Algebraic Number Theory

Guanghua Ji
School of Mathematics
Shandong University

June 30, 2012

Preface

This is a standard graduate course in algebraic number theory. The only prerequisites listed for this course are elementary number theory and abstract algebra. In this note we shall limit our attention essentially to algebra number fields (a finite extension of the rational number field), although overwhelming majority of the results also hold for for function fields (fields of algebraic functions over a finite field). The main reference book is H.P.F. Swinnerton-Dyer's book *a brief guide to algebraic number theory.* We will cover:

- Three fundamental theorems of ideal theory
- Hilbert's theory of Galois extension
- Valuation theory and the arithmetic of local fields
- Ramification theory
- Adele, idele and harmonic analysis on adele groups
- Dedekind zeta functions, Hecke L-funtions and Tate's thesis
- Artin L-functions

I would like to thank all the students who enjoined the course. Some theorems of this lecture notes were taken by students. The course webpage is *www.prime.sdu.edu.cn/ghji/algebraicnumbertheory.htm.*

Please feel free to put a copy. Use them at your own risk. Any comments or corrections about this notes are always welcomed at *guanghuaji@gmail.com.*

Guanghua Ji
School of Mathematics
Shandong University
Jinan, Shandong 250100
www.prime.sdu.edu.cn/ghji/guanghuaji.htm

Contents

Chapter 1

Ideal Theory

1.1 The Ring of Integers

1.1.1 Basic concepts

A complex number α is called *algebraic number* if it is a root of some polynomial with coefficients in $\mathbb{Q}$. A complex number α is called *algebraic integer* if it is a root of some monic polynomial with coefficients in $\mathbb{Z}$. An *algebraic number field* k is a finite algebraic extension of the rational number $\mathbb{Q}$. Let $\overline{\mathbb{Q}}$ be the algebraic closure of $\mathbb{Q}$, i.e., the set of all algebraic numbers.

Recall: Algebraic extensions Take $\alpha \in \overline{\mathbb{Q}}$. (1), $\mathbb{Q}(\alpha) = \mathbb{Q}[\alpha]$. (2), There exists a unique polynomial $p(x) \in \mathbb{Q}[x]$ which is monic, irreducible and of smallest positive degree such that $p(\alpha) = 0$. Furthermore, if $f(x) \in \mathbb{Q}[x]$ and $f(\alpha) = 0$, then $p(x)|f(x)$. $p(x)$ is called the minimal polynomial of α; the degree of $p(x)$ is called the degree of α and is denoted $\deg(\alpha)$. (3), The roots of the minimal polynomial $p(x)$ of α are called conjugates of α. α has $\deg(p(x))$ conjugates. Conjugates of α have the same minimal polynomial.

For the detailed proofs, we refer the reader to [1] or [5].

Theorem 1.1. *Let $\alpha \in \overline{\mathbb{Q}}$. Then the following statements are equivalent:*

(1), α is an algebraic integer.

(2), The minimal polynomial of α over $\mathbb{Q}$ has coefficients in $\mathbb{Z}$.

(3), $\mathbb{Z}[\alpha]$ is a finitely generated $\mathbb{Z}$-module.

(4), There exists a nonzero finite generated $\mathbb{Z}$-submodule M of $\mathbb{C}$ such that $\alpha M \subset M$.

Proof. (1) $\Rightarrow$ (2) α is an algebraic integer, then there exists a monic polynomial $f(x) \in \mathbb{Z}[x]$, such that $f(\alpha) = 0$. And let $p(x) \in \mathbb{Q}[x]$ be the minimal polynomial of α, so we have $p(x)|f(x)$, using Gauss Lemma(also by Exercise 1.3), $p(x) \in \mathbb{Z}(x)$ as required.

(2) $\Rightarrow$ (3) Suppose that $f(x) = x^m + c_1 x^{m-1} + \cdots + c_m \in \mathbb{Z}[x]$ is the minimal polynomial of α. Then $\alpha^m = -c_1\alpha^{m-1} - c_2\alpha^{m-2} - \cdots - c_m$. Hence for any integer N, we have $\alpha^N \in \mathbb{Z}\alpha^{m-1} \oplus \cdots \oplus \mathbb{Z}$. It gives that α^N is in the $\mathbb{Z}$-module generated by $1, \alpha, \ldots, \alpha^{m-1}$, so $\mathbb{Z}[\alpha]$ is a finite $\mathbb{Z}$-module.

(3) $\Rightarrow$ (4) Let $M = \mathbb{Z}[\alpha]$, (4) holds obviously.

(4) $\Rightarrow$ (1) Let $x_1, \cdots, x_r$ generate M over $\mathbb{Z}$. So $M \subset \mathbb{Z}x_1 \oplus \cdots \oplus \mathbb{Z}x_r$. By assumption, for $i = 1, \cdots, r$, we have

$$\alpha x_i = \sum_{j=1}^{r} c_{ij} x_j, c_{ij} \in \mathbb{Z},$$

that is,

$$\alpha \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_r \end{pmatrix} = (c_{ij}) \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_r \end{pmatrix} \Longleftrightarrow (\alpha I - C) \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_r \end{pmatrix} = 0$$

where $C = (c_{ij})$. Since not all of $x_1, \ldots, x_r$ can vanish, then $\det(\alpha I - C) = 0$. Take $f(x) = \det(xI - C)$. Then $f(x)$ is a monic polynomial in $\mathbb{Z}[x]$ such that $f(\alpha) = 0$. Thus α is an algebraic integer. $\square$

Corollary 1.2. *The set $\overline{\mathbb{Z}}$ of all algebraic integers is a ring. In particular, the ring of integers of a number field k is the ring $\mathfrak{o}_k = k \cap \overline{\mathbb{Z}}$. And $\mathbb{Q} \cap \mathfrak{o}_k = \mathbb{Q} \cap \overline{\mathbb{Z}} = \mathbb{Z}$.*

Proof. Suppose $\alpha, \beta \in \overline{\mathbb{Z}}$, then $\mathbb{Z}[\alpha]$ and $\mathbb{Z}[\beta]$ are finite generated abelian groups. And let $\{1, \alpha, \cdots, \alpha^m\}$ be a basis of $\mathbb{Z}[\alpha]$ and $\{1, \beta, \ldots, \beta^n\}$ be a basis of $\mathbb{Z}[\beta]$. It is clear that $\{\alpha^i\beta^j | 0 \le i \le m, 0 \le j \le n\}$ spans

$$\mathbb{Z}[\alpha, \beta] = \{f(\alpha, \beta) | f(x, y) \in \mathbb{Z}[x, y]\},$$

and then $\mathbb{Z}[\alpha, \beta]$ is a finite generated $\mathbb{Z}$-module, $\alpha \pm \beta, \alpha\beta \in \mathbb{Z}[\alpha, \beta]$. Hence $\alpha \pm \beta, \alpha\beta$ are algebraic integers, and the set $\overline{\mathbb{Z}}$ of all algebraic integers is a ring. $\square$

1.1.2 Norm, trace and discriminant

Let K/k be a finite separable field extension of degree $[K : k] = n$, and let τ be an embedding of k in $\mathbb{C}$, that is, a monomorphism. Then τ extends to exactly n embeddings σ of K of into $\mathbb{C}$ such that the restriction $\sigma|_k = \tau$. In particular, taking τ to be the identity mapping on k, there are exactly

n distinct k-embeddings of K into $\mathbb{C}$. For the detailed proofs, we refer the reader to [1] or [5].

Let K/k be any field extension of degree $[K : k] = n$, and let $x_1, ..., x_n$ be a basis for K as a k-vetor space. For any $\alpha \in K$, then left multiplication defines a k-linear transformation

$$\ell_\alpha : x \mapsto \alpha x.$$

There exists a_{ij} in k such that the matrix $A = (a_{ij})$

$$\ell_\alpha(x_1, \ldots, x_n) = (\alpha x_1, \ldots, \alpha x_n) = (x_1, \ldots, x_n)A.$$

The characteristic polynomial of ℓ_α is

$$f_\alpha(\lambda) = \det(\lambda I - A) = \lambda^n + a_{n-1}\lambda^{n-1} + \cdots + a_0 \in k[X].$$

Denote the *norm* and *trace* of α from K to k by

$$\begin{aligned} \mathrm{Tr}_{K/k}(\alpha) &= tr(\ell_\alpha) = tr(A) = -a_{n-1} \\ \mathrm{N}_{K/k}(\alpha) &= \det(\ell_\alpha) = \det(A) = (-1)^n a_0. \end{aligned}$$

Note that the trace and norm of α are independent of the choice of the basis for K over k.

Obviously, we can obtain the following properties for their definitions: for any $a, b \in k$ and $\alpha, \beta \in K$,

$$\begin{aligned} &(1), \mathrm{Tr}_{K/k}(a\alpha + b\beta) = a\mathrm{Tr}_{K/k}(\alpha) + b\mathrm{Tr}_{K/k}(\beta), \\ &(2), \mathrm{N}_{K/k}(\alpha\beta) = \mathrm{N}_{K/k}(\alpha)\mathrm{N}_{K/k}(\beta), \\ &(3), \mathrm{N}_{K/k}(a\alpha) = a^n \mathrm{N}_{K/k}(\alpha), \\ &(4), \mathrm{N}_{K/k}(a) = a^n, \text{ and } \mathrm{Tr}_{K/k}(a) = na. \end{aligned}$$

Therefore, $\mathrm{N}_{K/k} : K \to k$ and $\mathrm{Tr}_{K/k} : K^\times \to k^\times$ are group homomorphisms.

Proposition 1.3. *(1), Let $p(\lambda) = \lambda^m + c_{m-1}\lambda^{m-1} + \cdots + c_0 \in k[X]$ be the minimal polynomial of $\alpha \in K$ with $[k(\alpha) : k] = m$. Then $f_\alpha(\lambda) = p(\lambda)^{\frac{n}{m}}$, $N_{K/k}(\alpha) = (-1)^n(c_0)^{n/m}$ and $Tr_{K/k}(\alpha) = -\frac{n}{m}c_{m-1}$.*

(2), Let K/k be a finite separable field extension of degree $[K : k] = n$. Let $\sigma_1, ..., \sigma_n$ be distinct k-embeddings of K. Then $f_\alpha(\lambda) = \prod_{i=1}^n (\lambda - \sigma_i\alpha)$, $N_{K/k}(\alpha) = \prod_{i=1}^n \sigma_i(\alpha)$ and $Tr_{K/k}(\alpha) = \sum_{i=1}^n \sigma_i(\alpha)$.

(3), Suppose $k \subset L \subset K$ be a tower of number fields and let $\alpha \in K$. Then $N_{L/k}(N_{K/L}(\alpha)) = N_{K/k}(\alpha)$ and $Tr_{L/k}(Tr_{K/L}(\alpha)) = Tr_{K/k}(\alpha)$.

Proof. (1) Let $f(\lambda)$ be the characteristic polynomial of α. Clearly, it follows form the definition of characteristic polynomial that

$$f(\lambda) = \lambda^n - Tr_{K/k}(\alpha)\lambda^{n-1} + \cdots + (-1)^n N_{K/k}(\alpha),$$

and

$$f(\lambda) = p(\lambda)^{[K:k(\alpha)]} = p(\lambda)^{n/m}.$$

Therefore, if $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_m$ be the roots of $p(x)$ in a splitting field counting multiplicity, then we have

$$\sum_{i=1}^{m} \alpha_i = -c_1, \ \prod_{i=1}^{m} \alpha_i = (-1)^n c_m.$$

Hence, we have

$$N_{K/k}(\alpha) = (-1)^n c_m,$$

and the trace is the negative of the coefficient of the x^{n-1} in $p(x)^{n/m}$, that is

$$Tr_{K/k}(\alpha) = \frac{n}{m} \sum_{i=1}^{m} \alpha_i = -\frac{n}{m} c_1.$$

To prove (2), we know that there are m distinct k-embeddings of $K(\alpha)$ into $\mathbb{C}$, each of them takes α to a unique conjugate α_i, and extends to exactly $\frac{n}{m}$ distinct k-embeddings of K into $\mathbb{C}$, all of which also take α to a unique conjugate α_i. Thus

$$\prod_{i=1}^{n} \sigma_i(\alpha) = (\prod_{i=1}^{m} \alpha_i)^{n/m} = N_{K/k}(\alpha),$$

and

$$\sum_{i=1}^{n} \sigma_i(\alpha) = \frac{n}{m} \sum_{i=1}^{m} \alpha_i = Tr_{K/k}(\alpha).$$

(3), Let $\sigma_1, \cdots, \sigma_m$ be the distinct embeddings of k in to K, and let $\tau_1, \cdots, \tau_n$ be the distinct embeddings of K into L. Then L/k is Galois, and each mapping σ_i and τ_j extends to an automorphism of L. Therefore it makes sense to allow the mapping to be composed. By (2),

$$N_{L/k}(N_{K/L}(\alpha)) = \prod_{i=1}^{m} \sigma_i(\prod_{j=1}^{n} \tau_j(\alpha)) = \prod_{i=1}^{m} \prod_{j=1}^{n} \sigma_i \tau_j(\alpha).$$

Now each $\sigma_i \tau_j$ is an embedding of k into L, and the number of the mappings is $mn = [k : K][K : L] = [k : K]$. Furthermore, the $\sigma_i = \tau_j$ are distinct.

For if $\sigma_j\tau_j = \sigma_k\tau_l$, hence on K, then $\sigma_i = \sigma_k$ (because $\tau_j = \tau_k = 1$ on K). Thus $i = k$, so that $\tau_j = \tau_l$ on L. But then $i = k$. Therefore, we have $N_{L/k}(N_{K/L}(\alpha)) = N_{K/k}(\alpha)$. The trace is handled the same way, with products replaced be sums. □

Let $k/\mathbb{Q}$ is a number field and $\alpha \in \mathfrak{o}_k$. Then $N_{k/\mathbb{Q}}(\alpha), \mathrm{Tr}_{k/Q}(\alpha) \in \mathbb{Z}$. Write $N(\alpha), \mathrm{Tr}(\alpha)$ for $N_{k/\mathbb{Q}}(\alpha), \mathrm{Tr}_{k/\mathbb{Q}}(\alpha)$.

Let K/k be a finite separable field extension of degree n. Let $\sigma_1, \ldots, \sigma_n$ be distinct k-embeddings of K. For $a_1, \ldots, a_n \in K$, we can define the *discriminant* of $\{a_1, \ldots, a_n\}$

$$d_{K/k}(a_1, \ldots, a_n) = (\det(\sigma_i(a_j)))^2 = \det(\mathrm{Tr}_{K/k}(a_i a_j)).$$

Proposition 1.4. *With the notation and assumptions above.*

(1), Set $d_{K/k}(1, a, \ldots, a^{n-1})$ as $d_{K/k}(a)$. Then

$$d_{K/k}(a) = \prod_{i>j}(\sigma_i(a) - \sigma_j(a))^2. \tag{1.1}$$

(2), Suppose that $\beta_i = \sum c_{ij}\alpha_j, i = 1, ..., n$, $\alpha_i, \beta \in K$ and $c_{ij} \in k$. Then

$$d_{K/k}(\beta_1, \ldots, \beta_n) = (\det(c_{ij}))^2 d_{K/k}(\alpha_1, \ldots, \alpha_n). \tag{1.2}$$

(3), Let $\alpha_1, \ldots, \alpha_n$ be a base for K as k-vector space. Then the discriminant $d_{K/k}(\alpha_1, \ldots, \alpha_n) \neq 0$.

(4), The bilinear form $(x, y) = Tr_{K/k}(xy)$ is a nondegenerate on the k-vector space K.

Recall: Bilinear forms A bilinear form $B(x, y)$ over a finite-dimensional vector space V over a field F is said to be non-degenerate when if $B(x, y) = 0$ for all $x \in V$, then $y = 0$, and if $B(x, y) = 0$ for all $y \in V$, then $x = 0$; otherwise degenerate forms. Let $e_1, \ldots, e_n$ be a basis of V. Write $\alpha = \sum a_i e_i$ and $\beta = \sum b_i e_i$ with $a_i, b_i \in F$. Then

$$B(\alpha, \beta) = \sum_{i,j} a_i b_j B(e_i, e_j)$$

and we associate to $B(x, y)$ the matrix $(B(e_i, e_j))$. A bilinear form is degenerate if and only if the matrix is singular, and accordingly degenerate forms are also called singular forms. Likewise, a nondegenerate form is one for which the associated matrix is non-singular, and accordingly nondegenerate forms are also referred to as non-singular forms. These statements are independent of the chosen basis.

Proof. Let $\sigma_i(\alpha) = \alpha_i$, where $i = 1, \ldots, n$. Then it is easy to see that

$$d_{K/k}(a) = \left(\det\left((\sigma_i\alpha^{j-1})_{\substack{1\le i\le n\\ 1\le j\le n}}\right)\right)^2 = \left(\det\left((\alpha_i^{j-1})_{\substack{1\le i\le n\\ 1\le j\le n}}\right)\right)^2.$$

which is the Vandermonde matrix, and so

$$= \prod_{j<i}(\sigma_i(a) - \sigma_j(a))^2 = (-1)^{n(n-1)/2} \prod_{i \neq j}(\sigma_i(a) - \sigma_j(a)).$$

(2) Since $\beta_i = \sum c_{ij}\alpha_j, i = 1, ..., n$, we have

$$\begin{pmatrix} \beta_1 \\ \beta_2 \\ \vdots \\ \beta_n \end{pmatrix} = \begin{pmatrix} c_{11} & c_{12} & \cdots & c_{1n} \\ c_{21} & c_{22} & \cdots & c_{2n} \\ \vdots & \vdots & & \vdots \\ c_{n1} & c_{n2} & \cdots & c_{nn} \end{pmatrix} \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{pmatrix}.$$

Therefore,

$$\begin{aligned} d_{K/k}(\beta_1, \ldots, \beta_n) &= \det(\sigma_i\beta_j)^2 = \det\left(\sigma_i\left(\sum c_{ij}\alpha_j\right)\right)^2 \\ &= \det\left(\sum c_{ij}\sigma_i\alpha_j\right)^2 = (\det(c_{ij})\det(\sigma_i\alpha_j))^2 \\ &= (\det(c_{ij}))^2 d_{K/k}(\alpha_1, \ldots, \alpha_n) \end{aligned}$$

as requires.

