_1} \varphi(\mathfrak{m})}{[\mathcal{U}_F : \mathcal{U}^+_{F,\mathfrak{m}}]}$$

where

$$h_F = \#\mathcal{C}_F$$
$$r_1 = \#\text{ of real embeddings of } F$$
$$\varphi(\mathfrak{m}) = \#\left(\mathcal{O}_F/\mathfrak{m}\right)^\times = \prod_{\mathfrak{p}|\mathfrak{m}} N\mathfrak{p}^{e_\mathfrak{p}-1}(N\mathfrak{p} - 1), \text{ where } \mathfrak{m} = \prod_{\mathfrak{p}|\mathfrak{m}} \mathfrak{p}^{e_\mathfrak{p}}$$

Proof: Step 1: $\mathcal{I}_F(\mathfrak{m})/\mathcal{P}_F(\mathfrak{m}) \cong \mathcal{I}_F/\mathcal{P}_F = \mathcal{C}_F$.

Proof of Step 1: It suffice to notice that $\mathcal{I}_F = \mathcal{I}_F(\mathfrak{m})\mathcal{P}_F$

Step 2: $\mathcal{P}_F(\mathfrak{m})/\mathcal{P}^+_{F,\mathfrak{m}} \cong F(\mathfrak{m})/\mathcal{U}_F F^+_\mathfrak{m}$

Step 3: Denote $F_\mathfrak{p}$ the completion at $v_\mathfrak{p}$ with $\pi_\mathfrak{p}$ a fixed uniformlizer. And denote $\mathcal{O}_{v_\mathfrak{p}}$ the ring of integers of $F_\mathfrak{p}$. Then define a map

$$F(\mathfrak{m}) \to (\pm 1)^{r_1} \times \prod_{\mathfrak{p}|\mathfrak{m}} (\mathcal{O}_{v_\mathfrak{p}}/(\pi_\mathfrak{p}^{\operatorname{ord}_\mathfrak{p}(\mathfrak{m})}))^\times, \alpha \mapsto (\operatorname{sign}\sigma_1(\alpha), \dots, \operatorname{sign}\sigma_{r_1}(\alpha)) \times (\alpha, \dots, \alpha)$$

By Weak Approximation Theorem, it is a surjective homomorphism. And its kernel is exactly $F^+_{\mathfrak{m}}$. Hence, $[F(\mathfrak{m}) : F^+_{\mathfrak{m}}] = 2^{r_1}(\mathcal{O}_F/\mathfrak{m})^\times$

Step 4: $\mathcal{U}_F F^+_{\mathfrak{m}}/F_{\mathfrak{m}^+} \cong \mathcal{U}_F/\mathcal{U}_F \cap F^+_{\mathfrak{m}} = \mathcal{U}_F/\mathcal{U}^+_{F,\mathfrak{m}}$

Step 5:

$$\begin{tikzcd}
 & \mathcal{I}_F(\mathfrak{m}) \\
F(\mathfrak{m}) & \mathcal{P}_F(\mathfrak{m}) \arrow[u, "h_F"] \\
\mathcal{U}_F F^+_{\mathfrak{m}} \arrow[u, "b"] & \mathcal{P}^+_{F,\mathfrak{m}} \arrow[u, "b"] \\
F^+_{\mathfrak{m}} \arrow[u, "c"] \arrow[uu, bend left, "2^{r_1}(\mathcal{O}_F/\mathfrak{m})^\times"] &
\end{tikzcd}$$

$$\begin{aligned}
\# R^+_{F,\mathfrak{m}} &= \left[\mathcal{I}_F(\mathfrak{m}) : \mathcal{P}^+_{F,\mathfrak{m}}\right] = \left[\mathcal{I}_F(\mathfrak{m}) : \mathcal{P}_F(\mathfrak{m})\right]\left[\mathcal{P}_F(\mathfrak{m}) : \mathcal{P}^+_{F,\mathfrak{m}}\right] \\
&= \left[\mathcal{I}_F(\mathfrak{m}) : \mathcal{P}_F(\mathfrak{m})\right]\left[F(\mathfrak{m}) : F^+_{\mathfrak{m}}\right] / \left[\mathcal{U}_F F^+_{\mathfrak{m}} : F^+_{\mathfrak{m}}\right] \\
&= h_F 2^{r_1}\varphi(\mathfrak{m}) / \left[\mathcal{U}_F : \mathcal{U}^+_{F,\mathfrak{m}}\right].
\end{aligned}$$

Theorem 4.3.5 (idèle-class character induced by narrow ray class group character)**.** By Weak Approximation Theorem, $\mathbb{I}_F(\mathfrak{m})F^\times = \mathbb{I}_F$. Hence,

$$\mathbb{I}_F(\mathfrak{m})/\mathbb{I}_F(\mathfrak{m}) \cap F^\times = \mathbb{I}_F(\mathfrak{m})/F^+_{\mathfrak{m}} \simeq \mathbb{I}_F/F^\times$$