(3) and (4), We first show (4), that is, the bilinear form $(x, y) = Tr_{K/k}(xy)$ is a nondegenerate. Let θ be a primitive element for K/k, that is, $K = k[\theta]$. Then $1, \theta, \ldots, \theta^{n-1}$ is a basis with respect to which form (x, y) is given by the matrix $M = Tr_{K/k}(\theta^{i-1}\theta^{j-1})_{i,j=1,\ldots,n}$. It is nondegenerate because, for $\theta_i = \sigma_i\theta$, we have

$$\det(M) = d(1, \theta, \ldots, \theta^{n-1}) = \prod_{i<j}(\theta_i - \theta_j)^2 \neq 0.$$

If $\alpha_1, \ldots, \alpha_n$ be an arbitrary basis of K/k, then bilinear form (x, y) with respect to this basis is given by the matrix $M = (Tr_{K/k}(\alpha_i\alpha_j))$. From the above it follows that $d(\alpha_1 \ldots, \alpha_n) = \det(M) \neq 0$.

□

Let $k = \mathbb{Q}(\gamma)$ be a number field with $[k : \mathbb{Q}] = n$, and let $f(x) \in \mathbb{Q}[x]$ be the minimal polynomial of γ over $\mathbb{Q}$. Then there are r_1 real embeddings and r_2 pair complex embeddings where $r_1 + 2r_2 = n$. We say that k is *totally real* if $r_1 = n$ or *totally imaginary* if $r_1 = 0$. The couple (r_1, r_2) is called the *signature* of k.

Recall: Finitely generated abelian groups A group G is finitely generated if there exists $g_1, \ldots, g_n \in G$ such that every element of G can be expressed as a finite product of positive or negative powers of the g_i. An abelian group G is said to free if

there exist elements $g_1, \ldots, g_n \in G$ such that every element of G can be written uniquely in the form $x = k_1 g_1 + \cdots + k_n g_n$ where $k_i \in \mathbb{Z}$. The set consisting of $\{g_1, \ldots, g_n\}$ is said to be a basis of G and n is called the rank of G. If G is a finitely generated abelian group, so is the subgroup $H \leq G$. Let G be a finitely generated abelian group. Then there is an isomorphism

$$G \cong \underbrace{\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}}_{r} \oplus (\mathbb{Z}/d_1\mathbb{Z}) \oplus \cdots \oplus (\mathbb{Z}/d_s\mathbb{Z}),$$

where $d_1 > 1$ and $d_1 | d_2 | \cdots | d_s$. Furthermore, the integers r, s and d_i are uniquely determined by G. For the detailed proofs, we refer the reader to [1] or [5].

Theorem 1.5. *Let k be a number field with $[k : \mathbb{Q}] = n$. The ring of integers $\mathfrak{o}_k$ is a lattice in k, i.e., $\mathfrak{o}_k$ spans k and $\mathfrak{o}_k$ is a free abelian group of rank n.*

Proof. Let $\alpha_1, \ldots, \alpha_n$ be a basis of k as a $\mathbb{Q}$-vector space, then there exist $m_i \in \mathbb{Z}$ such that $m_i \alpha_i \in \mathfrak{o}_k$, $i = 1, \ldots, n$. Without loss of generality, let $\alpha_i \in \mathfrak{o}_k$ and $\{\alpha_1, \ldots, \alpha_n\}$ is a basis of k as $\mathbb{Q}$-vector space. Hence, $\mathfrak{o}_k$ spans k, i.e., for any $\alpha \in k$, there are $a_1, \ldots, a_n \in \mathbb{Z}$ such that $\alpha = a_1\alpha_1 + \cdots + a_n\alpha_n$. By the above theorem, we also have $d_{k/\mathbb{Q}}(\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}$.

Among all bases of $k/\mathbb{Q}$ that consist of integers, choose one, say $\{\omega_1, \ldots, \omega_n\}$, for which $|d_{k/\mathbb{Q}}(\alpha_1, \ldots, \alpha_n)|$ is minimal. We claim that $\{\omega_1, \ldots, \omega_n\}$ is a set of free $\mathbb{Z}$-generated for $\mathfrak{o}_k$.

For any $x \in \mathfrak{o}_k$, $x = \sum_{i=1}^{n} a_i\omega_i$, and $a_i \in \mathbb{Q}$, we claim that $a_i \in \mathbb{Z}$. If not, suppose $a_1 \notin \mathbb{Z}$. For $\omega_1' = \{a_1\}\omega_1 + a_2\omega_2 + \cdots + a_n\omega_n = x - [a_1]\omega_1 \in \mathfrak{o}_k$ where $\{a_1\}$ and $[a_1]$ are the fractional part and the integer part of the real number a_1 respectively, and $\{\omega_1', \omega_2, \ldots, \omega_n\}$ is also a basis of $\mathfrak{o}_k$, and

$$\begin{pmatrix} \omega_1' \\ \omega_2 \\ \vdots \\ \omega_n \end{pmatrix} = \begin{pmatrix} \{a_1\} & a_2 & a_3 & \cdots & a_n \\ 0 & 1 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix} \begin{pmatrix} \omega_1 \\ \omega_2 \\ \vdots \\ \omega_n \end{pmatrix} = M \begin{pmatrix} \omega_1 \\ \omega_2 \\ \vdots \\ \omega_n \end{pmatrix}.$$

Therefore,

$$\begin{aligned} |d_{k/\mathbb{Q}}(\omega_1', \omega_2, \ldots, \omega_n)| &= |(\det(M))^2 d_{k/\mathbb{Q}}(\omega_1, \ldots, \omega_n)| \\ &= |\{a_1\}^2 d_{k/\mathbb{Q}}(\omega_1, \ldots, \omega_n)| \\ &< |d_{k/\mathbb{Q}}(\omega_1, \ldots, \omega_n)|, \end{aligned}$$

which contradicts the fact that $|d_{k/\mathbb{Q}}(\omega_1, \ldots, \omega_n)|$ is minimal. Hence $a_1 \in \mathbb{Z}$, and the theorem is completely proved. □

We say that $\{\omega_1, \ldots, \omega_n\}$ in the above theorem is an *integral basis or minimal basis* for k. Let $\{\omega_1, \ldots, \omega_n\}$ be an integral basis for k. Define the *absolute discriminant of* k as

$$d_k = d_{k/\mathbb{Q}}(\omega_1, \ldots, \omega_n) = \det(\sigma_i(\omega_j)))^2 = \det(\mathrm{Tr}(\omega_i\omega_j)). \tag{1.3}$$

Clearly, the discriminant of the number field k over $\mathbb{Q}$ is well-defined and an integer. In other words, for two integral bases for k, we get the same discriminant for k. We also have that $d_k \neq 0$. This is a consequence of the following fact: the symmetric bilinear form $\mathrm{Tr}(xy)$ is non-degenerate.

For the relative algebraic number fields K/k,

Examples 1.6. *A quadratic field k is by definition an algebraic number field of degree two. There exists a unique square free $d \in \mathbb{Z}$ such that $k = \mathbb{Q}(\sqrt{d})$. Let*

$$\omega = \begin{cases} (1+\sqrt{d})/2, & \text{if } d \equiv 1 (mod 4) \\ \sqrt{d}, & \text{if } d \equiv 2, 3 (mod 4), \end{cases}$$

Then $\{1, \omega\}$ is an integral basis of k. And the discriminant of k is

$$d_k = \begin{cases} d, & \text{if } d \equiv 1 (mod 4) \\ 4d, & \text{if } d \equiv 2, 3 (mod 4). \end{cases}$$

Proposition 1.7. *(1), The sign of d_k is $(-1)^{r_2}$.*

(2), Stickelberger's theorem: $d_k \equiv 0$ or $1 \mod 4$.

Proof. (1), Clearly, the matrix $(\sigma_i(\omega_j))$ has r_2 pairs of complex conjugate rows, so its determinant is i^{r_2} times a real number; thus the sign of d_k is $(-1)^{r_2}$. In fact, we have $\overline{\det(\sigma_i(\omega_j))} = (-1)^{r_2} \det(\sigma_i(\omega_j))$.

(2), Write $n = [k : \mathbb{Q}]$, let $\alpha_1, \alpha_2, ..., \alpha_n$ be an integral basis for $\mathfrak{o}_k$, and let $\sigma_1, \ldots, \sigma_n$ be the distinct embeddings of k. Now write

$$A = \sum_{\pi \text{ even}} \left(\prod_{i=1}^{n} \sigma_i \alpha_{\pi(i)} \right), \quad B = \sum_{\pi \text{ odd}} \left(\prod_{i} \sigma_i \alpha_{\pi(i)} \right)$$

where π denotes a permutation of $1, ..., n$. We have

$$\begin{aligned} \det(\sigma_i \alpha_j) &= \sum_{\pi} (-1)^{\pi(1,2,\ldots,n)} \prod_{i=1}^{n} \sigma_i \alpha_{\pi(i)} \\ &= A - B, \end{aligned}$$

and therefore $d_k = (A-B)^2 = (A+B)^2 - 4AB$. Since $\sigma_i(A+B) = A+B$ and $\sigma_i(AB) = AB$, we see that they are rational numbers by Galois theory. Since $A+B, AB$ are algebraic integers, hence $A+B, AB \in \mathbb{Z}$. Therefore, $d_k \equiv 0$ or $1 \mod 4$. □

1.1.3 Noetherian ring

A ring R is *Noetherian* if every ideal in R is finitely generated. Obviously, any principal ideal domain is Noetherian.

Lemma 1.8. *The following conditions on a ring R are equivalent:*

(1), R is Noetherian.

(2) R satisfies the ascending chain condition, i.e., every ascending chain of ideals $I_1 \subset I_2 \subset \cdots \subset I_n \subset \cdots$ stabilizes.

(3), Every nonempty set S of ideals in R has a maximal element, i.e., there exists an ideal in S not properly contained in any other ideal in S.

Proof. (1)⇒(2): Set $I = \bigcup_{n=1}^{\infty} I_n$ is an $\mathfrak{o}_k$-submodule of R. Hence it is generated by a finite set $\alpha_1, \alpha_2, \ldots, \alpha_n$ of elements of I. If $\alpha_i \in I_{k_i}$, then $\alpha_1, \alpha_2, \ldots, \alpha_n \subset I_{k_n}$, then $I \subset I_{k_n}$; so the chain is constant from I_{k_n} on.

(2)⇒(3): If (3) were false we could construct strictly increasing sequence $I_1 \subset I_2 \subset \cdots$ of $\mathfrak{o}_k$-submodule of R. For suppose we have chosen $I_1, ..., I_n$. The $\mathfrak{o}_k$-submodule of R which contains I_n forms a non-empty family, and this family contains no maximal element; so we can choose an I_{n+1} which strictly contains I_n. This contradicts (2).

(3)⇒(1): Suppose that R contains an $\mathfrak{o}_k$-submodule N which is not finitely generated. Let S be the set of all finitely generated $\mathfrak{o}_k$-submodule of N, then by (3) we have that S has a maximal element M_0, but we can find ξ to be an element of N not in M_0. Then M_0 is not maximal in S because S contains a strictly larger $\mathfrak{o}_k$-submodule of N generated by M_0 and ξ. This forms a contradiction. □

Proposition 1.9. *The ring of integers $\mathfrak{o}_k$ of a number field k is Noetherian.*

Proof. For any ideal $\mathfrak{a}$ of $\mathfrak{o}_k$, we take a nonzero element $\alpha \in \mathfrak{a}$ and the minimal polynomial for α over $\mathbb{Q}$ is $p(x) = x^m + a_1 x^{m-1} + \cdots + a_m \in \mathbb{Z}[x]$. Then we have

$$a_m = -\alpha^m - a_1\alpha^{m-1} - \cdots - a_{m-1}\alpha \in \mathfrak{a} \cap \mathbb{Z}$$

and $a_m \neq 0$. Let $\omega_1, \ldots, \omega_n$ be an integral basis of $\mathfrak{o}_k$; then we have $a_m\omega_1, \ldots, a_m\omega_n \in \mathfrak{a}$. By considering a basis of k, whose elements are in $\mathfrak{a}$ and whose discriminant has minimal absolute value, we conclude, as in the proof of theorem, that $\mathfrak{a}$ is a free $\mathbb{Z}$-module of rank n. In particular, $\mathfrak{a}$ is finitely generated. This completes the proof of the theorem. □

1.2 Ideals and Factorization

Let $\mathfrak{o}_k$ be the ring of integers of a number field k. Unfortunately we do not in general have unique factorization. $\mathbb{Z}[\sqrt{-5}]$, the ring of integers of the number field $\mathbb{Q}[\sqrt{-5}]$, is well-known that it is not a unique factorization domain:

$$21 = 3 \cdot 7 = (1 + 2\sqrt{-5})(1 - 2\sqrt{-5}),$$

where the numbers $3, 7, 1+2\sqrt{-5}$ and $1-2\sqrt{-5}$ are all irreducible elements. In the following discussion, we shall prove that every ideal of $\mathfrak{o}_k$ can be written uniquely as a product of prime ideals, where uniqueness is understood to mean uniqueness up to the order of the facotrs. In fact, this is true in any Dedekind domain. Thus, in an algebraic number field, the prime ideals play the same role as the prime numbers do in rational number theory. For simplicity, we shall assume that *all ideals are nonzero* from now on.

1.2.1 Dedekind domain

An integral domain R is *integrally closed* in its field of fractions if whenever α is in the field of fractions of R and α satisfies a monic polynomial $f(x) \in R[x]$, then $\alpha \in R$.

Proposition 1.10. *$\mathfrak{o}_k$ is integrally closed. Also, the ring $\overline{\mathbb{Z}}$ of all algebraic integers is integrally closed in $\overline{\mathbb{Q}}$.*

Proof. Suppose that $\alpha \in k$, there exists

$$f(x) = x^m + c_1 x^{m-1} + \cdots + c_m \in \mathfrak{o}_k[x],$$

such that $f(\alpha) = 0$. We only need to prove that $\alpha \in \mathfrak{o}_k$. Clearly, $R = \mathbb{Z}[c_1, \ldots, c_m]$ is a subring of $\mathfrak{o}_k$. Then $\mathbb{Z}[c_1, \ldots, c_m]$ is finite generated by $\{\beta_1, \ldots, \beta_t\}$. Therefore, $\{\beta_i \alpha^j \,|\, 1 \le i \le t, 0 \le j \le m-1\}$ span $R[\alpha] = \mathbb{Z}[c_1, \ldots, c_m, \alpha]$, i.e. $\mathbb{Z}[c_1, \ldots, c_m, \alpha]$ is finitely generated. So $\alpha \in \mathfrak{o}_k$. This completes the proof of the proposition. □

A *Dedekind domain* is an integral domain R with 1 such that (1), R is Noetherian, (2), R is integrally closed, and (3), every nonzero prime ideal is maximal.

Lemma 1.11. *Any principal ideal domain is Dedekind.*

Proof. Let $\mathfrak{o}$ be a principal ideal domain, and therefore Noetherian. Suppose that β in k is integral over $\mathfrak{o}$ and write $\beta = \alpha_1/\alpha_2$ with α_1, α_2 in $\mathfrak{o}$. We can assume that $(\alpha_1, \alpha_2) = (1)$; for if $(\alpha_1, \alpha_2) = (\gamma)$ with γ not a unit, we can

divide α_1 and α_2 by γ. If $\beta^n + c_1\beta^{n-1} + \cdots + c_n = 0$ where the c_ν are in $\mathfrak{o}$ then $\alpha_1^n + c_1\alpha_1^{n-1}\alpha_2 + \cdots + c_n\alpha_2^n = 0$. It follows that $(\alpha_2) = (\alpha_1^n, \alpha_2) \supset (\alpha_1, \alpha_2)^n = (1)$, so that α_2 is a unit and β is in $\mathfrak{o}$. Now let (α) be a non-zero prime ideal of $\mathfrak{o}$ and let (β) be a maximal ideal containing (α). Thus α is in (β) and hence equal to $\beta\gamma$ for some γ in $\mathfrak{o}$. But (α) is prime, so one of β, γ must be in (α). If β is in (α) then $(\beta) \subset (\alpha)$ so that (α) is maximal; but if $\gamma = \alpha\delta$ then $\alpha = \beta\alpha\delta$ when $\beta\delta = 1$, and then $(\beta) = 1$ which is forbidden. □

Proposition 1.12. *$\mathfrak{o}_k$ is a Dedekind domain.*

Proof. Our first goal is to show that if $\mathfrak{a}$ is a nonzero ideal in $\mathfrak{o}_k$, then $\mathfrak{a}$ has finite index in $\mathfrak{o}_k$, that is, $\mathfrak{o}_k/\mathfrak{a}$ is a finite quotient ring. Let $\omega_1, \omega_2, \ldots, \omega_n$ be an integral basis of $\mathfrak{o}_k$. Take $m \in \mathfrak{a} \cap \mathbb{Z}^\times$. Then $(m) = \mathbb{Z}m\omega_1 \oplus \cdots \oplus \mathbb{Z}m\omega_n \subset \mathfrak{a} \subset \mathfrak{o}_k$. Obviously,

$$\mathfrak{o}_k/\mathfrak{a} \cong (\mathfrak{o}_k/(m))/(\mathfrak{a}/(m)).$$

And,

$$\begin{aligned} \mathfrak{o}_k/(m) &= (\mathbb{Z}\omega_1 \oplus \cdots \oplus \mathbb{Z}\omega_n)/(\mathbb{Z}m\omega_1 \oplus \cdots \oplus \mathbb{Z}m\omega_n) \\ &\cong (\mathbb{Z}\omega_1/\mathbb{Z}m\omega_1) \oplus \cdots \oplus (\mathbb{Z}\omega_n/\mathbb{Z}m\omega_n) \\ &\cong (\mathbb{Z}/m\mathbb{Z}) \oplus \cdots \oplus (\mathbb{Z}/m\mathbb{Z}). \end{aligned}$$

Thus,

$$|\mathfrak{o}_k/\mathfrak{a}| \leq |\mathfrak{o}_k/(m)| = m^n.$$

We only need to show that every non-zero prime ideal is maximal. For any prime ideal $\mathfrak{p}$ of $\mathfrak{o}_k$, $\mathfrak{o}_k/\mathfrak{p}$ is a domain. Hence $\mathfrak{o}_k/\mathfrak{p}$ is a finite domain, and then it's field. So $\mathfrak{p}$ is maximal. □

For some applications it is convenient to generalize $\mathfrak{o}_k$ the purpose being to enable us to ignore certain bad primes. If $\mathfrak{p}$ is prime ideal of $\mathfrak{o}_k$, we say that α in k is *integral* at $\mathfrak{p}$ if $\alpha = \alpha_1/\alpha_2$ where $\alpha_i \in \mathfrak{o}_k$ and $\alpha_2 \notin \mathfrak{p}$. More generally, let R be a Dedekind domain and let S be any set of prime ideals in R. Then R_S denotes the ring of elements $\alpha = \alpha_1/\alpha_2$ where $\alpha_i \in R$ and $\alpha_2 \notin \mathfrak{p}$ for all $\mathfrak{p} \in S$. It is easy to see that R_S is Dedekind domain with prime ideals $\mathfrak{p}' = \mathfrak{p}R_S$ for $\mathfrak{p} \in S$. If S is a finite set, then R_S is a principal ideal ring by Exercise (1.14). If S consists of one prime ideal $\mathfrak{p}$, then $R_S = R_\mathfrak{p}$ is called the *localization* of R at $\mathfrak{p}$. A *local ring* is a ring which has a unique maximal ideal.

Proposition 1.13. *Let R be a Dedekind domain and let $\mathfrak{p}$ be any prime ideal in R. Then*

(1), $R_\mathfrak{p}$ is local ring with a unique maximal ideal $\mathfrak{m}_\mathfrak{p} = \mathfrak{p}R_\mathfrak{p}$.

(2), Any element of the complement $R_\mathfrak{p} \setminus \mathfrak{m}_\mathfrak{p}$ of $\mathfrak{m}_\mathfrak{p}$ in $R_\mathfrak{p}$ is a unit.

(3), $\mathfrak{m}_\mathfrak{p} \cap R = \mathfrak{p}$.

Example 1.14. *The localization $\mathbb{Z}_{(p)}$ of $\mathbb{Z}$ at (p) consists of all rational numbers a/b, $a, b \in \mathbb{Z}$, with $p \nmid b$.*

1.2.2 Fractional ideal

A nonzero *fractional ideal* $\mathfrak{a}$ of k is a finitely generated $\mathfrak{o}_k$-submodule (i.e., $\mathfrak{o}_k\mathfrak{a} \subset \mathfrak{a}$) of k. If $\alpha_1, \ldots, \alpha_m$ spans $\mathfrak{a}$ as an $\mathfrak{o}_k$-submodule and $\alpha_i = a_i/b_i$ with $a_i, b_i \in \mathfrak{o}_k$, then $c\mathfrak{a} \subset \mathfrak{o}_k$ where $c = \prod_{i=1}^m b_i$. Conversely, if there exists $c \in k^\times$ such that $c\mathfrak{a} \subset \mathfrak{o}_k$, then $c\mathfrak{a}$ is finitely generated as an ideal of $\mathfrak{o}_k$. If c$\mathfrak{a}$ is generated as an ideal by $\{\beta_1, ..., \beta_m\}$, then $\mathfrak{a}$ is generated by $\{c^{-1}\beta_1, ..., c^{-1}\beta_m\}$, as an $\mathfrak{o}_k$-submodule. Thus, $\mathfrak{a}$ is finitely generated as an $\mathfrak{o}_k$-module. This yields an equivalent definition of fractional ideal. An $\mathfrak{o}_k$-submodule $\mathfrak{a}$ of k is called a fractional ideal if there exists $c \in k^\times$ such that $c\mathfrak{a} \subset \mathfrak{o}_k$.

To avoid ambiguity, an ideal in $\mathfrak{o}_k$ sometimes has to be called an *integral ideal*. For any $c \in k^\times$, $(c) = c\mathfrak{o}_k$ is called *principal fractional ideal* . The *inverse* of a fractional ideal $\mathfrak{a}$, denoted $\mathfrak{a}^{-1}$, is the $\mathbb{Z}$-module

$$\mathfrak{a}^{-1} = \{x \in k \,|\, x\mathfrak{a} \subset \mathfrak{o}_k\}.$$

Take $d \in \mathfrak{a} \setminus \{0\}$, then $d\mathfrak{a}^{-1} \subset \mathfrak{a}\mathfrak{a}^{-1} \subset \mathfrak{o}_k$. Therefore $\mathfrak{a}^{-1}$ is also a fractional ideal of k. A fractional ideal $\mathfrak{a}$ is said to be *invertible* if there exists a fractional ideal $\mathfrak{b}$ such that $\mathfrak{a}\mathfrak{b} = \mathfrak{o}_k$.

Let J_k be the set of all nonzero fractional ideals of $\mathfrak{o}_k$. All the obvious rules extend from ideals to fractional ideals. For any $\mathfrak{a}, \mathfrak{b} \in J_k$, denote

$$\mathfrak{a} + \mathfrak{b} = \{a + b | a \in \mathfrak{a}, b \in \mathfrak{b}\}$$

$$\mathfrak{a}\mathfrak{b} = \left\{ \sum_{i=1}^{n} a_i b_i | a_i \in \mathfrak{a}, b_i \in \mathfrak{b}, n \in \mathbb{N} \right\}.$$

It is easy to show that the sum and product of two fractional ideals are again fractional ideals. If $\mathfrak{a} + \mathfrak{b} = \mathfrak{o}_k$, then we say that $\mathfrak{a}$ and $\mathfrak{b}$ are *relatively prime* and write $(\mathfrak{a}, \mathfrak{b}) = 1$. Obviously, we have $\mathfrak{a} \cap \mathfrak{b} = \mathfrak{a}\mathfrak{b}$ as $(\mathfrak{a}, \mathfrak{b}) = 1$.

Theorem 1.15. *The set J_k of nonzero fractional ideals of $\mathfrak{o}_k$ is an abelian group under ideal multiplication. J_k is called the ideal group of k with the identity $\mathfrak{o}_k$.*

Proof. It suffices to show that every fractional ideal $\mathfrak{a}$ is invertible. Before proving theorem we prove firstly some lemmas. Note that we assume that all ideals are nonzero.

- If $\mathfrak{a}$ is an integral ideal then $\mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_m \subset \mathfrak{a}$ for some prime ideals $\mathfrak{p}_i$.

Let S be the set of all proper ideals of $\mathfrak{o}_k$ that do not contain a product of prime ideals. We need to show that S is empty. If not, then since $\mathfrak{o}_k$ is Noetherian, S has a maximal element, say $\mathfrak{a}$. Then, $\mathfrak{a}$ is not a prime ideal of $\mathfrak{o}_k$ since $\mathfrak{a} \in S$, so there exists $a, b \in \mathfrak{o}_k$, with $ab \in \mathfrak{a}$, $a \notin \mathfrak{a}$, $b \notin \mathfrak{a}$. Then, $(\mathfrak{a}, a) \supsetneq \mathfrak{a}$, $(\mathfrak{a}, b) \supsetneq \mathfrak{a}$. Therefore, $(\mathfrak{a}, a) \notin S$, $(\mathfrak{a}, b) \notin S$ by the maximality of $\mathfrak{a}$.

It follows that there exists prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_r, \mathfrak{q}_1, \ldots, \mathfrak{q}_s$, such that $(\mathfrak{a}, a) \supset \mathfrak{p}_1 \cdots \mathfrak{p}_r$ and $(\mathfrak{a}, b) \supset \mathfrak{q}_1 \cdots \mathfrak{q}_s$. But $ab \in \mathfrak{a}$, we have

$$\mathfrak{a} = (\mathfrak{a}, ab) \supset (\mathfrak{a}, a)(\mathfrak{a}, b) = \mathfrak{p}_1, \ldots, \mathfrak{p}_r\mathfrak{q}_1, \ldots, \mathfrak{q}_s,$$

which contradicts $\mathfrak{a} \in S$. Thus, S must actually be empty, which means if $\mathfrak{a}$ is an integral ideal then $\mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_m \subset \mathfrak{a}$ for some prime ideals $\mathfrak{p}_i$.

• For every prime ideal $\mathfrak{p}$ of $\mathfrak{o}_k$, we have $\mathfrak{o}_k \subsetneq \mathfrak{p}^{-1}$.

Since $1 \in \mathfrak{p}^{-1}$, we have $\mathfrak{p} \subset \mathfrak{p}^{-1}\mathfrak{p} \subset \mathfrak{o}_k \subset \mathfrak{p}^{-1}$ by definition. Take $\alpha \in \mathfrak{p}$. From the previous lemma, (α) contains a product of prime ideals. Let r be the least integer such that (α) contains a product of r prime ideals, and say $(\alpha) \supset \mathfrak{p}_1 \cdots \mathfrak{p}_r$, with the $\mathfrak{p}_i$ nonzero prime ideals. Since $\mathfrak{p} \supset (\alpha) \supset \mathfrak{p}_1 \cdots \mathfrak{p}_r$, there exists some integer i such that $\mathfrak{p} \supset \mathfrak{p}_i$ ($\mathfrak{ab} \subset \mathfrak{p} \Rightarrow \mathfrak{a} \subset \mathfrak{p}$, or $\mathfrak{b} \subset \mathfrak{p}$). We can assume that $i = 1$, so $\mathfrak{p} \supset \mathfrak{p}_1$. But $\mathfrak{p}_1$ is a nonzero prime ideal of $\mathfrak{o}_k$, and so is maximal. Hence, $\mathfrak{p} = \mathfrak{p}_1$. Thus, $\mathfrak{p}_2 \cdots \mathfrak{p}_r \nsubseteq (\alpha)$, since r was chosen to be minimal. Choose an element $\beta \in \mathfrak{p}_2 \cdots \mathfrak{p}_r \setminus (\alpha)$. Then $\beta\alpha^{-1} \notin \mathfrak{o}_k$ and

$$\beta\alpha^{-1}\mathfrak{p} \subset (\mathfrak{p}_2 \cdots \mathfrak{p}_r)(\alpha^{-1}\mathfrak{p}_1) \subset \alpha^{-1}(\alpha) = \mathfrak{o}_k.$$

Hence, $\beta\alpha^{-1} \in \mathfrak{p}^{-1}$. The proof of the lemma is completed.

• Every prime ideal $\mathfrak{p}$ is invertible. In fact, we have $\mathfrak{p}\mathfrak{p}^{-1} = \mathfrak{p}^{-1}\mathfrak{p} = \mathfrak{o}_k$.

Since $\mathfrak{p} \subset \mathfrak{p}\mathfrak{p}^{-1} \subset \mathfrak{o}_k \subset \mathfrak{p}^{-1}$ and $\mathfrak{p}$ is maximal, then we have either $\mathfrak{p}\mathfrak{p}^{-1} = \mathfrak{o}_k$, or $\mathfrak{p}\mathfrak{p}^{-1} = \mathfrak{p}$. It remains to show that $\mathfrak{p}\mathfrak{p}^{-1} = \mathfrak{o}_k$.

Assume that $\mathfrak{p}\mathfrak{p}^{-1} = \mathfrak{p}$, then $\gamma\mathfrak{p} \subset \mathfrak{p}$ for any $\gamma \in \mathfrak{p}^{-1}$. Since $\mathfrak{p}$ is a finitely generated $\mathbb{Z}$-module, $\gamma \in \mathfrak{o}_k$ by Theorem (1.1). Thus, $\mathfrak{p}^{-1} \subset \mathfrak{o}_k$ which is a contradiction to $\mathfrak{o}_k \subsetneq \mathfrak{p}^{-1}$. Therefore, every prime ideal $\mathfrak{p}$ is invertible and we have $\mathfrak{p}\mathfrak{p}^{-1} = \mathfrak{p}^{-1}\mathfrak{p} = \mathfrak{o}_k$.

• Every integral ideal $\mathfrak{a}$ is invertible.

If not, there would be a maximal non-invertible ideal $\mathfrak{a}$. Among the ideals containing $\mathfrak{a}$, there is one which is maximal and therefore prime; denote it by $\mathfrak{p}$. Thus $\mathfrak{a} \subset \mathfrak{p}^{-1}\mathfrak{a} \subset \mathfrak{p}^{-1}\mathfrak{p} = \mathfrak{o}_k$. If $\mathfrak{a} = \mathfrak{p}^{-1}\mathfrak{a}$ then an argument like that for the previous displayed statement shows that $\mathfrak{p}^{-1} \subset \mathfrak{o}_k$, which would imply $\mathfrak{o}_k = \mathfrak{p}\mathfrak{p}^{-1} \subset \mathfrak{p}$. So $\mathfrak{a} \neq \mathfrak{p}^{-1}\mathfrak{a}$. By maximality, $\mathfrak{p}^{-1}\mathfrak{a}$ has an inverse $\mathfrak{b}$, and $\mathfrak{b}\mathfrak{p}^{-1}$ is an inverse for $\mathfrak{a}$.

• Every fractional ideal $\mathfrak{a}$ is invertible.

Since every fractional ideal $\mathfrak{a}$, there exists $\delta \in k^\times$ such that $\delta\mathfrak{a} \subset \mathfrak{o}_k$. Then the integral ideal $\mathfrak{b} = \delta\mathfrak{a}$ is invertible. We have

$$\mathfrak{a}(\delta\mathfrak{b}^{-1}) = (\delta\mathfrak{a})\mathfrak{b}^{-1} = \mathfrak{b}\mathfrak{b}^{-1} = \mathfrak{o}_k.$$

Hence, $\mathfrak{a}$ is invertible and its inverse is $\mathfrak{a}^{-1}$. □

Example 1.16. *Consider the ideal $\mathfrak{p} = 3\mathbb{Z}$ of $\mathbb{Z}$. We have that*

$$\mathfrak{p}^{-1} = \{\alpha \in \mathbb{Q} \,|\, \alpha\mathfrak{p} \subset \mathbb{Z}\} = \{\alpha \in \mathbb{Q} \,|\, 3\alpha \in \mathbb{Z}\} = \frac{1}{3}\mathbb{Z}.$$

We have

$$\mathfrak{p} \subsetneq \mathbb{Z} \subsetneq \mathfrak{p}^{-1} \subsetneq \mathbb{Q}.$$

We say $\mathfrak{b}$ *divides* $\mathfrak{a}$, denoted by $\mathfrak{b}|\mathfrak{a}$, if there exists an integral ideal $\mathfrak{c}$ such that $\mathfrak{a} = \mathfrak{b}\mathfrak{c}$. $\mathfrak{b}$ is called a factor of $\mathfrak{a}$ and $\mathfrak{a}$ is called a multiple of $\mathfrak{b}$. We have the following equivalent assertions.

Corollary 1.17. *For any $\mathfrak{a}, \mathfrak{b} \in J_k$, the following assertions $\mathfrak{a} \subset \mathfrak{b}, \mathfrak{a}\mathfrak{b}^{-1} \subset \mathfrak{o}_k$, $\mathfrak{o}_k \subset \mathfrak{a}^{-1}\mathfrak{b}$ and $\mathfrak{b}|\mathfrak{a}$ are equivalent.*

Proof. If $\mathfrak{a} \subset \mathfrak{b}$, then $\mathfrak{a}\mathfrak{b}^{-1} \subset \mathfrak{b}\mathfrak{b}^{-1} = \mathfrak{o}_k$. Reversely, if $\mathfrak{a}\mathfrak{b}^{-1} \subset \mathfrak{o}_k$, then $\mathfrak{a}\mathfrak{b}^{-1} \subset \mathfrak{o}_k = \mathfrak{b}\mathfrak{b}^{-1}$, which means $\mathfrak{a} \subset \mathfrak{b}$. For the other statement, $\mathfrak{a} \subset \mathfrak{b}$ if and only if $\mathfrak{a}^{-1}\mathfrak{b} \supset \mathfrak{o}_k$, the same argument shows that it is true as well. □

Theorem 1.18. *Any fractional ideal $\mathfrak{a}$ of k can be written uniquely in the form*

$$\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{\mathrm{ord}_{\mathfrak{p}}(\mathfrak{a})}, \quad \mathrm{ord}_{\mathfrak{p}}(\mathfrak{a}) \in \mathbb{Z},$$

where the product runs over all prime ideals of $\mathfrak{o}_k$. All but a finite number of the exponents are zeros, so that the product is actually well defined. In particular, $\mathfrak{a}$ is an integral ideal if and only if $\mathrm{ord}_{\mathfrak{p}}(\mathfrak{a}) \geq 0$ for all $\mathfrak{p}$.