Obviously, the map

$$f : \mathbb{I}_F(\mathfrak{m}) \to I_F(\mathfrak{m})/\mathcal{P}^+_{F,\mathfrak{m}}, (\alpha_{\mathfrak{p}}) \mapsto \prod_{\mathfrak{p} \text{ finite}} \mathfrak{p}^{\operatorname{ord}_{\mathfrak{p}}(\alpha_{\mathfrak{p}})}$$

is surjective. Since $\mathbb{I}_F(\mathfrak{m}) \cap F^\times$ is contained in the kernel of f, f induces a surjective map j in the following diagram.

$$\begin{tikzcd}
\mathbb{I}_F/F^\times \arrow[r, "\simeq"] & \mathbb{I}_F(\mathfrak{m})/F^\times \cap \mathbb{I}_F(\mathfrak{m}) \arrow[d, two heads, "j"] & \\
\mathbb{I}_F \arrow[u] \arrow[r, dashed, "\varphi"] & \mathcal{I}_F(\mathfrak{m})/\mathcal{P}^+_{F,\mathfrak{m}} \arrow[r, "\chi"] & \mathbb{C}^\times
\end{tikzcd}$$

Notice that the kernel of

$$\tilde{f} : \mathbb{I}_F(\mathfrak{m}) \to I_F(\mathfrak{m}), (\alpha_{\mathfrak{p}}) \mapsto \prod_{\mathfrak{p} \text{ finite}} \mathfrak{p}^{\operatorname{ord}_{\mathfrak{p}}(\alpha_{\mathfrak{p}})}$$

is $\mathbb{U}_F(\mathfrak{m})$. Then, since $f(\mathbb{I}_F(\mathfrak{m}) \cap F^\times) = \mathcal{P}^+_{F,\mathfrak{m}}$, the kernel of φ identifies with $\mathbb{U}_F(\mathfrak{m})F^\times$.

Hence, we may obtain a idèle-class character from a narrow ray class group character through the isomorphism

$$\mathbb{I}_F/\mathbb{U}_F(\mathfrak{m})F^\times \simeq \mathcal{R}^+_{F,\mathfrak{m}}$$

Corollary 4.3.6. There's ono-to-one correspond between character of narrow ray class group $\mathcal{R}^+_{F,\mathfrak{m}}$ and idèle-class character trivial on $\mathbb{U}_F(\mathfrak{m})$. Moreover, for all finite order idèle-class character, there's integral ideal $\mathfrak{m}$ such that it is trivial on $\mathbb{U}_F(\mathfrak{m})$.

4.4 Galois Group Action

Setting: Let K/F be a finite extension of number fields. Let

$$\mathcal{N}_{K/F}(\mathfrak{m}) = \left\{\mathfrak{a} \in \mathcal{I}_F(\mathfrak{m}) : \mathfrak{a} = N_{K/F}(\mathfrak{A}) \text{ for some } \mathfrak{A} \in \mathcal{I}_K\right\}$$

.

Definition 4.4.1. Let K/F be a finite extension of number fields, we now define a norm $N_{K/F} : \mathbb{I}_K \to \mathbb{I}_F$ as follow: Let $(\ldots, a_w, \ldots) = a \in \mathbb{I}_K$, where the w are places of K. For a fixed place v of F, the set $\{w \text{ place of } K : w \mid v\}$ is finite. We construct the norm of a as an idèle of F by computing each v-component in terms of the corresponding set $\{w \text{ place of } K : w \mid v\}$. Specifically, we let $b_v = \prod_{w|v} N_{K_w/F_v}(a_w)$ and define $N_{K/F}(a) = (\ldots, b_v, \ldots) \in \mathbb{I}_F$. Recall that if $\alpha \in K$, then for any fixed place v of F,

$$N_{K/F}(\alpha) = \prod_{w|v} N_{K_w/F_v}(\iota_w(\alpha))$$

Hence, we obtain the following commutative diagram:

$$\begin{tikzcd}
K^\times \arrow[r] \arrow[d, "N_{K/F}"'] & \mathbb{I}_K \arrow[d, "N_{K/F}"] \\
F^\times \arrow[r] & \mathbb{I}_F
\end{tikzcd}$$

Chapter 5

L-function

5.1 Dirchlet Series

Definition 5.1.1. A Dirchlet character is a homomorphism

$$\chi : (\mathbb{Z}/m\mathbb{Z})^\times \to \mathbb{C}^\times$$

Usually, we define $\chi(n) = 0$ if $(n, m) = 1$.

Definition 5.1.2. For a Dirchlet character module m with an integer $d|m$. The following three conditions are equivalent

(1) there's Dirchlet character χ_0 module d such that χ factors through $(\mathbb{Z}/m\mathbb{Z})^\times \to (\mathbb{Z}/d\mathbb{Z})^\times \xrightarrow{\chi_0} \mathbb{C}^\times$.

(2) $(a, m) = 1, a \equiv 1 (\operatorname{mod} d)$, then $\chi(a) = 1$.

(3) $(a, m) = (a', m) = 1, a \equiv a' (\operatorname{mod} d)$, then $\chi(a) = \chi(a')$.

We call the minimal positive divisor of m such that one of the three above conditions holds the conductor of χ. If m is the conductor of χ, we call χ primitive Dirchlet character module m.