Proof. Claim that $\mathfrak{a}$ can be written in the desired form in at least one way. It suffices to consider the case of $\mathfrak{a}$ integral. For if $\mathfrak{a}$ is arbitrary, let $c \in \mathfrak{o}_k$ be such that $c\mathfrak{a}$ is integral. Let $c\mathfrak{o}_k = \mathfrak{q}_1 \dots \mathfrak{q}_h$, $c\mathfrak{a} = \mathfrak{p}_1 \dots \mathfrak{p}_g$. Then

$$\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_g \mathfrak{q}_1^{-1} \cdots \mathfrak{q}_h^{-1}.$$

Let S be the set of ideals of $\mathfrak{o}_k$ that cannot be written as a product of prime ideals. Since $\mathfrak{o}_k$ is Noetherian, we can choose $\mathfrak{a}$, maximal with respect to

this property. Then $\mathfrak{a}$ is not prime, so $\mathfrak{a} \subsetneq \mathfrak{p}$ for some maximal ideal $\mathfrak{p}$, hence $\mathfrak{p}$ is prime. Since $\mathfrak{p}$ is invertible, we have

$$\mathfrak{a} \subset \mathfrak{a}\mathfrak{p}^{-1} \subsetneq \mathfrak{o}_k. \tag{1.4}$$

Claim that $\mathfrak{a} \neq \mathfrak{a}\mathfrak{p}^{-1}$. If $\mathfrak{a}\mathfrak{p}^{-1} = \mathfrak{a}$, then $\mathfrak{p}^{-1} = \mathfrak{o}_k$ by multiplying by $\mathfrak{a}^{-1}$, which is a contradiction. Thus, $\mathfrak{a} \subsetneq \mathfrak{a}\mathfrak{p}^{-1}$. Hence $\mathfrak{a}\mathfrak{p}^{-1}$ is a product of primes by the maximality of $\mathfrak{a}$ and if we multiply this product by $\mathfrak{p}$ we get a product for $\mathfrak{a}$. Note that the above argument also shows that an integral ideal can be expressed as a product of nonnegative powers of prime ideals.

Without loss of generality, let us restrict ourselves to integral ideals. Let

$$\mathfrak{a} = \mathfrak{p}_1 \dots \mathfrak{p}_g = \mathfrak{q}_1 \dots \mathfrak{q}_h \tag{1.5}$$

be two factorizations of $\mathfrak{a}$ into prime factors. Then $\mathfrak{p}_1 \supset \mathfrak{a}$ implies $\mathfrak{p}_1$ contains some $\mathfrak{q}_i$, say $\mathfrak{q}_1$. But $\mathfrak{q}_1$ is prime and hence maximal, so that $\mathfrak{p}_1 = \mathfrak{q}_1$. Multiplying both side of (1.5) by $\mathfrak{p}_1^{-1}$, we arrive at

$$\mathfrak{p}_2 \dots \mathfrak{p}_g = \mathfrak{q}_2 \dots \mathfrak{q}_h.$$

The proof may now be completed by induction. □

The integer $\mathrm{ord}_{\mathfrak{p}}(\mathfrak{a})$ is called the *order* of $\mathfrak{a}$ in $\mathfrak{p}$, also denoted by $\mathrm{ord}_{\mathfrak{p}}(\mathfrak{a})$. Denote $\mathfrak{d}$ to be the *greatest common divisor* of $\mathfrak{a}$ and $\mathfrak{b}$, if (1), $\mathfrak{d}|\mathfrak{a}$ and $\mathfrak{d}|\mathfrak{b}$; and (2), if $\mathfrak{c}|\mathfrak{a}$ and $\mathfrak{c}|\mathfrak{b}$, then $\mathfrak{c}|\mathfrak{d}$. Denote $\mathfrak{d}$ by $\gcd(\mathfrak{a}, \mathfrak{b})$. Similarly, define $\mathfrak{m}$ to be the *least common multiple* of $\mathfrak{a}$ and $\mathfrak{b}$, if (1), $\mathfrak{a}|\mathfrak{m}$ and $\mathfrak{b}|\mathfrak{m}$; and (2), if $\mathfrak{a}|\mathfrak{n}$ and $\mathfrak{b}|\mathfrak{n}$, then $\mathfrak{m}|\mathfrak{n}$. Denote $\mathfrak{m}$ by $\mathrm{lcm}(\mathfrak{a}, \mathfrak{b})$.

Corollary 1.19. *For any ideals $\mathfrak{a},\ \mathfrak{b} \in J_k$ and any prime ideal $\mathfrak{p}$ of $\mathfrak{o}_k$, we have*

(1), $\mathrm{ord}_{\mathfrak{p}}(\mathfrak{a}^{-1}) = -\mathrm{ord}_{\mathfrak{p}}(\mathfrak{a}),\ \mathrm{ord}_{\mathfrak{p}}(\mathfrak{a}\mathfrak{b}) = \mathrm{ord}_{\mathfrak{p}}(\mathfrak{a}) + \mathrm{ord}_{\mathfrak{p}}(\mathfrak{b})$;

(2), $\mathfrak{a} + \mathfrak{b} = \gcd(\mathfrak{a}, \mathfrak{b}),\ \ \mathfrak{a} \cap \mathfrak{b} = \mathrm{lcm}(\mathfrak{a}, \mathfrak{b})$*; and*

(3),

$$\mathrm{ord}_{\mathfrak{p}}(\mathfrak{a} + \mathfrak{b}) = \min\{\mathrm{ord}_{\mathfrak{p}}(\mathfrak{a}), \mathrm{ord}_{\mathfrak{p}}(\mathfrak{b})\}$$
$$\mathrm{ord}_{\mathfrak{p}}(\mathfrak{a} \cap \mathfrak{b}) = \max\{\mathrm{ord}_{\mathfrak{p}}(\mathfrak{a}), \mathrm{ord}_{\mathfrak{p}}(\mathfrak{b})\}.$$

Proof. It is clear that $\mathrm{ord}_{\mathfrak{p}}(\mathfrak{a}^{-1}) = -\mathrm{ord}_{\mathfrak{p}}(\mathfrak{a})$ and $\mathrm{ord}_{\mathfrak{p}}(\mathfrak{a}\mathfrak{b}) = \mathrm{ord}_{\mathfrak{p}}(\mathfrak{a}) + \mathrm{ord}_{\mathfrak{p}}(\mathfrak{b})$. Therefore, we have

$$\begin{aligned} \mathfrak{b} \,|\, \mathfrak{a} &\Leftrightarrow \mathfrak{a} \subset \mathfrak{b} \Leftrightarrow \mathfrak{a}\mathfrak{b}^{-1} \subset \mathfrak{o}_k \\ &\Leftrightarrow \mathrm{ord}_{\mathfrak{p}}(\mathfrak{a}\mathfrak{b}^{-1}) \geq 0 \\ &\Leftrightarrow \mathrm{ord}_{\mathfrak{p}}(\mathfrak{a}) \geq \mathrm{ord}_{\mathfrak{p}}(\mathfrak{b}), \end{aligned}$$

for all $\mathfrak{p}$.

Since $\mathfrak{a} \subset \mathfrak{a}+\mathfrak{a}, \mathfrak{b} \subset \mathfrak{a}+\mathfrak{b}$, we see that $\mathfrak{a}+\mathfrak{b}|\mathfrak{a}$ and $\mathfrak{a}+\mathfrak{b}|\mathfrak{b}$. If $\mathfrak{c}|\mathfrak{a}, \mathfrak{c}|\mathfrak{b}$, then $\mathfrak{a} \subset \mathfrak{c}$ and $\mathfrak{b} \subset \mathfrak{c}$, so that, $\mathfrak{a}+\mathfrak{b} \subset \mathfrak{c}$, i.e., $\mathfrak{c}|\mathfrak{a}+\mathfrak{b}$. Therefore $\mathfrak{a}+\mathfrak{b} = \gcd(\mathfrak{a}, \mathfrak{b})$. Similarly, we have $\mathfrak{a} \cap \mathfrak{b} = \mathrm{lcm}(\mathfrak{a}, \mathfrak{b})$. Since $\mathfrak{a} + \mathfrak{b}$ (respectively, $\mathfrak{a} \cap \mathfrak{b}$) is the smallest ideal containing both $\mathfrak{a}$ and $\mathfrak{b}$ (respectively, the largest ideal contained in $\mathfrak{a}$ and $\mathfrak{b}$), the formulas of follow. □

1.2.3 The Chinese Remainder Theorem

In this subsection we will prove the Chinese Remainder Theorem for the ring of integers, deduce several useful consequences. In algebraic number theory, we often have need of a notion of congruence that generalizes the usual notion of congruence modulo an ideal. Let $\mathfrak{a}$ be an integral ideal of $\mathfrak{o}_k$ and $\alpha, \beta \in k$. Two elements α, β are called *congruent modulo* $\mathfrak{a}$ if $\alpha - \beta \in \mathfrak{a}$, say, $\alpha \equiv \beta (\mathrm{mod} \mathfrak{a})$.

Theorem 1.20. *(The Chinese Remainder Theorem) Let* $\mathfrak{a} = \prod_{i=1}^{g} \mathfrak{p}_i^{e_i}$ *be a non-zero ideal of* $\mathfrak{o}_k$*; then the natural map*

$$\varphi : \mathfrak{o}_k \longrightarrow \bigoplus_{i=1}^{g} \mathfrak{o}_k/\mathfrak{p}_i^{e^i}$$

is onto and induces an isomorphism

$$\mathfrak{o}_k/\mathfrak{a} \cong \bigoplus_{i=1}^{g} \mathfrak{o}_k/\mathfrak{p}_i^{e^i}.$$

Proof. Since

$$ker\varphi = \{x \in \mathfrak{o}_k | \varphi(x) = 0\} = \{x \in \mathfrak{o}_k | x \in \bigcap_{i=1}^{g} \mathfrak{p}_i^{e_i}\} = \prod_{i=1}^{g} \mathfrak{p}_i^{e_i}.$$

Thus only to prove φ is surjective. We only show a special case. Suppose a ring R, and I, J are ideals in R, such that $I + J = R$. Choose $x \in I$ and $y \in J$ such that $x+y = 1$. Then $x = 1-y$ maps to $(0, 1)$ in $R/I \oplus R/J$, and $y = 1-x$ maps to $(1, 0)$ in $R/I \oplus R/J$. Thus the map $R/(I \cap J) \to R/I \oplus R/J$ is surjective. By induction, we conclude φ is surjective. □

Corollary 1.21. *Let* $\mathfrak{a}_1, ..., \mathfrak{a}_m$ *be nonzero integral ideals coprime in pairs and let* $\beta_1, \ldots, \beta_m$ *be elements of* $\mathfrak{o}_k$*. Then there exists* $\alpha \in \mathfrak{o}_k$ *such that*

$$\alpha \equiv \beta_i \,(\mathrm{mod}\, \mathfrak{a}_i), \quad i = 1, 2, \ldots, m. \tag{1.6}$$

Proof. It's trivial by the above theorem. □

The following corollary means that ideals can be generated by two elements!

Corollary 1.22. *Let $\mathfrak{a}$ be a fractional ideal of $\mathfrak{o}_k$ and a nonzero $\alpha \in \mathfrak{a}$. Then there exists $\beta \in \mathfrak{a}$ such that*

$$(\alpha, \beta) = \langle \alpha, \beta \rangle = \alpha\mathfrak{o}_k + \beta\mathfrak{o}_k = \mathfrak{a}.$$

Proof. Let us first assume that $\mathfrak{a}$ is an integral ideal. Let $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_m$ be all the prime factors of $(\alpha) \subset \mathfrak{a}$, so that $\mathfrak{a}$ can be written as

$$\mathfrak{a} = \prod_{i=1}^{m} \mathfrak{p}_i^{e_i},\ e_i \geq 0.$$

Let us choose $\beta_i \in \mathfrak{p}_i^{e_i} \backslash \mathfrak{p}_i^{e_i+1}$, by Corollary 1.21, there exists $\beta \in \mathfrak{a}$, such that $\beta \equiv \beta_i \pmod{\mathfrak{p}_i^{e_i+1}}$, $i = 1, 2, \ldots, m$. Thus, $\beta \in \mathfrak{p}_i^{e_i} \backslash \mathfrak{p}_i^{e_i+1}$, i.e., $\mathfrak{p}_i^{e_i} \| (\beta)$, so $\beta \in \mathfrak{a}$. Since for every $i, \mathfrak{p}_i \nmid (\beta)\mathfrak{a}^{-1}$, then we have $((\beta)\mathfrak{a}^{-1}, (\alpha)) = 1$, i.e., $(\beta)\mathfrak{a}^{-1} + (\alpha) = \mathfrak{o}_k$. To conclude, we have that

$$\mathfrak{a} = (\beta) + (\alpha)\mathfrak{a} \subset (\alpha) + (\beta) \subset \mathfrak{a}.$$

If $\mathfrak{a}$ is a fractional ideal, there exists by definition $0 \neq c \in \mathfrak{o}_k$ such that $\mathfrak{a} = c\mathfrak{b}$ with $\mathfrak{b}$ an integral ideal. Thus $\alpha/c \in \mathfrak{b}$. By the first part there exists $\beta \in \mathfrak{b}$, such that $\mathfrak{b} = (\alpha/c, \beta)$. Thus $\mathfrak{a} = (\alpha, \beta/c)$. □

Corollary 1.23. *Let $\mathfrak{p}$ be a nonzero prime ideal of $\mathfrak{o}_k$. Then for any $n \geq 1$*

$$\mathfrak{o}_k/\mathfrak{p} \cong \mathfrak{p}^n/\mathfrak{p}^{n+1} \tag{1.7}$$

as $\mathfrak{o}_k$-modules.

Proof. Take $\beta \in \mathfrak{p}^n \backslash \mathfrak{p}^{n+1}$, i.e., $\mathfrak{p}^n \parallel (\beta)$. We consider the map

$$\begin{aligned} \varphi : \quad \mathfrak{o}_k &\longrightarrow \mathfrak{p}^n/\mathfrak{p}^{n+1} \\ \alpha &\longmapsto \alpha\beta. \end{aligned}$$

This will conclude the proof since we will prove that $\ker \varphi = \mathfrak{p}$ and φ is surjective.

Firstly, we have

$$\ker \varphi = \{x \in \mathfrak{o}_k | x\beta \in \mathfrak{p}^{n+1}\} = \{x \in \mathfrak{o}_k | x \in \mathfrak{p}\} = \mathfrak{p}.$$

Secondly, given any $\gamma \in \mathfrak{p}^n$, by Corollary 1.21, we can find $\delta \in \mathfrak{o}_k$, such that

$$\begin{aligned} \delta &\equiv \gamma \pmod{\mathfrak{p}^{n+1}} \\ \delta &\equiv 0 \pmod{(\beta)\mathfrak{p}^{-n}} \end{aligned}$$

since $((\beta)\mathfrak{p}^{-n}, \mathfrak{p}^n) = 1$. And we have $\delta \in \mathfrak{p}^n \cap (\beta)\mathfrak{p}^{-n} = (\beta)$. In other words, $\delta/\beta \in \mathfrak{o}_k$. Therefore

$$\varphi(\delta/\beta) = \delta \mod \mathfrak{p}^{n+1} = \gamma.$$

Thus φ is surjective. □

1.2.4 Norm of ideals

Let $\mathfrak{a}$ be an integral ideal of $\mathfrak{o}_k$. We know that $\mathfrak{a}$ is also a free abelian group of rank $[k : \mathbb{Q}] = n$. Suppose that $\{\alpha_1, \ldots, \alpha_n\}, \{\beta_1, \ldots, \beta_n\}$ are respectively integral basis of $\mathfrak{o}_k$ and $\mathfrak{a}$. Then there exists a square matrix $T = (t_{ij})$ with integral coefficients, such that

$$\begin{pmatrix} \beta_1 \\ \vdots \\ \beta_n \end{pmatrix} = T \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix}.$$

Denote the *absolute norm* of the integral ideal $\mathfrak{a}$ by

$$N(\mathfrak{a}) = N_k(\mathfrak{a}) = N_{k/\mathbb{Q}}(\mathfrak{a}) = |\det(T)|.$$

Clearly, it is well-defined, independent of the choice of bases. By convention, the norm of the zero ideal is taken to be zero.

Proposition 1.24. $N(\mathfrak{a}) = |\mathfrak{o}_k/\mathfrak{a}|$.

Proof. According to the abelian fundamental theorem, we can take an integral basis $\{\omega_1, \ldots, \omega_n\}$ of $\mathfrak{o}_k$, such that $\mathfrak{o}_k = \mathbb{Z}\omega_1 \oplus \cdots \oplus \mathbb{Z}\omega_n, \mathfrak{a} = \mathbb{Z}a_1\omega_1 \oplus \cdots \oplus \mathbb{Z}a_n\omega_n, a_i \in \mathbb{Z}$. Then,

$$\begin{pmatrix} a_1\omega_1 \\ \vdots \\ a_n\omega_m \end{pmatrix} = \begin{pmatrix} a_1 & & \\ & \ddots & \\ & & a_n \end{pmatrix} \begin{pmatrix} \omega_1 \\ \vdots \\ \omega_n \end{pmatrix}.$$

Thus we obtain $N_k(\mathfrak{a}) = |a_1 a_2 \cdots a_n|$ from the definition of the norm of ideal. On the other hand,

$$\begin{aligned} \mathfrak{o}_k/\mathfrak{a} &= (\mathbb{Z}\omega_1 \oplus \cdots \oplus \mathbb{Z}\omega_n)/(\mathbb{Z}a_1\omega_1 \oplus \cdots \oplus \mathbb{Z}a_n\omega_n) \\ &\cong (\mathbb{Z}\omega_1/\mathbb{Z}a_1\omega_1) \oplus \cdots \oplus (\mathbb{Z}\omega_n/\mathbb{Z}a_n\omega_n) \\ &\cong (\mathbb{Z}/a_1\mathbb{Z}) \oplus \cdots \oplus (\mathbb{Z}/a_n\mathbb{Z}). \end{aligned}$$

Therefore, $|\mathfrak{o}_k/\mathfrak{a}| = \prod_{i=1}^{n} |\mathbb{Z}/a_i\mathbb{Z}| = |a_1 \cdots a_n| = N_k(\mathfrak{a})$. □

Theorem 1.25. *Suppose that* $\mathfrak{a}$, $\mathfrak{b}$ *are integral ideals of* $\mathfrak{o}_k$, *and* $\mathfrak{a} = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$ *with* $\mathfrak{p}_i$ *are distinct prime ideals of* $\mathfrak{o}_k$. *Then*

(1), $N(\mathfrak{a}) = N(\mathfrak{p}_1)^{e_1} \cdots N(\mathfrak{p}_r)^{e_r}$.

(2), $N(\mathfrak{ab}) = N(\mathfrak{a})N(\mathfrak{b})$.

(3), Let $\{\beta_1, \ldots, \beta_n\}$ *be an integral basis of* $\mathfrak{a}$. *Then*

$$d(\beta_1, \ldots, \beta_n) = N(\mathfrak{a})^2 d_k. \tag{1.8}$$

(4), Let $\mathfrak{a} = (a)$ *be a principal ideal of* $\mathfrak{o}_k$. *Then* $N(\mathfrak{a}) = |N(a)|$.

Proof. (1), (2), Let $\mathfrak{a}, \mathfrak{b}$ be two coprime integral ideals. By CRT, we have

$$\mathfrak{o}_k/\mathfrak{ab} \cong \mathfrak{o}_k/\mathfrak{a} \oplus \mathfrak{o}_k/\mathfrak{b},$$

thus $N(\mathfrak{ab}) = N(\mathfrak{a})N(\mathfrak{b})$.

We are left to prove that $N(\mathfrak{p}^i) = N(\mathfrak{p})^i$, for $i \geq 1$. Now one of the isomorphism theorems for rings allows us to write that

$$N(\mathfrak{p}^{i-1}) = |\mathfrak{o}_k/\mathfrak{p}^{i-1}| = |(\mathfrak{o}_k/\mathfrak{p}^i)/(\mathfrak{p}^{i-1}/\mathfrak{p}^i)|.$$

By the above Corollary (1.23), we have

$$N(\mathfrak{p}^{i-1}) = N(\mathfrak{p}^i)/N(\mathfrak{p}).$$

Thus $N(\mathfrak{p}^i) = N(\mathfrak{p}^{i-1})N(\mathfrak{p})$, and by induction on i, we conclude the proof of (1) and (2).

(3), Form the formula (1.2), we have

$$d(\beta_1, \beta_2, \ldots, \beta_n) = \big(\det \sigma_i(\beta_j)\big)^2 = N(\mathfrak{a})^2 d_k.$$

(4), Let $\alpha_1, \alpha_2, \ldots, \alpha_n$ be an integral basis of $\mathfrak{o}_k$. Then $a\alpha_1, a\alpha_2, \ldots, a\alpha_n$ is an integral basis of $(a) = a\mathfrak{o}_k$. An easy induction gives

$$d(a\alpha_1, a\alpha_2, \ldots, a\alpha_n) = N(\mathfrak{a})^2 d_k.$$

On the other hand,

$$\begin{aligned} d(a\alpha_1, a\alpha_2, \ldots, a\alpha_n) &= \det(\sigma_i(a\alpha_j))^2 \\ &= \det(\sigma_i(a)\sigma_i(\alpha_j))^2 \\ &= \left(\prod_{i=1}^{n} \sigma_i(a)\right)^2 \det(\sigma_i(\alpha_j))^2 \\ &= N(a)^2 d_k. \end{aligned}$$

Hence $N(\mathfrak{a}) = |N(a)|$. □

We can extend the definition of norm to fractional ideals, in the following way. Since any fractional ideal $\mathfrak{A}$ of k can be written uniquely in the form $\mathfrak{A} = \mathfrak{a}/\mathfrak{b}$ where $\mathfrak{a}$ and $\mathfrak{b}$ are ideals of $\mathfrak{o}_k$, we can put

$$N(\mathfrak{A}) = N(\mathfrak{a})/N(\mathfrak{b}).$$

Similarly, we have the same theorem (1.25) about the norm of fractional ideals.

1.3 Ideal Class Group and Units

We are now interested in understanding two aspects of the ring of integers of algebraic number fields: what is the proportion of principal ideals among all the fractional ideals, and what is the structure of their group of units. We will introduce the notion of class number and prove it is finite. And we will then prove Dirichlet's unit theorem for the structure of the group of units. Both results will be as consequences of Minkowski's theorem.

1.3.1 Lattices and Minkowski's theorem

A *lattice* Λ in $\mathbb{R}^n$ is a subgroup of the form

$$\Lambda = \left\{ \sum_{i=1}^{n} a_i \alpha_i \,|\, a_i \in \mathbb{Z} \right\} = \mathbb{Z}\alpha_1 \oplus \cdots \oplus \mathbb{Z}\alpha_n,$$

where $\alpha_1, \ldots, \alpha_n$ is a basis for $\mathbb{R}^n$. Hence Λ is a free abelian group($\mathbb{Z}$-module) of rank n. A subgroup H of $\mathbb{R}^n$ is *discrete* if each bounded subset of $\mathbb{R}^n$ intersects H in a finite set.

Proposition 1.26. *A subgroup Λ of $\mathbb{R}^n$ is discrete if it is a lattice; and every discrete subgroup of $\mathbb{R}^n$ is a lattice of $\mathbb{R}^m$ for some $0 \leq m \leq n$.*

Proof. Let $\Lambda = \mathbb{Z}\alpha_1 \oplus \cdots \oplus \mathbb{Z}\alpha_n$ be a lattice in $\mathbb{R}^n$. Then for any $\alpha \in \mathbb{R}^n$, we have $\alpha = \sum_{i=1}^{n} r_i \alpha_i$, where $r_i \in \mathbb{R}$. And let U be a bounded subset of $\mathbb{R}^n$, which means, there exists a positive number M such that for any $\alpha = \sum_{i=1}^{n} r_i \alpha_i \in U$, $|r_i| < M$ for any $i = 1, \ldots, n$. If $\alpha \in \Lambda \cap U$, then $|r_i| < M$ and $r_i \in \mathbb{Z}$, which clearly have finitely many possibilities. Consequently, $\Lambda \cap U$ is a finite set, hence that Λ is discrete.

Let H be a discrete subgroup of $\mathbb{R}^n$ with a maximal $\mathbb{R}$-linear independent subset $\{\alpha_1, \ldots, \alpha_m\}$. It is clear that we have $0 \leq m \leq n$. We will show that H is a lattice of $\mathbb{R}^m$. Denote $\mathcal{D}$ as the parallelepiped generated by $\alpha_1, \ldots, \alpha_m$, that is,

$$\mathcal{D} = \mathcal{D}(\alpha_1, \ldots, \alpha_m) = \left\{ \sum_{i=1}^{m} a_i \alpha_i \mid 0 \leq a_i < 1 \right\}.$$

Clearly $\mathcal{D} \subseteq \mathbb{R}^n$ is bounded, and hence $H \cap \mathcal{D}$ is a finite set. For any $x \in H$, x can be denoted as $x = \sum_{i=1}^{m} \lambda_i \alpha_i$, where $\lambda_i \in \mathbb{R}$. Write, for any $j \in \mathbb{Z}$,

$$x_j = jx - \sum_{i=1}^{m} [j\lambda_i]\alpha_i = \sum_{i=1}^{m} \{j\lambda_i\}\alpha_i \in H \cap \mathcal{D}.$$

Then $x_1 \in H \cap \mathcal{D}$ and $x = x_1 + \sum_{i=1}^{m} [\lambda_i]\alpha_i$, so H is a subgroup of $\mathbb{R}^n$ generated by a finite set $(H \cap \mathcal{D}) \cup \{\alpha_1, \ldots, \alpha_m\}$, which implies H is a finitely generated abelian group.

Moreover, $x_j \in H \cap \mathcal{D}$ for any $j \in \mathbb{Z}$ but $H \cap \mathcal{D}$ is finite. Thus there exist $j, k \in \mathbb{Z}$ such that $j \neq k$ but $x_j = x_k$, which gives

$$(j-k)\lambda_i = [j\lambda_i] - [k\lambda_i] \in \mathbb{Z},$$

so $\lambda_i \in \mathbb{Q}$, for any $i = 1, \ldots, m$. Then every generator of H is a $\mathbb{Q}$-linear combination of $\alpha_1, \ldots, \alpha_m$. Multiplying H with a common denominator d ($d \neq 0$) of all the coefficients of the finite generators of H, we obtain $dH \subseteq \mathbb{Z}\alpha_1 \oplus \cdots \oplus \mathbb{Z}\alpha_m$. So dH is a subgroup of $\mathbb{Z}\alpha_1 \oplus \cdots \oplus \mathbb{Z}\alpha_m$, and thus $m \leq \mathrm{rank}H = \mathrm{rank}(dH) \leq m$. It follows that $\mathrm{rank}dH = m$. Therefore,

$$dH = \mathbb{Z}\beta_1 \oplus \cdots \oplus \mathbb{Z}\beta_m,$$

where $\beta_i \in \mathbb{R}^n$ for any $i = 1, \ldots, m$. Then

$$H = \mathbb{Z}(\beta_1/d) \oplus \cdots \oplus \mathbb{Z}(\beta_m/d),$$

which yields H is a lattice of $\mathbb{R}^m$ spanned by $\{\beta_1/d, \ldots, \beta_m/d\}$. □

Let $\Lambda = \mathbb{Z}\alpha_1 \oplus \cdots \oplus \mathbb{Z}\alpha_n$ be a lattice of $\mathbb{R}^n$. Denote the fundamental parallelepiped for Λ by

$$\mathcal{D} = \left\{ \sum_{i=1}^{n} a_i\alpha_i \,|\, 0 \leq a_i < 1 \right\}.$$

Let $e_1, \ldots, e_n$ be a canonical basis of $\mathbb{R}^n$. Suppose $\alpha_i = \sum_{j=1}^{n} c_{ij}e_j$ with $c_{ij} \in \mathbb{R}$. Denote the volume of Λ by

$$V(\Lambda) = V(\mathbb{R}^n/\Lambda) = |\det(c_{ij})|.$$

The subset S of $\mathbb{R}^n$ is said to be *convex* if whenever $x, y \in S$ then the line connecting x and y lies entirely in S. And S is called *symmetric* about the origin if whenever $x \in S$ then $-x \in S$ also.

Corollary 1.27. *Let Λ be a lattice of $\mathbb{R}^n$. Then $\mathbb{R}^n/\Lambda$ is compact.*

Lemma 1.28. *(Minkowski's lattice point theorem) Let Λ be a lattice of $\mathbb{R}^n$, and let $S \subset \mathbb{R}^n$ be a convex compact subset which is symmetric with respect to the origin. If*

$$\mathrm{V}(S) \geq 2^n V(\Lambda),$$

then there exists $0 \neq \lambda \in S \cap \Lambda$.

Proof. Firstly, assume that $\mathrm{V}(S) > 2^n V(\Lambda)$, let us consider the map

$$\begin{aligned} \varphi : \ \frac{1}{2}S &\longrightarrow \mathbb{R}^n/\Lambda \\ x &\longmapsto x + \Lambda \end{aligned}$$

If φ is injective, then $V(\frac{1}{2}S) \leq V(\Lambda)$, hence $V(S) \leq 2^n V(\Lambda)$, a contradiction. Hence, there exist $x_1, x_2 \in \frac{1}{2}S$ and $x_1 \neq x_2$, such that $\varphi(x_1) = \varphi(x_2)$, and then $\varphi(x_1 - x_2) = 0$, and finally that $x_1 - x_2 \in \Lambda$. Since S is convex, $0 \neq \frac{1}{2}(x_1 - x_2) \in S$, then $0 \neq \frac{1}{2}(x_1 - x_2) \in S \cap \Lambda$.

If $V(S) = 2^n V(\Lambda)$, then for all $\epsilon > 0$, there exists a piont λ_ϵ such that $\lambda_\epsilon \in (1+\epsilon)S \cap \Lambda$ because $V((1+\epsilon)S) > V(S) = 2^n V(\Lambda)$. If $\epsilon < 1$, then the candidates for λ_ϵ lie in the bounded discrete set $2S \cap \Lambda$, so they belong to a finite set. Hence there exists nonzero $\lambda = \lambda_\epsilon \in (1+\epsilon)S \cap \Lambda$ for arbitrarily small ϵ. According to S is closed, we have $\lambda \in S \cap \Lambda$. □

Let $\sigma_1, \ldots, \sigma_{r_1}$ be r_1 real embeddings and $\sigma_{r_1+1} = \bar{\sigma}_{r_1+r_2+1}, \ldots, \sigma_{r_1+r_2} = \bar{\sigma}_n$ be r_2 pairs complex conjugate embeddings of k. We consider the following maping, called *canonical embedding* of k,

$$\begin{aligned} \sigma : k &\longrightarrow \mathbb{R}^n \\ \alpha &\longmapsto (\sigma_1\alpha, \ldots, \sigma_{r_1}\alpha, \Re\sigma_{r_1+1}\alpha, \ldots, \Re\sigma_{r_1+r_2}\alpha, \Im\sigma_{r_1+1}\alpha, \ldots, \Im\sigma_{r_1+r_2}\alpha). \end{aligned}$$

Lemma 1.29. *Let $\mathfrak{a}$ be any fractional ideal and σ be the canonical embedding of k. Then $\sigma(\mathfrak{a})$ is a lattice in $\mathbb{R}^n$, and*

$$V(\sigma(\mathfrak{a})) = 2^{-r_2}\sqrt{|d_k|}N(\mathfrak{a}).$$

Proof. Let $\alpha_1, \alpha_2, \ldots, \alpha_n$ be an integral basis of $\mathfrak{a}$, that is,

$$\mathfrak{a} = \mathbb{Z}\alpha_1 \oplus \cdots \oplus \mathbb{Z}\alpha_n.$$

Then

$$\sigma(\mathfrak{a}) = \mathbb{Z}\sigma\alpha_1 \oplus \cdots \oplus \mathbb{Z}\sigma\alpha_n.$$

As shows in the part above, $V(\sigma(\mathfrak{a}))$ is the absolute value of the determination of the matrix M

$$\begin{pmatrix} \sigma_1\alpha_1 & \cdots & \sigma_{r_1}\alpha_1 & \Re\sigma_{r_1+1}\alpha_1 & \cdots & \Re\sigma_{r_1+r_2}\alpha_1 & \Im\sigma_{r_1+1}\alpha_1 & \cdots & \Im\sigma_{r_1+r_2}\alpha_1 \\ \sigma_1\alpha_2 & \cdots & \sigma_{r_1}\alpha_2 & \Re\sigma_{r_1+1}\alpha_2 & \cdots & \Re\sigma_{r_1+r_2}\alpha_2 & \Im\sigma_{r_1+1}\alpha_2 & \cdots & \Im\sigma_{r_1+r_2}\alpha_2 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ \sigma_1\alpha_n & \cdots & \sigma_{r_1}\alpha_n & \Re\sigma_{r_1+1}\alpha_n & \cdots & \Re\sigma_{r_1+r_2}\alpha_n & \Im\sigma_{r_1+1}\alpha_n & \cdots & \Im\sigma_{r_1+r_2}\alpha_n \end{pmatrix}$$

By doing the column operators, we have

$$\begin{aligned} V(\sigma(\mathfrak{a})) &= |\det M| \\ &= \left|(-2i)^{-r_2}\right| \sqrt{d_{k/\mathbb{Q}}(\alpha_1, \alpha_2, \cdots, \alpha_n)} \\ &= 2^{-r_2}\sqrt{|d_k|}N(\mathfrak{a}). \end{aligned}$$

Since $\det M \neq 0$, show that $\sigma\alpha_1, \ldots, \sigma\alpha_n$ are $\mathbb{R}$-linearly independent. It follows that $\sigma(\mathfrak{a})$ is a lattice in $\mathbb{R}^n$. □

1.3.2 The class number

Let P_k denote the subgroup of J_k formed by the principal fractional ideals, that is, ideals of the form $(\alpha) = \alpha\mathfrak{o}_k$, for every $\alpha \in k^\times$. The *ideal class group* of k, denoted by $\mathcal{C}_k$, is

$$\mathcal{C}_k = J_k/P_k.$$

And we denoted by h_k the cardinality $\mathcal{C}_k$, called the *class number* of k. Before the proof of the class number is finite, we firstly prove the following lemma.