Proposition 5.1.3. Define $\varphi^*(q)$ be the number of primitive Dirchlet character module q. Then

$$\varphi^*(q) = q \prod_{p||q} (1 - 2/p) \prod_{p^2|q} (1 - 1/p)^2$$

Hence, a primitive Dirchlet character exists if and only if $q \equiv 0, 1, 3 (\operatorname{mod} 4)$.

Proposition 5.1.4. Suppose that the Dirichlet series $\alpha(s) = \sum_{n=1}^{\infty} a_n n^{-s}$ converges at the point $s = s_0$, and that $H > 0$ is an arbitrary constant. Then the series $\alpha(s)$ is uniformly convergent in the sector $S = \{s : \sigma \geq \sigma_0, |t - t_0| \leq H(\sigma - \ \sigma_0)\}$.

Proof: We may assume $s_0 = 0$. By Abel's Lemma, it suffice to show

$$\sum_{M<n\leq M+N} |n^{-s} - (n+1)^{-s}|$$

is uniformly bounded. Notice that

$$\begin{aligned}\sum_{M<n\le M+N} |n^{-s}-(n+1)^{-s}| = &\sum_{M<n\le M+N} |e^{-\log(n)s}-e^{-\log(n+1)s}|\\ \le&|s|\int_{\log M}^{\log M+N} e^{-\mathrm{Re}(s)t}dt\\ \le&|s|/\mathrm{Re}(s)((M+N)^{-t}-M^{-t})\end{aligned}$$

Let σ be the real part of s.

Corollary 5.1.5. Any Dirichlet series $\alpha(s) = \sum_{n=1}^{\infty} a_n n^{-s}$ has an abscissa of convergence σ_c with the property that $\alpha(s)$ converges for all s with $\sigma > \sigma_c$, and for no s with $\sigma < \sigma_c$. Moreover, if s_0 is a point with $\sigma_0 > \sigma_c$, then there is a neighbourhood of s_0 in which $\alpha(s)$ converges uniformly.

Proposition 5.1.6. Let $A(x) = \sum_{n\le x} a_n$. If $\sigma_c < 0$, then $A(x)$ is a bounded function, and

$$\sum_{n=1}^{\infty} a_n n^{-s} = s\int_1^{\infty} A(x)x^{-s-1}dx$$

for $\sigma > 0$. If $\sigma_c \ge 0$, then

$$\sigma_c = \inf\{\sigma \ge 0 : A(x) = \mathcal{O}(x^{\sigma})\}$$

and

$$\sum_{n=1}^{\infty} a_n n^{-s} = s\int_1^{\infty} A(x)x^{-s-1}dx$$

holds for $\sigma > \sigma_c$.

Proof: Let $m = \inf\{\sigma : A(x) = \mathcal{O}(x^{\sigma})\}$. By Integration by part,(1^- means the integration region is open on the left)

$$\begin{aligned}\sum_{n=1}^{N} a_n n^{-s} = \int_{1^-}^{N} x^{-s}dA(x) = A(x)x^{-s}\big|_{1^-}^{N} - \int_{1^-}^{N} A(x)dx^{-s}\\ = A(N)N^{-s} + s\int_1^N A(x)x^{-s-1}dx\end{aligned}$$

Take $\sigma \ge 0$ with $A(x) = O(x^{\sigma})$. For all $\epsilon > 0$, take $s = \sigma + \epsilon$, we have

$$\sum_{n=1}^{N} a_n n^{-s} = O(N^{-\epsilon}) + O(\int_1^N x^{-1-\epsilon})$$

Hence $m \ge \sigma_c$. On the other hand, for all $\sigma \ge 0$ such that $\sum a_n n^{-\sigma}$ converges, since

$$\sum_{n\le x} a_n n^{-\sigma}$$

is bounded, we have

$$\sum_{n\le x} a_n = \sum_{n\le x} a_n n^{-\sigma} n^{\sigma} = O(x^{\sigma})$$

Hence $m \le \sigma_c$.

Definition 5.1.7. Then σ_a, the abscissa of absolute convergence, is the abscissa of convergence of the series $\sum_{n=1}^{\infty} |a_n| n^{-s}$, and we see that $\sum a_n n^{-s}$ is absolutely convergent if $\sigma > \sigma_a$, but not if $\sigma < \sigma_a$.

Theorem 5.1.8. $\sigma_c \leq \sigma_a \leq \sigma_c + 1$.

Theorem 5.1.9. If $\sum a_n n^{-s} = \sum b_n n^{-s}$ for all s with $\sigma > \sigma_0$ then $a_n = b_n$ for all positive integers n.

Proof: We put $c_n = a_n - b_n$, and consider $\sum c_n n^{-s}$. Suppose that $c_n = 0$ for all $n < N$. Since $\sum c_n n^{-\sigma} = 0$ for $\sigma > \sigma_0$ we may write

$$c_N = -\sum_{n>N} c_n (N/n)^{\sigma}$$

This sum is absolutely convergent for $\sigma > \sigma_0 + 1$. Since each term tends to 0 as $\sigma \to \infty$, we see that the right-hand side tends to 0 , by the principle of dominated convergence. Hence $c_N = 0$, and by induction we deduce that this holds for all N.

Theorem 5.1.10 (Landau). Let $\alpha(s) = \sum a_n n^{-s}$ be a Dirichlet series whose abscissa of convergence σ_c is finite. If $a_n \geq 0$ for all n, and $\alpha(s)$ has a holomorphic continuation in the domain $\mathcal{D} = \{s : \mathrm{Re}(s) > \sigma_c\} \cup \{|s - \sigma_c| < \delta\}$ except the point $s = \sigma_c$, then σ_c is a singularity of the function $\alpha(s)$.

Proof: By replacing a_n by $a_n n^{-\sigma_c}$, we may assume that $\sigma_c = 0$. Suppose that $\alpha(s)$ is analytic at $s = 0$, so that $\alpha(s)$ is analytic in the domain $\mathcal{D} = \{s : \sigma > 0\} \cup \{|s| < \delta\}$ if $\delta > 0$ is sufficiently small. We expand $\alpha(s)$ as a power series at $s = 1$:

$$\alpha(s) = \sum_{k=0}^{\infty} c_k (s-1)^k$$

The coefficients c_k can be calculated by

$$c_k = \frac{\alpha^{(k)}(1)}{k!} = \frac{1}{k!} \sum_{n=1}^{\infty} a_n (-\log n)^k n^{-1}$$

Since $\alpha(s)$ is analytic in $\mathcal{D}$, the radius of convergence is at least $\sqrt{1+\delta^2} = 1 + \delta'$, say. That is,

$$\alpha(s) = \sum_{k=0}^{\infty} \frac{(1-s)^k}{k!} \sum_{n=1}^{\infty} a_n (\log n)^k n^{-1}$$

for $|s-1| < 1 + \delta'$. If $s < 1$ then all terms above are non-negative. Since series of non-negative numbers may be arbitrarily rearranged, for $-\delta' < s < 1$ we may interchange the summations over k and n to see that

$$\begin{aligned} \alpha(s) &= \sum_{n=1}^{\infty} a_n n^{-1} \sum_{k=0}^{\infty} \frac{(1-s)^k (\log n)^k}{k!} \\ &= \sum_{n=1}^{\infty} a_n n^{-1} \exp((1-s)\log n) = \sum_{n=1}^{\infty} a_n n^{-s} \end{aligned}$$

Hence this last series converges at $s = -\delta'/2$, contrary to the assumption that $\sigma_c = 0$. Thus $\alpha(s)$ is not analytic at $s = 0$.

Theorem 5.1.11 (Euler Product)**.** $f : \mathbb{Z} \to \mathbb{C}$ is multiplicative(for all $(m, n) = 1$, $f(mn) = f(m)f(n)$). If

$$\sum_p \sum_{v \geq 1} |\frac{f(p^v)}{p^{vs}}| < \infty$$

then

$$\sum_{n=1}^{\infty} a_n n^{-s}$$

converges and

$$\sum_{n=1}^{\infty} a_n n^{-s} = \sum_p \sum_{v \geq 1} \frac{f(p^v)}{p^{vs}}$$

Proposition 5.1.12. For non-principal Dirchlet character χ module m, the abscissa of convergence for Dirchlet L-function

$$\sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$$

is 0. And for principal Dirchlet character χ, the abscissa of convergence is 1.

Proposition 5.1.13. For all $\mathrm{Re}(s) > 1$, we have Euler product

$$L(s, \chi) = \prod_p \left(1 - \frac{\chi(p)}{p^s}\right)^{-1}$$

Proposition 5.1.14. χ is a Dirchlet character module m induced by a primitive Dirchlet character χ' module m', we have

$$L(s, \chi) = L(s, \chi') \prod_{p|m} (1 - \chi'(p)p^{-s})$$

5.2 Artin L-Functions

Definition 5.2.1. Let L/K be a Galois extension of finite algebraic number fields with Galois group $G = \mathrm{Gal}(L/K)$. Let $G_{\mathfrak{P}}$ be the decomposition group and $I_{\mathfrak{P}}$ the inertia group of $\mathfrak{P}$ over $\mathfrak{p}$. Then we have a canonical isomorphism

$$G_{\mathfrak{P}}/I_{\mathfrak{P}} \simeq \mathrm{Gal}(\kappa(\mathfrak{P})/\kappa(\mathfrak{p}))$$

The factor group $G_{\mathfrak{P}}/I_{\mathfrak{P}}$ is therefore generated by the Frobenius automorphism $\varphi_{\mathfrak{P}}$ whose image in $\mathrm{Gal}(\kappa(\mathfrak{P})/\kappa(\mathfrak{p}))$ is the q-th power map $x \mapsto x^q$, where $q = |\kappa(\mathfrak{p})|$.

Representation ρ and Frobenious automorphism $\varphi_{\mathfrak{P}}$ naturally induce an endomorphism on $V^{I_{\mathfrak{P}}}$ and we still denote it by $\varphi_{\mathfrak{P}}$. Consider the determinant of its characteristic polynomial

$$\det\left(1 - \varphi_{\mathfrak{P}} t; V^{I_{\mathfrak{P}}}\right) \in \mathbb{C}[t]$$

and we can check this polynomial is independent of the choice of prime ideals over $\mathfrak{p}$.