Lemma 1.30. *(1), Let $\mathfrak{a}$ be a nonzero fractional ideal of the number field k with $[k : \mathbb{Q}] = n = r_1 + 2r_2$. There exists a nonzero $\alpha \in \mathfrak{a}$, such that*

$$|N(\alpha)| \leq \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n}\sqrt{|d_k|}N(\mathfrak{a}). \tag{1.9}$$

(2) Every ideal calss of k contains an integral ideal $\mathfrak{a}$ such that

$$N(\mathfrak{a}) \leq \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n}\sqrt{|d_k|}. \tag{1.10}$$

Proof. (1) Let σ be the canonical mapping of k, and let $f : \mathbb{R}^n \to \mathbb{R}$ be the function defined by

$$f(x_1, \ldots, x_n) = \sum_{i=1}^{r_1} |x_i| + 2\sum_{j=1}^{r_2} \sqrt{x_{r_1+j}^2 + x_{r_1+r_2+j}^2}.$$

Write $S_t = \{x = (x_1, \ldots, x_n) \in \mathbb{R}^n : f(x) \leq t\}$, for any $t > 0$. It is easy to check that S_t is a convex compact subset of $\mathbb{R}^n$ which is symmetric about the origin. And we have

$$V(S_t) = \int \cdots \int_{f(x)\leq t} dx_1 \ldots dx_n = 2^{r_1}\left(\frac{\pi}{2}\right)^{r_2} \frac{t^n}{n!}.$$

By the lemma (1.29) and taking $t^n = (\frac{4}{\pi})^{r_2} n! \sqrt{|d_k|} N(\mathfrak{a})$, we have $V(S_t) = 2^n V(\sigma(\mathfrak{a}))$. There exists $0 \neq \alpha \in \mathfrak{a}$ such that $\sigma\alpha \in S_t$, that is, $f(\sigma\alpha) \leq t$. Therefore,

$$\begin{aligned} |N(\alpha)| &= \prod_{i=1}^{n} |\sigma_i(\alpha)| \leq \left(\frac{1}{n} \sum_{i=1}^{n} |\sigma_i(\alpha)| \right)^n \\ &= \frac{1}{n^n} (f(\sigma\alpha))^n \leq \frac{1}{n^n} t^n \\ &= \left(\frac{4}{\pi} \right)^{r_2} \frac{n!}{n^n} \sqrt{|d_k|} N(\mathfrak{a}). \end{aligned}$$

This completes the first part of the lemma.

(2), Suppose $\mathfrak{a}$ is any nonzero fractional ideal of $\mathfrak{o}_k$. Our goal is to prove there is an integral ideal $\alpha\mathfrak{a}$ with small norm. By the above, there exists a nonzero $\alpha \in \mathfrak{a}^{-1}$ such that

$$|N(\alpha)| \leq \left(\frac{4}{\pi} \right)^{r_2} \frac{n!}{n^n} \sqrt{|d_k|} / N(\mathfrak{a}).$$

The ideal $(\alpha)\mathfrak{a}$ is an integral ideal, say $\mathfrak{b}$. Then

$$N(\mathfrak{b}) = |N(\alpha)| N(\mathfrak{a}) \leq \left(\frac{4}{\pi} \right)^{r_2} \frac{n!}{n^n} \sqrt{|d_k|},$$

which proves the second part of the lemma. □

$M_k = \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} \sqrt{|d_k|}$ is called the *Minkowski's constant* of the number field k.

Theorem 1.31. *The class number of k is finite.*

Proof. We claim that there are only finitely many integral ideals $\mathfrak{a}$ of $\mathfrak{o}_k$ with norm at most any give positive integer q. Indeed, if $N(\mathfrak{a}) = m$, that is $|\mathfrak{o}_k/\mathfrak{a}| = m$, then $m \in \mathfrak{a}$, see exercis. It follows that

$$\mathfrak{a}|(m) = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g},$$

where $\mathfrak{p}_i$ are different prime ideals of $\mathfrak{o}_k$. the number of $\mathfrak{a}$ which satisfies $N(\mathfrak{a}) = m$ is finite. And then there are only finite integral ideals satisfy (1.10) and every ideal class of k contains also an integral ideal satisfy (1.10). Then the class number of k is finite. □

Corollary 1.32. *Suppose that $k \neq \mathbb{Q}$ is an algebraic number field. Then*

$$|d_k| \geq \left(\frac{\pi}{4} \right)^{r_2} \frac{n^n}{n!} > 1. \tag{1.11}$$

Gauss' class number problem: The problem of finding an effective algorithm to determine all imaginary quadratic fields with a given class number h is known as the Gauss class number problem. Stark (1967) and Baker (1966) gave independent proofs of the fact that only nine such numbers exist; both proofs were accepted.

1.3.3 Dirichlet's units theorem

We say a nonzero $\alpha \in \mathfrak{o}_k$ is a *unit* if $\alpha\beta = 1$ for some $\beta \in \mathfrak{o}_k$. Clearly, the units of $\mathfrak{o}_k$ form a group which in standard notation is just $\mathfrak{o}_k^*$ or U_k. $\omega \in k$ is called the *root of unity* if $\omega^m = 1$ for some integer m. All the roots of unity in k forms a group W_k.

Lemma 1.33. *W_k is a finite cyclic group. If H be a finite subgroup of $k^\times$, then $H \leq W_k$.*

Proof. Let z be an element of H whose order n is the exponent of H, that is, the least common multiple of the orders of all the elements of H. Then $y^n = 1$ for every $y \in H$, so H consists of roots of unity. Since the polynomial $X^n - 1$ has at most n distinct roots, we have $|H| \leq n$. But $1, z, \ldots, z^{n-1}$ are distinct elements of H, because z has order n. Thus H is cyclic. □

Lemma 1.34. *(1), $u \in U_k \iff N(u) = \pm 1$.*
(2), $u \in W_k \iff |\sigma_i(u)| = 1, i = 1, \ldots, n$.

Proof. (1), If u is a unit, then u^{-1} is also a unit, and $N(u), N(u^{-1})$ are integers. But $N(u)N(u^{-1}) = 1$, it follows that $\mathrm{N}(u) = \pm 1$.

Conversely, if $u \in \mathfrak{o}_k$ and $\mathrm{N}(u) = \pm 1$, then u is a root of the equation

$$f(x) = x^m + a_{m-1}x^{m-1} + \cdots + a_1 x \pm 1 \in \mathbb{Z}[X].$$

So, the u^{-1} is a root of the equation

$$g(x) = x^m \pm (a_1 x^{m-1} + \cdots + a_{m-1}x + 1) \in \mathbb{Z}[X].$$

Thus $u^{-1} \in \mathfrak{o}_k$, which implies $u \in U_k$.

(2), If $u \in W_k$, then there is m satisfies $u^m = 1$. And then $|\sigma_i(u)|^m = |\sigma_i(u^m)| = 1$, it follows that $|\sigma_i(u)| = 1$, for every $i = 1, \ldots, n$.

Conversely, if $|\sigma_i(u)| = 1, i = 1, \ldots, n$, then $\sigma_i(u) = e^{2\pi i n_i/m_i}$, where $0 \leq n_i/m_i < 1, n_i, m_i \in \mathbb{Z}$, and $(n_i, m_i) = 1$. So $(\sigma_i(u))^{m_i} = 1$, specially the embedding is identity, we have $u^m = 1$. Thus $u \in W_k$. □

Theorem 1.35. *(Dirichlet's unit theorem)*

$$U_k \cong W_k \otimes \mathbb{Z}^r$$

where $r = r_1 + r_2 - 1$. *That is, there exist* r *units* $\{\epsilon_1, \ldots, \epsilon_r\}$ *such that every unit* u *of* $\mathfrak{o}_k$ *can be expressed uniquely as*

$$u = \omega \epsilon_1^{n_1} \cdots \epsilon_r^{n_r}, \tag{1.12}$$

where the $\omega \in W_k$ *and* $n_i \in \mathbb{Z}$.

Proof. Let $\sigma : k \to \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \simeq \mathbb{R}^n$ be the canonical embedding of k. The logarithmic embedding of k is the mapping

$$\begin{aligned} \lambda : U_k &\longrightarrow \mathbb{R}^{r_1+r_2} \\ \alpha &\longmapsto (\log|\sigma_1(\alpha)|, \ldots, \log|\sigma_{r_1+r_2}(\alpha)|). \end{aligned}$$

Since $\lambda(\alpha\beta) = \lambda(\alpha) + \lambda(\beta)$, λ is a homomorphism from multiplicative group U_k to the additive group of $\mathbb{R}^{r_1+r_2}$.

- The image of λ lies in the hyperplane:

$$x_1 + \cdots + x_{r_1} + 2x_{r_1+1} + \cdots 2x_{r_1+r_2} = 0.$$

If $\alpha \in U_k$, then by the Lemma (1.34),

$$\sum_{i=1}^{r_1+r_2} \lambda_i \log|\sigma_i(\alpha)| = \sum_{i=1}^{n} \log|\sigma_i(\alpha)| = \log|N(\alpha)| = 0,$$

with $\lambda_i = 1, i = 1, \ldots, r_1$ and $\lambda_i = 2, i = r_1 + 1, \ldots, r_1 + r_2$. Clearly, the hyperplane has dimension $r = r_1 + r_2 - 1$.

- The kernel of λ consists of exactly all the roots of unity W_k.

$$\begin{aligned} \alpha \in \ker\lambda &\Leftrightarrow \log|\sigma_i(\alpha)| = 0, i = 1, \ldots, r_1 + r_2 \\ &\Leftrightarrow |\sigma_i(\alpha)| = 1, i = 1, \ldots, n \\ &\Leftrightarrow \alpha \in W_k. \end{aligned}$$

- The image of λ is a discrete subgroup of $\mathbb{R}^{r_1+r_2}$.

That is, any bounded subset of $\mathbb{R}^{r_1+r_2}$ contains only finitely many points of $\lambda(U_k)$. Thus $\lambda(U_k)$ is a lattice in $\mathbb{R}^s$, hence a free $\mathbb{Z}$-module of rank s, for some $s \leq r_1 + r_2$. Now by the first isomorphism theorem, we have that

$$\lambda(U_k) \simeq U_k / W_k$$

with $\lambda(x)$ corresponding to the coset xW_k.

In order to do so, we prove that if C is a bounded subset of $\mathbb{R}^{r_1+r_2}$, then $C' = \{x \in U_k \,|\, \lambda(x) \in C\}$ is a finite set.

Since C is bounded, all $|\sigma_i(x)|$, $x \in U_k$, $i = 1, \ldots, n$ belong to some interval say $[a^{-1}, a], a > 1$. Thus the elementary polynomials in the $\sigma_i(x)$ will also belong to some interval of the same form. Now they are the coefficients of the characteristic polynomial of x_i, which has integer coefficients since $x \in U_k$. Thus there are only finitely many possible characteristic polynomials of elements $x \in C'$, hence only finitely many possible roots of minimal polynomials of elements $x \in C'$, which shows that x can belong to C' for only finitely many x.

• The kernel of λ is a finite group.

Now if we set $C = 0$, C' is the kernel $\ker(\lambda)$ of λ restricted to U_k and is thus finite.

• U_k is a finite generated abelian group, isomorphic to $\mu(\mathfrak{o}_k)\times\mathbb{Z}^s$, $s \leq r_1+r_2$.

If $x_1\mu(\mathfrak{o}_k), \ldots, x_s\mu(\mathfrak{o}_k)$ form a basis for $U_k/\mu(\mathfrak{o}_k)$ and $x \in U_k$, then $x\mu(\mathfrak{o}_k)$ is a finite product of powers of the x_iG, so x is an element if $\mu(\mathfrak{o}_k)$ times a finite product of powers of x_i. Since the $\lambda(x_i)$ are linearly independent, so are the x_i (provided that the notion of linear independence is translated to a multiplicative setting: $x_1, \ldots, x_s$ are multiplicatively independent if $x_1^{m_1} \cdots x_s^{m_s} = 1$ implies that $m_i = 0$ for all i, from which it follows that $x_1^{m_1} \cdots x_s^{m_s} = x_1^{n_1} \cdots x_s^{n_s}$ implies $m_i = n_i$ for all i). The result follows.

We now improve the estimate of s and show that $s \leq r_1 + r_2 - 1$. so as above, $\lambda(U_k)$ is free $\mathbb{Z}$-module of rank $s \leq r_1 + r_2 - 1$. □

We call $\{\epsilon_1, \ldots, \epsilon_r\}$ in (1.12) a *fundamental system of units* for the number field k. Let $\{\epsilon_1, \ldots, \epsilon_r\}$ be a fundamental system of generators of k modulo roots of unity (this is, modulo the torsion subgroup). Let M be the $r \times (r+1)$ matrix

$$\begin{pmatrix} \log|\sigma_1(\epsilon_1)| & \cdots & \log|\sigma_{r_1}(\epsilon_1)| & 2\log|\sigma_{r_1+1}(\epsilon_1)| & \cdots & 2\log|\sigma_{r+1}(\epsilon_1)| \\ \log|\sigma_1(\epsilon_2)| & \cdots & \log|\sigma_{r_1}(\epsilon_2)| & 2\log|\sigma_{r_1+1}(\epsilon_2)| & \cdots & 2\log|\sigma_{r+1}(\epsilon_2)| \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ \log|\sigma_1(\epsilon_r)| & \cdots & \log|\sigma_{r_1}(\epsilon_r)| & 2\log|\sigma_{r_1+1}(\epsilon_r)| & \cdots & 2\log|\sigma_{r+1}(\epsilon_r)| \end{pmatrix}$$

and let M_j be the $r \times r$ matrix

$$(\lambda_i \log|\sigma_i(\epsilon_j)|)_{r\times r}$$

where $\lambda_i = 1$ if σ_i is a real embedding and $\lambda_i = 2$ if σ_i is a complex embedding, obtained by deleting any jth-column. It can be checked that the determinant of M_j, is independent up to sign of the choice of fundamental system of generators of k and is also independent of the choice of j. The

absolute value of the determinant of the matrix M_j is called the *regulator* of the number field k, say R_k. The regulator is one of the main ingredients in the analytic class number formula for number fields.

1.3.4 Units in quadratic fields

Imaginary quadratic fields:

Let $k = \mathbb{Q}(\sqrt{-d})$ be an imaginary quadratic field. There are no real embeddings, so $r_1 = 0, r_2 = 1$ and $r = r_1 + r_2 - 1 = 0$, the only units in $\mathfrak{o}_k$ are the roots of unity in k.

$$U_k \cong W_k = \begin{cases} \langle i \rangle, & \text{as } k = \mathbb{Q}(\sqrt{-1}) \\ \langle \rho | \rho = \frac{1+\sqrt{-3}}{2} \rangle, & \text{as } k = \mathbb{Q}(\sqrt{-3}) \\ \langle -1 \rangle, & \text{otherwise.} \end{cases}$$

Real quadratic fields:

Let $k = \mathbb{Q}(\sqrt{d})$ be a real quadratic field. Since the $\mathbb{Q}$-automorphisms of k are the identity and $\tau : \alpha + \beta\sqrt{d} \mapsto \alpha - \beta\sqrt{d}$, there are two real embeddings and no complex embeddings. Thus $r_1 = 2, r_2 = 0$ and $r = r_1 + r_2 - 1 = 1$. The only roots of unity in $\mathbb{R}$ are ± 1. By Dirichlet's unit theorem, the group of units in the ring of algebraic integers is isomorphic to

$$U_k \cong \{\pm 1\} \times u^{\mathbb{Z}} \cong \{\pm 1\} \times \mathbb{Z}.$$

If u a unit, then $\pm u, \pm u^{-1}$ are also units. The unique generator greater than 1 is called the *fundamental unit* of k.

1.4 Extensions of Fields

Let K/k be an extension of algebraic number fields with $[K : k] = n$, and let $\mathfrak{p}$ be a prime ideal of $\mathfrak{o}_k$. Let $\mathfrak{p}\mathfrak{O}_K$ denote the ideal of $\mathfrak{O}_K$ generated by $\mathfrak{p}$; it consists of all finite sums $\sum \alpha\pi$ with $\alpha \in \mathfrak{O}_K, \pi \in \mathfrak{p}$. The ideal $\mathfrak{p}\mathfrak{O}_K$ is not in general prime ideal. In this section, we will consider the following general problem: Given any prime ideal $\mathfrak{p}$ of $\mathfrak{o}_k$, determine the factorization of $\mathfrak{p}\mathfrak{O}_K$ into prime ideals of $\mathfrak{O}_K$.

1.4.1 Factoring of prime ideals in extensions

Recall: Finite Fields (1), Let E be a finite field of characteristic p. Then $|E| = p^n$ for some positive integer n. Moreover, E is a splitting field for the separable polynomial $f(X) = X^{p^n} - X$ over $\mathbb{F}_p$, so that any finite field with p^n elements is isomorphic to E.

(2), If E is a finite field of characteristic p, then $E/\mathbb{F}_p$ is a Galois extension. The Galois group is cyclic and is generated by the Frobenius automorphism $\sigma(x) = x^p, x \in E$.

(3), Let E/F be a finite extension of a finite field, with $|E| = p^n, |F| = p^m$. Then E/F is a Galois extension. Moreover, $m|n$, and $\mathrm{Gal}(E/F)$ is cyclic and is generated by the automorphism $\tau(x) = x^{p^m}, x \in E$. Furthermore, F is the only subfield of E of size p^m.

(4), The multiplicative group of a finite field is cyclic. More generally, if G is a finite subgroup of the multiplicative group of an arbitrary field, then G is cyclic.

(5), $GF(p^m)$ is a subfield of $GF(p^n)$ if and only if m is a divisor of n.

For more details, we refer the reader to [1] or [5].

Let K/k be a finite extension of algebraic number fields with $[K : k] = n$ and $\mathfrak{p}$ be a prime ideal of $\mathfrak{o}_k$. Let $\mathfrak{p}\mathfrak{O}_K$ be written in a unique way as

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

where $\mathfrak{P}_1, \ldots, \mathfrak{P}_g$ are distinct prime ideals of $\mathfrak{O}_K$ and the e_i are positive integers. Then the $\mathfrak{P}_i$ are called the *prime divisors* of $\mathfrak{p}$ in K by writing $\mathfrak{P}|\mathfrak{p}$. If $\mathfrak{P}|\mathfrak{p}$, then $\mathfrak{p}$ is called the *restriction* of $\mathfrak{P}$ to k, or that $\mathfrak{P}$ lies over $\mathfrak{p}$ ($\mathfrak{P}$ is above $\mathfrak{p}$) since $\mathfrak{P} \cap \mathfrak{o}_k = \mathfrak{p}$. We then actually have the following lemma.