Then, we may define Artin L-Functions associated to representation ρ and Galois extension L/K to be

$$\mathcal{L}(L/K,\rho,s)=\prod_{\mathfrak{p}}\frac{1}{\det(1-\varphi_{\mathfrak{P}}\mathfrak{N}(\mathfrak{p})^{-s};V^{I_{\mathfrak{P}}})}$$

Proposition 5.2.2. The Artin L-series converges absolutely and uniformly in the half-plane $\mathrm{Re}(s)\geq 1+\delta$, for any $\delta>0$. It thus defines an analytic function on the half-plane $\mathrm{Re}(s)>1$. This is because,

$$\det\left(1-\varphi_{\mathfrak{P}}\mathfrak{N}(\mathfrak{p})^{-s};V^{I_{\mathfrak{P}}}\right)=\prod_{i=1}^{d}\left(1-\varepsilon_i\mathfrak{N}(\mathfrak{p})^{-s}\right)$$

where ε_i are roots of unity and $d=\dim V^{I_{\mathfrak{P}}}$.

Example 5.2.3 (Artin L-function for cyclotomic extension)**.** Let $L=\mathbb{Q}(\zeta_m), K=\mathbb{Q}$, then $G=\mathrm{Gal}(L/K)\simeq(\mathbb{Z}/m\mathbb{Z})^{\times}$.

$$\begin{tikzcd}
\mathbb{Q}(\zeta_m) & 1 \arrow[d] \\
\mathbb{Q}(\zeta_n) \arrow[u, "\varphi(p^\alpha)"'] & I_p=\{a:(a,p)=1,a\equiv 1(\mathrm{mod}\,n)\} \arrow[d] \\
Z_p \arrow[u, "\mathrm{ord}_n(p)"] & D_p=\left\{a:(a,p)=1,a\equiv p^k(\mathrm{mod}\,n)\right\} \arrow[d] \\
\mathbb{Q} \arrow[u, "\varphi(n)/\mathrm{ord}_n(p)"] & (\mathbb{Z}/m\mathbb{Z})^{\times}
\end{tikzcd}$$

Let χ be a primitive Dirchlet character and it's natural to view it as a representation of Galois group of cyclotomic field. Notice that χ is nontrivial on I_p, $V^{I_{\mathfrak{P}}}$ will degenerate when $I_{\mathfrak{P}}$ is ramified. Hence

$$\mathcal{L}(\mathbb{Q}(\zeta_m)/\mathbb{Q},\chi,s)=L(s,\chi)$$

Proposition 5.2.4. L/K be a Galois extension and let $G = \mathrm{Gal}(L/K)$.

(1) For the trivial represention $\mathbf{1}$ of G, one has

$$\mathcal{L}(L/K, \mathbf{1}, s) = \zeta_K(s)$$

(2) If ρ, ρ' are two representations of G, then

$$\mathcal{L}\left(L/K, \rho \oplus \rho', s\right) = \mathcal{L}(L/K, \rho', s)\mathcal{L}\left(L/K, \chi', s\right)$$

(3) For a bigger Galois extension $L'/K, L' \supseteq L \supseteq K$, and a representation ρ of $\mathrm{Gal}(L/K)$, notice that $G \xrightarrow{\pi} G/\mathrm{Gal}(L/M) \simeq \mathrm{Gal}(L/K)$, ρ induces a representation $\rho \circ \pi$ of G. Then, we have

$$\mathcal{L}\left(L'/K, \rho \circ \pi, s\right) = \mathcal{L}(L/K, \rho, s).$$

(4) If M is an intermediate field, $L \supseteq M \supseteq K$, and (ρ, V) is a representation of $H = \mathrm{Gal}(L/M)$, then

$$\mathcal{L}(L/M, \rho, s) = \mathcal{L}\left(L/K, \mathrm{Ind}_H^G(\rho), s\right).$$

Proof: (1): trivial

(2): If $(\rho, V), (\rho', V')$ are representations of G, we have

$$\begin{aligned}\det\left(1 - \varphi_{\mathfrak{P}}t; (V \oplus V')^{I_{\mathfrak{P}}}\right) &= \det\left(1 - \varphi_{\mathfrak{P}}t; V^{I_{\mathfrak{P}}} \oplus (V')^{I_{\mathfrak{P}}}\right) \\ &= \det\left(1 - \varphi_{\mathfrak{P}}t; V^{I_{\mathfrak{P}}}\right)\det\left(1 - \varphi_{\mathfrak{P}t}; (V')^{I_{\mathfrak{P}}}\right).\end{aligned}$$

This yields (2).

(3): Let $\mathfrak{P}', \mathfrak{P}|, \mathfrak{p}$ be prime ideals of L', L, K, each lying above the next. The projection $\mathrm{Gal}\left(L'/K\right) \to G(L/K)$ induces surjective homomorphisms

$$G_{\mathfrak{P}'} \longrightarrow G_{\mathfrak{P}}, I_{\mathfrak{P}'} \longrightarrow I_{\mathfrak{P}}, G_{\mathfrak{P}'}/I_{\mathfrak{P}'} \longrightarrow G_{\mathfrak{P}}/I_{\mathfrak{P}}$$

of the decomposition and inertia groups. To show $G_{\mathfrak{P}'} \longrightarrow G_{\mathfrak{P}}$ is surjective, it suffices to notice that $\mathrm{Gal}(L'/L)$ acts transitively on the prime ideals of $\mathcal{O}_{L'}$ lying over $\mathfrak{P}$.

The latter maps the Frobenius automorphism $\varphi_{\mathfrak{P}'}$ to the Frobenius automorphism $\varphi_{\mathfrak{P}}$ so that $\left(\varphi_{\mathfrak{P}'}, V^{I_{\mathfrak{P}'}}\right) = \left(\varphi_{\mathfrak{P}}, V^{I_{\mathfrak{P}}}\right)$. Hence,

$$\det\left(1 - \varphi_{\mathfrak{P}'}t; V^{I_{\mathfrak{P}'}}\right) = \det\left(1 - \varphi_{\mathfrak{P}}t; V^{I_{\mathfrak{P}}}\right) \text{ in } \mathbb{C}[t]$$

This yields (3).

(4): Firstly, Let $\mathfrak{p}$ be a prime ideal of K, $\mathfrak{q}_1, \ldots, \mathfrak{q}_g$ the various prime ideals of M above $\mathfrak{p}$, and $\mathfrak{P}_i$ a prime ideal of L above $\mathfrak{q}_i, i = 1, \ldots, g$. We introduce several notations as follow:

- $D_{\mathfrak{P}_\mathrm{i}/\mathfrak{q}}$ be the decomposition group of $\mathfrak{P}_\mathrm{i}$ over $\mathfrak{q}$
- $I_{\mathfrak{P}_\mathrm{i}/\mathfrak{q}}$ be the inertia group of $\mathfrak{P}_\mathrm{i}$ over $\mathfrak{q}$

- $D_{\mathfrak{P}_i/\mathfrak{q}_i} = H \cap D_{\mathfrak{P}_i/\mathfrak{q}}$ be the decomposition group of $\mathfrak{P}_i$ over $\mathfrak{q}_i$
- $I_{\mathfrak{P}_i/\mathfrak{q}_i} = H \cap I_{\mathfrak{P}_i/\mathfrak{q}}$ be the inertia group of $\mathfrak{P}_i$ over $\mathfrak{q}_i$
- $e_i = e(\mathfrak{q}_i|\mathfrak{q})$ be the ramified degree of $\mathfrak{q}_i$ over $\mathfrak{q}$
- $f_i = f(\mathfrak{q}_i|\mathfrak{q})$ be the residue field degree of $\mathfrak{q}_i$ over $\mathfrak{q}$
- $n = [M : K]$ be the degree of the extension M/K
- $\tau_i \in G$ an element such that $\tau_i(\mathfrak{P}_1) = \mathfrak{P}_i$ with $\tau_1 = \mathrm{id}$
- $\omega_{i,1}, \ldots, \omega_{i,e_i}$ be a left coset representatives of $I_{\mathfrak{P}_i/\mathfrak{q}}/I_{\mathfrak{P}_i/\mathfrak{q}_i}$
- $\varphi_{\mathfrak{P}_i/\mathfrak{q}} \in D_{\mathfrak{P}_i/\mathfrak{q}}$ a element such that its image in $D_{\mathfrak{P}_i/\mathfrak{q}}/I_{\mathfrak{P}_i/\mathfrak{q}}$ be the Frobenious Automorphism. In addition, we may assume $\tau_i \varphi_{\mathfrak{P}_1/\mathfrak{q}} \tau_i^{-1} = \varphi_{\mathfrak{P}_i/\mathfrak{q}}$
- $V^{I_{\mathfrak{P}_i/\mathfrak{q}_i}}$ the invariant subspace of V under the action of $I_{\mathfrak{P}_i/\mathfrak{q}_i}$

$$\begin{tikzcd}
L & 1 \arrow[d] & \mathfrak{P}_1 \arrow[loop above, "\tau_1"] \arrow[r, "\tau_2"'] \arrow[rrr, bend left, "\tau_g"] & \mathfrak{P}_2 & & \mathfrak{P}_g \\
M \arrow[u] & H \arrow[d] & \mathfrak{q}_1 \arrow[u] & \mathfrak{q}_2 \arrow[u] & \cdots & \mathfrak{q}_g \arrow[u] \\
K \arrow[u, "n"] & G & & \mathfrak{q} \arrow[ul, "{e_1,f_1}"] \arrow[u] \arrow[urr, "{e_g,f_g}"'] & &
\end{tikzcd}$$

Then we have

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

With notations above, we have the following diagram which descirbes the relationship between $D_{\mathfrak{P}_i/\mathfrak{q}}, I_{\mathfrak{P}_i/\mathfrak{q}}, D_{\mathfrak{P}_i/\mathfrak{q}_i}, I_{\mathfrak{P}_i/\mathfrak{q}_i}$:

$$\begin{tikzcd}
& D_{\mathfrak{P}_i/\mathfrak{q}} & \\
D_{\mathfrak{P}_i/\mathfrak{q}_i} \arrow[ur, "f_i e_i"] & & I_{\mathfrak{P}_i/\mathfrak{q}} \arrow[ul, "f_i f(\mathfrak{P}_i|\mathfrak{q}_i)"', "\text{normal}"] \\
& I_{\mathfrak{P}_i/\mathfrak{q}_i} \arrow[ul, "f(\mathfrak{P}_i|\mathfrak{q}_i)"', "\text{normal}"] \arrow[ur, "e_i"'] &
\end{tikzcd}$$