Lemma 1.36. *Let K/k be a finite extension of algebraic number fields and $\mathfrak{P}$ be a prime ideal of $\mathfrak{O}_K$. Then*

(1), $\mathfrak{p} = \mathfrak{P} \cap \mathfrak{o}_k$ is a prime ideal of $\mathfrak{o}_k$; and $\mathfrak{p} = \mathfrak{P} \cap \mathfrak{o}_k \Leftrightarrow \mathfrak{P}|\mathfrak{p}$;

(2), If $\mathfrak{p} = \mathfrak{P} \cap \mathfrak{o}_k$, then the residue class field $\mathfrak{o}_k/\mathfrak{p}$ is a subfield of the finite field $\mathfrak{O}_K/\mathfrak{P}$. In particular, the finite field $\mathfrak{o}_k/\mathfrak{p}$ has characteristic p where p is the restriction of $\mathfrak{p}$ in $\mathbb{Z}$.

Proof. (1), Clearly, $\mathfrak{P} \cap \mathfrak{o}_k$ is an ideal of $\mathfrak{o}_k$. For any $\alpha, \beta \in \mathfrak{o}_k$ and $\alpha\beta \in \mathfrak{P} \cap \mathfrak{o}_k$, then $\alpha \in \mathfrak{P}$ or $\beta \in \mathfrak{P}$. Hence, $\alpha \in \mathfrak{P} \cap \mathfrak{o}_k$ or $\beta \in \mathfrak{P} \cap \mathfrak{o}_k$. It follows that $\mathfrak{P} \cap \mathfrak{o}_k$ is prime.

If $\mathfrak{p} = \mathfrak{P} \cap \mathfrak{o}_k$, then $\mathfrak{p} \subset \mathfrak{P}$. Hence $\mathfrak{p}\mathfrak{O}_K \subset \mathfrak{P}$, and then $\mathfrak{P}|\mathfrak{p}\mathfrak{O}_K$. Conversely, assume that $\mathfrak{P}|\mathfrak{p}$, hence contains $\mathfrak{p}\mathfrak{O}_K \subset \mathfrak{P}$. Then

$$\mathfrak{p} = \mathfrak{p} \cap \mathfrak{o}_k \subset \mathfrak{p}\mathfrak{O}_K \cap \mathfrak{o}_k \subset \mathfrak{P} \cap \mathfrak{o}_k.$$

We have $\mathfrak{p} = \mathfrak{P} \cap \mathfrak{o}_k$, because every nonzero prime ideal is maximal in the Dedekind domain $\mathfrak{o}_k$.

(2), Let φ be the mapping

$$\begin{aligned} \varphi : \mathfrak{o}_k &\longrightarrow \mathfrak{O}_K/\mathfrak{P} \\ \alpha &\longmapsto \alpha + \mathfrak{P}. \end{aligned}$$

It's easily check that φ is a homomorphism of rings, and $\ker \varphi = \mathfrak{P} \cap \mathfrak{o}_k = \mathfrak{p}$. By the homomorphism, we may view $\mathfrak{o}_k/\mathfrak{p}$ as a subring of $\mathfrak{O}_K/\mathfrak{P}$, hence $\mathfrak{O}_K/\mathfrak{P}$ a finite dimensional vector space over the finite field $\mathfrak{o}_k/\mathfrak{p}$. □

If we lift $\mathfrak{p}$ to $\mathfrak{O}_K$ and factor $\mathfrak{p}\mathfrak{O}_K$ as $\mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}$, that is,

$$\mathfrak{p}\mathfrak{O}_K = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}, \tag{1.13}$$

the positive integer $e(\mathfrak{P}_i/\mathfrak{p}) = e_i$ is called the *ramification index* of $\mathfrak{P}_i$ over $\mathfrak{p}$. The degree $[\mathfrak{O}_K/\mathfrak{P}_i : \mathfrak{o}_k/\mathfrak{p}] = f(\mathfrak{P}_i/\mathfrak{p}) = f_i$ of the finite fields extension is called the *residue class degree (inertial degree)* of $\mathfrak{P}_i$ over $\mathfrak{p}$. The integer g is called the *degree of split*(*decomposition number*) of $\mathfrak{p}$.

Theorem 1.37.

$$\sum_{i=1}^{g} e_i f_i = [\mathfrak{O}_K/\mathfrak{p}\mathfrak{O}_K : \mathfrak{o}_k/\mathfrak{p}] = [K : k]. \tag{1.14}$$

Proof. Taking norm form two sides (1.13), we have

$$\begin{aligned} N(\mathfrak{p}\mathfrak{O}_K) &= \prod_{i=1}^{g} N(\mathfrak{P}_i)^{e_i} = \prod_{i=1}^{g} |\mathfrak{O}_K/\mathfrak{P}_i|^{e_i} \\ &= \prod_{i=1}^{g} |\mathfrak{o}_k/\mathfrak{p}|^{f_i e_i} = |\mathfrak{o}_k/\mathfrak{p}|^{\sum_{i=1}^{g} e_i f_i} = N(\mathfrak{p})^{\sum_{i=1}^{g} e_i f_i}. \end{aligned}$$

On the other hand, denote the mapping ϕ by

$$\begin{aligned} \phi : \mathfrak{o}_k &\longrightarrow \mathfrak{O}_K/\mathfrak{p}\mathfrak{O}_K \\ \alpha &\longmapsto \alpha + \mathfrak{p}\mathfrak{O}_K. \end{aligned}$$

It is easily seen that the mapping ϕ is a ring homomorphism and its kernel is $\mathfrak{p}$. Then the ring $V = \mathfrak{O}_K/\mathfrak{p}\mathfrak{O}_K$ can be look as a vector space over the finite field $\mathbb{F}_\mathfrak{p} = \mathfrak{o}_k/\mathfrak{p}$. It follows that

$$N(\mathfrak{p}\mathfrak{O}_K) = |\mathfrak{O}_K/\mathfrak{p}\mathfrak{O}_K| = |\mathfrak{o}_k : \mathfrak{p}|^{\dim_{\mathbb{F}_\mathfrak{p}} V} = N(\mathfrak{p})^{\dim_{\mathbb{F}_\mathfrak{p}} V},$$

hence that $\sum_{i=1}^{g} e_i f_i = \dim_{\mathbb{F}_\mathfrak{p}} V$. Now, it sufficient to show that $\dim_{\mathbb{F}_\mathfrak{p}} V = [\mathfrak{O}_K/\mathfrak{p}\mathfrak{O}_K : \mathfrak{o}_k/\mathfrak{p}] = n$.

• We claim that $\dim_{\mathbb{F}_\mathfrak{p}} V \leq n$.

Let $x_1, \ldots, x_{n+1}$ be any elements of $\mathfrak{O}_K$. Since $[K : k] = n$, there exist $\alpha_1, \ldots, \alpha_{n+1} \in k$ which are not all zeros such that

$$\alpha_1 x_1 + \cdots + \alpha_{n+1} x_{n+1} = 0.$$

Without loss of generality we can assume that $\alpha_1, \ldots, \alpha_{n+1} \in \mathfrak{o}_k$. Let $\mathfrak{a} = (\alpha_1, \ldots, \alpha_{n+1})$ be an ideal of $\mathfrak{o}_k$. There exists an integral ideal $\mathfrak{b}$ such that $\mathfrak{a}\mathfrak{b} = (\alpha) \nsubseteq (\alpha)\mathfrak{p}$ where $\alpha \in \mathfrak{o}_k$ by the exercise. It follows that there is $\beta \in \mathfrak{b}$ such that $\beta\mathfrak{a} \nsubseteq (\alpha)\mathfrak{p}$. Therefore $(\beta/\alpha)\mathfrak{a} = \beta\mathfrak{b}^{-1} \subset \mathfrak{o}_k$, and then we obtain $(\beta/\alpha)\alpha_i \in \mathfrak{o}_k$ for $1 \leq i \leq n+1$.

On the other hand, we have $(\beta/\alpha)\mathfrak{a} \nsubseteq \mathfrak{p}$. Then there exists j such that $(\beta/\alpha)\alpha_j \notin \mathfrak{p}$. In other words, set $\gamma_i = (\beta/\alpha)\alpha_i$, then $\gamma_i \in \mathfrak{o}_k$ for $1 \leq i \leq n+1$ but $\gamma_j \notin \mathfrak{p}$ for some j. Hence $\overline{\gamma_j} \neq \overline{0}$ in the residue field $\mathfrak{o}_k/\mathfrak{p}$. Multiplying by β/α, we have

$$\gamma_1 x_1 + \cdots + \gamma_{n+1} x_{n+1} = 0.$$

Let

$$\bar{\gamma}_1 \bar{x}_1 + \cdots + \bar{\gamma}_{n+1} \bar{x}_{n+1} = \bar{0}$$

be reductions mod $\mathfrak{p}\mathfrak{O}_K$ of the above equation. It follows that any $n+1$ elements $\bar{x}_1, \ldots, \bar{x}_{n+1}$ of $\mathfrak{O}_K/\mathfrak{p}\mathfrak{O}_K$ are linearly dependent because $\bar{\gamma}_1, \ldots, \bar{\gamma}_{n+1}$ are not all zeros. Hence $\dim_{\mathbb{F}_\mathfrak{p}} V \leq n$, which is our claim.

• We have $\dim_{\mathbb{F}_\mathfrak{p}} V = n$ when $k = \mathbb{Q}$.

Let

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

By Theorem (1.25), we have

$$N(p\mathfrak{O}_K) = |N_{K/\mathbb{Q}}(p)| = p^n.$$

Therefore, we get $\dim_{\mathbb{F}_p} V = \sum_{i=1}^{g} e_i f_i = n$.

• We have $\dim_{\mathbb{F}_\mathfrak{p}} V = n$ for any number field k.

Let $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$ and

$$p\mathfrak{o}_k = \mathfrak{p}_1^{\tilde{e}_1} \cdots \mathfrak{p}_r^{\tilde{e}_r},$$

where $\tilde{e}_i = e(\mathfrak{p}_i/p)$ and $\tilde{f}_i = f(\mathfrak{p}_i/p)$. Then $\sum_{i=1}^{r} \tilde{e}_i\tilde{f}_i = [k : \mathbb{Q}] = m$ and $\mathfrak{p}_j = \mathfrak{p}$ for some $1 \leq j \leq r$. Setting $[\mathfrak{O}_K/\mathfrak{p}_i\mathfrak{O}_K : \mathfrak{o}_k/\mathfrak{p}_i] = \tilde{n}_i$, we have $\tilde{n}_i \leq n$. Since

$$p\mathfrak{O}_K = (p\mathfrak{o}_k)\mathfrak{O}_K = (\mathfrak{p}_1\mathfrak{O}_K)^{\tilde{e}_1} \cdots (\mathfrak{p}_r\mathfrak{O}_K)^{\tilde{e}_r},$$

we see that

$$\begin{aligned} |\mathfrak{O}_K/p\mathfrak{O}_K| &= N(p\mathfrak{O}_K) = \prod_{i=1}^{r} N_K(\mathfrak{p}_i\mathfrak{O}_K)^{\tilde{e}_i} \\ &= \prod_{i=1}^{r} |\mathfrak{O}_K/\mathfrak{p}_i\mathfrak{O}_K|^{\tilde{e}_i} = \prod_{i=1}^{r} |\mathfrak{o}_k/\mathfrak{p}_i|^{\tilde{n}_i\tilde{e}_i} \\ &= \prod_{i=1}^{r} p^{\tilde{n}_i\tilde{e}_i\tilde{f}_i} = p^{\sum_{i=1}^{r} \tilde{n}_i\tilde{e}_i\tilde{f}_i}. \end{aligned}$$

On the other hand, we have

$$|\mathfrak{O}_K/p\mathfrak{O}_K| = p^{[K:\mathbb{Q}]} = p^{[K:k][k:\mathbb{Q}]} = p^{mn}$$

which follows that

$$mn = \sum_{i=1}^{r} \tilde{n}_i\tilde{f}_i\tilde{e}_i \leq n\sum_{i=1}^{r} \tilde{f}_i\tilde{e}_i = nm.$$

Thus $\tilde{n}_i = n$ for any $i = 1, 2, \ldots, r$. In particular, we have $\tilde{n}_j = n$ which completes the proof. □

Definition 1.38. *Let k, K and $\mathfrak{p}, \mathfrak{P}_i$ be as above.*

(1), If $e_i = 1$ for some i, then we say that $\mathfrak{P}_i$ unramifies over $\mathfrak{p}$. If $e_i > 1$ for some i, then we say that $\mathfrak{P}_i$ ramifies over $\mathfrak{p}$ and $\mathfrak{p}$ ramifies over in K/k. If $e_i = 1$ for all i then we say that $\mathfrak{p}$ is unramified in K/k.

(2), Let p be the characteristic of the residue field $\mathfrak{o}_k/\mathfrak{p}$. If $e_i > 1$ and $p \nmid e_i$, then we say that $\mathfrak{P}_i$ is tamely ramified. If $p|e_i$ then we say that $\mathfrak{P}_i$ is wildly ramified.

(3), The prime ideal $\mathfrak{p}$ is totally split in K if $g = n$; totally ramified if $e = n$; undecomposed (interia) if $f = n$.

Lemma 1.39. *Let $k \subset L \subset K$ be a finite extension of number fields. Let $\mathfrak{P}$ be a prime ideal of $\mathfrak{O}_K$, $\mathfrak{P}_L = \mathfrak{P} \cap \mathfrak{O}_L$ and $\mathfrak{p} = \mathfrak{P} \cap \mathfrak{o}_k$. Then*

$$\begin{aligned} e(\mathfrak{P}/\mathfrak{p}) &= e(\mathfrak{P}/\mathfrak{P}_L)e(\mathfrak{P}_L/\mathfrak{p}), \\ f(\mathfrak{P}/\mathfrak{p}) &= f(\mathfrak{P}/\mathfrak{P}_L)f(\mathfrak{P}_L/\mathfrak{p}). \end{aligned}$$

Proof. Clearly. □

An efficient factorization of a rational prime in a number field

Theorem 1.40. *(Dedekind-Kummer Theorem) Suppose that there is an element $\alpha \in k$ such that $\mathfrak{o}_k = \mathbb{Z}[\alpha]$. Let $f(x)$ be the minimal polynomial of α over $\mathbb{Z}[\alpha]$. Let p be a rational prime and suppose*

$$f(x) \equiv f_1(x)^{e_1} \cdots f_g(x)^{e_g} (\mathrm{mod}\, p),$$

where each $f_i(x)$ is irreducible in $\mathbb{F}_p[X]$. Then

$$p\mathfrak{o}_k = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g}$$

where $\mathfrak{p}_i = (p, f_i(\alpha))$ are prime ideals, with $N(\mathfrak{p}_i) = p^{\deg f_i}$.

Proof. We first note that

$$(p, f_1(\alpha))^{e_1} \cdots (p, f_g(\alpha))^{e_g} \subset p\mathfrak{o}_k.$$

Thus it suffices to show that $\mathfrak{p}_i = (p, f_i(\alpha))$ are prime ideals, with $N(\mathfrak{p}_i) = p^{d_i}, d_i = \deg f_i$.

Now, since $f_i(x)$ is irreducible over $\mathbb{F}_p[X]$, then $\mathbb{F}_p[X]/(f_i(x))$ is a field. Also

$$\mathbb{Z}[X]/(p) \cong \mathbb{F}_p[X] \Rightarrow \mathbb{Z}[X]/(p, f_i(x)) \cong \mathbb{F}_p[X]/(f_i(x)),$$

and so $\mathbb{Z}[X]/(p, f_i(x))$ is a field.

Consider the map $\varphi : \mathbb{Z}[X] \to \mathbb{Z}[\alpha]/(p, f_i(\alpha))$, Clearly

$$(p, f_i(x)) \subset \ker(\varphi) = \{n(x) : n(\alpha) \in (p, f_i(\alpha))\}$$

If $n(x) \in \ker(\varphi)$, we can divide by $f_i(x)$ to get

$$n(x) = q(x)f_i(x) + r_i(x), \deg(r_i) < \deg(f_i)$$

We assume that r_i is nonzero, for otherwise the result is trivial. Since $n(\alpha) \in (p, f_i(\alpha))$, then $r_i(\alpha) \in (p, f_i(\alpha))$, so $r_i(\alpha) = pa(\alpha) + f_i(\alpha)b(\alpha)$. Here we have used the fact that $\mathfrak{o}_k = \mathbb{Z}[\alpha]$.

Now define the polynomial $h(x) = r_i(x) - pa(x) - f_i(x)b(x)$. Since $h(\alpha) = 0$ and f is the minimal polynomial of α, then $h(x) = g(x)f(x)$ for some polynomial $g(x) \in \mathbb{Z}[X]$. We conclude that $r_i(x) = p\tilde{a}(x) + f_i(x)\tilde{b}(x)$ for some $\tilde{a}(x), \tilde{b}(x) \in \mathbb{Z}[X]$. Therefore $r_i(x) \in (p, f_i(x))$.

Thus,

$$\mathbb{Z}[\alpha]/(p, f_i(\alpha)) \cong \mathbb{Z}[X]/(p, f_i(x)) \cong \mathbb{F}_p[X]/(f_i(x))$$

and is therefore a field. Hence,$(p, f_i(\alpha))$ is a maximal ideal and is therefore prime.