Since $I_{\mathfrak{P}_i/\mathfrak{q}}$ is a normal subgroup of $D_{\mathfrak{P}_i/\mathfrak{q}}$, $D_{\mathfrak{P}_i/\mathfrak{q}_i} I_{\mathfrak{P}_i/\mathfrak{q}}$ is a subgroup of $D_{\mathfrak{P}_i/\mathfrak{q}}$. Moreover, we claim that $[D_{\mathfrak{P}_i/\mathfrak{q}} : D_{\mathfrak{P}_i/\mathfrak{q}_i} I_{\mathfrak{P}_i/\mathfrak{q}}] = f_i$. This is because, since $D_{\mathfrak{P}_i/\mathfrak{q}_i} \cap I_{\mathfrak{P}_i/\mathfrak{q}} = D_{\mathfrak{P}_i/\mathfrak{q}} \cap H \cap I_{\mathfrak{P}_i/\mathfrak{q}} = I_{\mathfrak{P}_i/\mathfrak{q}_i}$, by Algebra 1.2.1, we have

$$[D_{\mathfrak{P}_i/\mathfrak{q}} : D_{\mathfrak{P}_i/\mathfrak{q}_i} I_{\mathfrak{P}_i/\mathfrak{q}}] = \frac{|D_{\mathfrak{P}_i/\mathfrak{q}}||I_{\mathfrak{P}_i/\mathfrak{q}_i}|}{|D_{\mathfrak{P}_i/\mathfrak{q}_i}||I_{\mathfrak{P}_i/\mathfrak{q}}|} = f_i$$

Hence, $\varphi_{\mathfrak{P}_i/\mathfrak{q}}^{f_i} = \varphi_{\mathfrak{P}_i/\mathfrak{q}_i} \psi_i$ for some $\varphi_{\mathfrak{P}_i/\mathfrak{q}_i} \in D_{\mathfrak{P}_i/\mathfrak{q}_i}$ and $\psi_i \in I_{\mathfrak{P}_i/\mathfrak{q}}$.

We claim that the image of $\varphi_{\mathfrak{P}_i/\mathfrak{q}_i}$ in $D_{\mathfrak{P}_i/\mathfrak{q}_i}/I_{\mathfrak{P}_i/\mathfrak{q}_i}$ is the Frobenious Automorphism. This is because, by definition of $I_{\mathfrak{P}_i/\mathfrak{q}}$, for all $x \in \mathcal{O}_L$, $\psi_i(x) \equiv x(\operatorname{mod} \mathfrak{P}_i)$, then

$$\varphi_{\mathfrak{P}_i/\mathfrak{q}_i}(x) \equiv \varphi_{\mathfrak{P}_i/\mathfrak{q}_i}\psi_i(x) \equiv \varphi^{f_i}_{\mathfrak{P}_i/\mathfrak{q}}(x) \equiv x^{\mathfrak{N}(\mathfrak{q}_i)}(\operatorname{mod} \mathfrak{P}_i).$$

Now, we show that $\tau_i^{-1}\varphi^j_{\mathfrak{P}_i/\mathfrak{q}}\omega_{i,k}, i = 1, \ldots, g, j = 0, \ldots, (f_i - 1), k = 1, \ldots, e_i$ be n distinct element of G and form a left coset representatives of G/H. Notice that G contains disjoint union of some parts of its right coset of $G/D_{\mathfrak{P}_1/\mathfrak{q}}$

$$G \supset \bigcup_{i=1}^{g} D_{\mathfrak{P}_1/\mathfrak{q}}\tau_i$$

and

$$\begin{aligned}
\bigcup_{i=1}^{g} D_{\mathfrak{P}_1/\mathfrak{q}}\tau_i^{-1} &= \bigcup_{i=1}^{g} \tau_i^{-1} D_{\mathfrak{P}_i/\mathfrak{q}} \\
&= \bigcup_{i=1}^{g}\bigcup_{j=1}^{f_i-1} \tau_i^{-1}\varphi^j_{\mathfrak{P}_i/\mathfrak{q}} I_{\mathfrak{P}_i/\mathfrak{q}} \\
&= \bigcup_{i=1}^{g}\bigcup_{j=1}^{f_i-1}\bigcup_{k=1}^{e_i} \tau_i^{-1}\varphi^j_{\mathfrak{P}_i/\mathfrak{q}}\omega_{i,k} I_{\mathfrak{P}_i/\mathfrak{q}_i} \\
&\subset \bigcup_{i=1}^{g}\bigcup_{j=1}^{f_i-1}\bigcup_{k=1}^{e_i} \tau_i^{-1}\varphi^j_{\mathfrak{P}_i/\mathfrak{q}}\omega_{i,k} H
\end{aligned}$$

And for all $\sigma \in G$, assume $\sigma(\mathfrak{P}_1) \cap \mathcal{O}_M = \mathfrak{q}_i$, there's $h \in H$ such that $\tau_i^{-1} g\sigma \in D_{\mathfrak{P}_1/\mathfrak{q}}$. Then, $\sigma^{-1} \in D_{\mathfrak{P}_1/\mathfrak{q}}\tau_i^{-1}H$. This shows $\tau_i^{-1}\varphi^j_{\mathfrak{P}_i/\mathfrak{q}}\omega_{i,k}, i = 1, \ldots, g, j = 0, \ldots, (f_i - 1), k = 1, \ldots, e_i$ be n distinct element of G and form a left coset representatives of G/H.

By the claim above, for all $x \in \mathbb{C}[G] \otimes_{\mathbb{C}[H]} V$, there's unique $v_{i,j,k} \in V$ such that

$$x = \sum_{i=1}^{g}\sum_{j,k} \tau_i^{-1}\varphi^j_{\mathfrak{P}_i/\mathfrak{q}}\omega_{i,k} \otimes v_{i,j,k}$$

It's easy to check that

$$x \in (\mathbb{C}[G] \otimes_{\mathbb{C}[H]} V)^{I_{\mathfrak{P}_1/\mathfrak{q}}}$$

if and only if

$$v_{i,j,k} \in V^{I_{\mathfrak{P}_i/\mathfrak{q}_i}} \text{ and for all } k = 1, \ldots, e_i \ v_{i,j,k} = v_{i,j,1}.$$

Then,

$$\dim_{\mathbb{C}}(\mathbb{C}[G] \otimes_{\mathbb{C}[H]} V)^{I_{\mathfrak{P}_1/\mathfrak{q}}} = \sum_{i=1}^{g} f_i \dim_{\mathbb{C}} V^{I_{\mathfrak{P}_i/\mathfrak{q}_i}}$$

To show

$$\mathcal{L}(L/M, \rho, s) = \mathcal{L}\left(L/K, \operatorname{Ind}_H^G(\rho), s\right),$$

it suffices to check the following identity in $\mathbb{C}[t]$:

$$\det(\mathrm{id} - t\varphi_{\mathfrak{P}_1/\mathfrak{q}}; (\mathbb{C}[G] \otimes_{\mathbb{C}[H]} V)^{I_{\mathfrak{P}_1/\mathfrak{q}}}) = \prod_{i=1}^{g} \det(\mathrm{id} - t^{f_i}\varphi_{\mathfrak{P}_i/\mathfrak{q}_i}; V^{I_{\mathfrak{P}_i/\mathfrak{q}_i}})$$

Assume $v_1, \ldots, v_{r_i}$ with $r_i = \dim_{\mathbb{C}} V^{I_{\mathfrak{P}_i/\mathfrak{q}_i}}$ be a basis of $V^{I_{\mathfrak{P}_i/\mathfrak{q}_i}}$ and let

$$\varphi_{\mathfrak{P}_i/\mathfrak{q}_i}(v_1, \ldots, v_{r_i}) = (v_1, \ldots, v_{r_i})A_i$$

Then, $\det(\mathrm{id} - t^{f_i}\varphi_{\mathfrak{P}_i/\mathfrak{q}_i}; V^{I_{\mathfrak{P}_i/\mathfrak{q}_i}}) = \det(E - t^{f_i}A_i)$.

Notice that

$$\begin{aligned}
&\varphi_{\mathfrak{P}_1/\mathfrak{q}}(\mathcal{A} = \left(\sum_k \tau_i^{-1}\varphi^j_{\mathfrak{P}_i/\mathfrak{q}}\omega_{i,k} \otimes v_s\right), (s,j) = (1,1), \ldots, (r_i, 1), (1,2), \ldots, (r_i, f_i)) \\
=&\mathcal{A}\begin{pmatrix} 0 & 0 & \cdots & 0 & A_i \\ E & 0 & \cdots & 0 & 0 \\ 0 & E & \cdots & 0 & 0 \\ 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & \cdots & E & 0 \end{pmatrix}
\end{aligned}$$

Hence,

$$\det(\mathrm{id} - t\varphi_{\mathfrak{P}_1/\mathfrak{q}}; (\mathbb{C}[G] \otimes_{\mathbb{C}[H]} V)^{I_{\mathfrak{P}_1/\mathfrak{q}}}) = \prod_{i=1}^{g} \det\begin{pmatrix} E & 0 & \cdots & 0 & -tA_i \\ -tE & E & \cdots & 0 & 0 \\ 0 & -tE & \cdots & 0 & 0 \\ 0 & 0 & \cdots & E & 0 \\ 0 & 0 & \cdots & -tE & E \end{pmatrix}$$

$$= \prod_{i=1}^{g} \det(E - t^{f_i}A_i) = \prod_{i=1}^{g} \det(\mathrm{id} - t^{f_i}\varphi_{\mathfrak{P}_i/\mathfrak{q}_i}; V^{I_{\mathfrak{P}_i/\mathfrak{q}_i}})$$

Chapter 6

Modular Forms