Now, let h_i be the ramification index of $\mathfrak{p}_i$, so that

$$p\mathfrak{o}_k = \mathfrak{p}_1^{h_1} \cdots \mathfrak{p}_g^{h_g},$$

and let $d_i = [\mathfrak{o}_k/\mathfrak{p}_i : \mathbb{Z}/p\mathbb{Z}]$. Clearly d_i is the degree of the polynomial $f_i(x)$. Since $f(\alpha) = 0$, and since $f(x) - f_1(x)^{e_1} \cdots f_g(x)^{e_g} \in p\mathbb{Z}[X]$. Also, $\mathfrak{p}_i^{e_i} \subset p\mathfrak{o}_k + (f_i(x)^{e_i})$ and so

$$\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g} \subset p\mathfrak{o}_k = \mathfrak{p}_1^{h_1} \cdots \mathfrak{p}_g^{h_g}.$$

Therefore, $e_i \geq h_i$ for all i. But

$$\sum e_i d_i = \deg f = [K : \mathbb{Q}] = \sum h_i d_i$$

Thus, $e_i = h_i$ for all i. □

The above theorem gives a concrete method to compute the factorization of a prime p in $\mathfrak{o}_k$:

(1), Let $f(x)$ be the minimal polynomial of α such that $\mathfrak{o}_k = \mathbb{Z}[\alpha]$.

(2), Compute the factorization of $\widetilde{f}(x) = f(x) \mod p$: $\widetilde{f}(x) = \prod_{i=1}^{g} f_i(x)^{e_i}$.

(3), Compute $\mathfrak{p}_i = (p, f_i(\alpha))$.

Examples 1.41. *1, Let us consider $k = \mathbb{Q}(\sqrt[3]{2})$ with ring of integers $\mathfrak{o}_k = \mathbb{Z}[\sqrt[3]{2}]$. We want to factorize $5\mathfrak{o}_k$. By the above theorem, we compute*

$$x^3 - 2 \equiv (x+2)(x^2 - 2x - 1) \mod 5.$$

We thus get that

$$5\mathfrak{o}_k = \mathfrak{p}_1\mathfrak{p}_2 = (5, 2 + \sqrt[3]{2})(5, \sqrt[3]{4} - 2\sqrt[3]{2} - 1).$$

2, As all know, there are two essentially different factorizations into prime elements

$$21 = 3 \cdot 7 = (1 + 2\sqrt{-5})(1 - 2\sqrt{-5})$$

in the ring $\mathfrak{o}_k = \mathbb{Z}[\sqrt{-5}]$. By the above theorem, we have the decompositions of prime ideals

$$\begin{aligned} (3) &= \mathfrak{p}_1\mathfrak{p}_2 \stackrel{\text{def}}{=} (3, \sqrt{-5} - 1)(3, \sqrt{-5} - 2) \\ (7) &= \mathfrak{p}_3\mathfrak{p}_4 \stackrel{\text{def}}{=} (7, \sqrt{-5} - 3)(7, \sqrt{-5} - 4). \end{aligned}$$

This is implied by the decompositions:

$$x^2+5 \equiv (x-1)(x-2)(\mathrm{mod}3),\ x^2+5 \equiv (x-3)(x-4)(\mathrm{mod}7).$$

We also have

$$(1+2\sqrt{-5}) = \mathfrak{p}_1\mathfrak{p}_3,\ (1-2\sqrt{-5}) = \mathfrak{p}_2\mathfrak{p}_4.$$

Then the factorization $(21) = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4$ *is unique decomposition as a product of four prime ideals of* $\mathfrak{o}_k$.

1.4.2 Applications in special fields

Theorem 1.42. *Let* $k = \mathbb{Q}(\sqrt{d})$ *be any quadratic field where* d *is a square-free integer.*

(1), If $p|d_k$, *then* $p\mathfrak{o}_k = \mathfrak{p}^2$ *and* $N(\mathfrak{p}) = p$, *i.e.,* p *is totally ramified.*

(2), Assume that $p > 2$ *and* $p \nmid d_k$.

(i), If $(\frac{d}{p}) = 1$, *then we have* $p\mathfrak{o}_k = \mathfrak{p}_1\mathfrak{p}_2, \mathfrak{p}_1 \neq \mathfrak{p}_2$ *and* $N(\mathfrak{p}_1) = N(\mathfrak{p}_2) = p$, *i.e.,* p *is totally splits.*

(ii), If $(\frac{d}{p}) = -1$, *then we have* $p\mathfrak{o}_k = \mathfrak{p}, N(\mathfrak{p}) = p^2$, *i.e.,* p *is interia*

(3), Assume that $p = 2$ *and* $p \nmid d_k$.

(i), If $d \equiv 1(\mathrm{mod}8)$, *then* 2 *is* p *is totally splits in* $k/\mathbb{Q}$.

(ii), If $d \equiv 5(\mathrm{mod}8)$, *then* 2 *is* p *is interia.*

Corollary 1.43. *A positive integer* n *is a sum of two squares if and only if* m *is even where* $p^m \parallel n$ *for all primes* $p \equiv 3(\mathrm{mod}4)$.

1.4.3 Relative norms

Let $k \subset K$ be algebraic number fields. Let J_k and J_K be the groups of fractional ideals of k and K respectively. We can also generalize the *relative norm* by multiplicativity as follows:

$$\begin{aligned} N_{K/k} : J_K &\to J_k \\ \mathfrak{P} &\mapsto \mathfrak{p}^{f(\mathfrak{P}/\mathfrak{p})}, \end{aligned}$$

which is a group homomorphism. This definition may be extended to each nonzero fractional ideal $\mathfrak{A} \in J_K$. Note that this defines a relative norm for ideals, which is itself an ideal.

Proposition 1.44. *Let* $N_{K/k}$ *be the relative norm of number fields* K/k *with* $n = [K : k]$.

(1), For every $\mathfrak{a} \in J_k$, $N_{K/k}(\mathfrak{a}\mathfrak{O}_K) = \mathfrak{a}^n$.

(2), For $k = \mathbb{Q}$ and each nonzero fractional ideal $\mathfrak{A}$ of K, we have

$$N_{K/\mathbb{Q}}(\mathfrak{A}) = N(\mathfrak{A})\mathbb{Z},$$

where $N(\mathfrak{A}) = |\mathfrak{O}_K : \mathfrak{A}|$ is the absolute norm.

(3), Let $k \subset L \subset K$ be an extension of number fields. Then

$$N_{K/k} = N_{L/k} \circ N_{K/L}.$$

Proof. (1), Due to the multiplicativity of the relative norm of an ideal, it suffices to prove this for a prime ideal $\mathfrak{p} \in J_k$. Let

$$\mathfrak{p}\mathfrak{O}_K = \mathfrak{P}_1^{e_1}\mathfrak{P}_2^{e_2}\cdots\mathfrak{P}_g^{e_g},$$

where $\mathfrak{P}_i$ are distinct prime ideals of $\mathfrak{O}_K$ and $|\mathbb{F}_{\mathfrak{P}_i}| = f_i$. Then we have

$$N_{K/k}(\mathfrak{p}\mathfrak{O}_K) = \prod_{i=1}^{g} N_{K/k}(\mathfrak{P}_i)^{e_i} = \prod_{i=1}^{g} \mathfrak{p}^{e_i f_i} = \mathfrak{p}^n.$$

(2), Let $\mathfrak{P}$ be any prime ideal of $\mathfrak{O}_K$, and let $\mathfrak{P} \cap \mathbb{Z} = (p)$. Let $[\mathfrak{O}_K/\mathfrak{P} : \mathbb{Z}/p\mathbb{Z}] = f$, that is, $N\mathfrak{P} = p^f$. By definition,

$$N_{K/\mathbb{Q}}(\mathfrak{P}) = (p\mathbb{Z})^f = p^f\mathbb{Z} = (N\mathfrak{P})\mathbb{Z},$$

which proves the assertion form the multiplicativity of the relative norm.

(3), By the multiplicativity of the relative norm, it suffices to prove the statement for a prime ideal $\mathfrak{P}$ of K. Let $\mathfrak{P} \cap \mathfrak{O}_L = \mathfrak{P}_L$ and $\mathfrak{P} \cap \mathfrak{o}_k = \mathfrak{p}$. Then $N_{K/k}(\mathfrak{P}) = \mathfrak{p}^{f(\mathfrak{P}/\mathfrak{p})}$. On the other hand, we have

$$N_{K/L}(\mathfrak{P}) = \mathfrak{P}_L^{f(\mathfrak{P}/\mathfrak{P}_L)} \quad \text{and} \quad N_{L/k}(\mathfrak{P}_L) = \mathfrak{p}^{f(\mathfrak{P}_L/\mathfrak{p})}.$$

Therefore, by the Lemma (1.39),

$$\begin{aligned} N_{L/k}\left(N_{K/L}(\mathfrak{P})\right) &= N_{L/k}\left(\mathfrak{P}_L^{f(\mathfrak{P}/\mathfrak{P}_L)}\right) = \mathfrak{p}^{f(\mathfrak{P}_L/\mathfrak{p})f\mathfrak{P}/\mathfrak{P}_L)} \\ &= \mathfrak{p}^{f(\mathfrak{P}/\mathfrak{p})} = N_{K/k}(\mathfrak{P}). \end{aligned}$$

□

Since $\mathbb{Z}$ is a principal ideal domain, every finitely generated torsion-free $\mathbb{Z}$-module has a finite $\mathbb{Z}$-basis; in particular, any fractional ideal in a number field has an integral basis. If K/k is a finite extension of number fields where $\mathfrak{o}_k$ is a Dedekind domain but not necessarily a principal ideal domain, then the fractional ideals of K are finitely generated and torsion-free as $\mathfrak{o}_k$-modules, but not necessarily free. That is, the integer ring $\mathfrak{O}_K$ may not exist a basis as an $\mathfrak{o}_k$-module.

1.5 Global Hilbert Theory

Recall: (Galois Theory) If E/F is normal and separable, it is said to be a Galois extension; we also say that E is Galois over F. If E/F is a finite Galois extension, then there are exactly $[E : F]$ F-automorphisms of E. If E/F is an arbitrary extension, the Galois group of the extension, denoted by

$$\mathrm{Gal}(E/F) = \{\sigma \,|\, \sigma \text{ is an automorphism of } E \text{ and } \sigma|_F = 1\}$$

is the set of F-automorphisms of E.

- An important theorem of Emil Artin states that for a finite extension E/F, each of the following statements is equivalent to the statement that E/F is Galois:

  (1), E/F is a normal extension and a separable extension.

  (2), E is a splitting field of a separable polynomial with coefficients in F.

  (3), $[E : F] = |\mathrm{Gal}(E/F)|$; that is, the degree of the field extension is equal to the order of the automorphism group of E/F.

- Let E/F be a finite Galois extension with Galois group $G = \mathrm{Gal}(E/F)$. Then the fixed field of G is F. If H is a proper subgroup of G, then the fixed field of H properly contains F.

- **Fundamental Theorem of Galois Theory**: Let E/F be a finite Galois extension with Galois group G. If H is a subgroup of G, let $\mathcal{F}(H)$ be the fixed field of H, and if K is an intermediate field, let $\mathcal{G}(K)$ be $\mathrm{Gal}(E/K)$, the fixing group of K.

  $\mathcal{F}$ is a bijective map from subgroups to intermediate fields, with inverse $\mathcal{G}$. Both maps are inclusion-reversing, that is, if $H_1 \leq H_2$ then $\mathcal{F}(H_1) \geq \mathcal{F}(H_2)$, and if $K_1 \leq K_2$, then $\mathcal{G}(K_1) \geq \mathcal{G}(K_2)$.

  Suppose that the intermediate field K corresponds to the subgroup H under the Galois correspondence. Then

  ▶ E/K is always normal, hence Galois;

  ▶ K/F is normal if and only if H is a normal subgroup of G, and in this case,

  ▶ the Galois group of K/F is isomorphic to the quotient group G/H. Moreover, whether

  or not K/F is normal,

  ▶ $[K : F] = [G : H]$ and $[E : K] = |H|$.

- If the intermediate field K corresponds to the subgroup H and σ is any automorphism in G, then the field $\sigma K = \{\sigma(x) \,|\, x \in K\}$ corresponds to the conjugate subgroup $\sigma H \sigma^{-1}$. For this reason, σK is called a conjugate subfield of K.

  For the proofs we refer the reader to [1] or [5].

Throughout this section, let K/k be a Galois extension of number fields with the Galois group $G = \mathrm{Gal}(K/k)$ and $[K : k] = n$. In particular, the Galois extensions K/k are called the *abelian extension* and *cyclic extension* whose the Galois groups are abelian and cyclic respectively.

1.5.1 Decomposition of prime ideals: $efg = n$

Let $\mathfrak{p}$ be a prime ideal of $\mathfrak{o}_k$ and $\mathfrak{P}$ be a prime ideal above $\mathfrak{p}$ in $\mathfrak{O}_K$. We firstly show that the Galois group G acts on the set of prime ideals lying above $\mathfrak{p}$.

Lemma 1.45. *If $\sigma \in G$, then $\sigma\mathfrak{O}_K = \mathfrak{O}_K$. If $\mathfrak{P}$ is a prime ideal above $\mathfrak{p}$ in $\mathfrak{O}_K$ and $\sigma \in G$, then so does $\sigma\mathfrak{P}$.*

Proof. If $\alpha \in \mathfrak{O}_K$, then the conjugate $\sigma\alpha$ for every element $\sigma \in G$ has the same minimal polynomial. Hence $\sigma\alpha \in \mathfrak{O}_K$ and $\sigma\mathfrak{O}_K \subset \mathfrak{O}_K$. But $\sigma^{-1}\mathfrak{O}_K$ is also contained in $\mathfrak{O}_K$, hence $\sigma\mathfrak{O}_K = \mathfrak{O}_K$.

If $\mathfrak{p}\mathfrak{O}_K = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}$, then apply σ to get

$$\sigma(\mathfrak{p}\mathfrak{O}_K) = \mathfrak{p}\mathfrak{O}_K = \sigma(\mathfrak{P}_1)^{e_1} \cdots \sigma(\mathfrak{P}_g)^{e_g}.$$

Thus $\sigma\mathfrak{P}_i$ must be prime ideals, because σ perserves all algebraic relation. Since $\mathfrak{P}_i \cap \mathfrak{O}_K = \mathfrak{p}$, it follows that $\sigma\mathfrak{P}_i \cap \mathfrak{O}_K = \mathfrak{p}$, so $\sigma\mathfrak{P}_i$ is a prime factor of $\mathfrak{p}$. □

The ideals $\sigma\mathfrak{P}$, for $\sigma \in G$, are called the *conjugate prime ideals* to $\mathfrak{P}$.

Recall: (The Orbit-Stabilizer Theorem) Suppose that a group G acts on a set X. Let $B(x) = \{gx \,|\, g \in G\}$ be the orbit of $x \in X$, and let $G(x) = \{g \in G \,|\, gx = x\}$ be the stabilizer of x. Then the size of the orbit is the index of the stabilizer, that is, $|B(x)| = [G : G(x)]$. Thus if G is finite, then $|B(x)| = |G|/|G(x)|$; in particular, the orbit size divides the order of the group.

For the proofs we refer the reader to [1]

Proposition 1.46. *Let $\mathfrak{p}$ be a prime ideal of $\mathfrak{o}_k$ and*

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

Then (1), G acts transitively on the the set $\{\mathfrak{P}_1, \ldots, \mathfrak{P}_g\}$, that is, for any i, j there exists $\sigma \in G$ such that $\mathfrak{P}_i = \sigma\mathfrak{P}_j$.

(2), For any i, $\{\mathfrak{P}_1, \ldots, \mathfrak{P}_g\}$ are all the prime ideals conjugate to $\mathfrak{P}_i$.

(3), We have that $e_1 = \cdots = e_g = e$, $f_1 = \cdots = f_g = f$, and $n = efg$.

(4), Let $\mathfrak{A}$ be an ideal of the integral ring $\mathfrak{O}_K$. Then

$$N_{K/k}(\mathfrak{A})\mathfrak{O}_K = \prod_{\sigma \in G} \sigma\mathfrak{A}.$$

Proof. (1), Only need to show that for any $\mathfrak{P}_i$, there exists $\sigma \in G$, such that $\mathfrak{P}_i = \sigma\mathfrak{P}_1$. Suppose that, for any $i \neq 1$, $\mathfrak{P}_i \notin \{\sigma\mathfrak{P}_1 : \sigma \in G\}$. By the Chinese Remainder Theorem, there is $\alpha \in \mathfrak{O}_K$, such that

$$\alpha \in \mathfrak{P}_i \text{ and } \alpha \notin \sigma\mathfrak{P}_1, \text{ for any } \sigma \in G,$$

which gives $\sigma\alpha \notin \mathfrak{P}_1$. Then

$$N_{K/k}(\alpha) = \prod_{\sigma \in G} \sigma\alpha \in \mathfrak{P}_i \cap \mathfrak{o}_k = \mathfrak{p} \subset \mathfrak{P}_1,$$

this is a contradiction.

(2), It suffices to show that the conjugate prime ideal of $\mathfrak{P}_1$ is one of $\mathfrak{P}_1, \ldots, \mathfrak{P}_g$. Let $\mathfrak{P}$ be any conjugate prime ideal of $\mathfrak{P}_1$. Then there exists $\sigma \in G$, such that $\mathfrak{P} = \sigma\mathfrak{P}_1$. Since $\mathfrak{P}_1 \cap \mathfrak{o}_k = \mathfrak{p}$, it follows that

$$\mathfrak{P} \cap \mathfrak{o}_k = \sigma\mathfrak{P}_1 \cap \sigma\mathfrak{o}_k = \sigma(\mathfrak{P}_1 \cap \mathfrak{o}_k) = \sigma\mathfrak{p} = \mathfrak{p}.$$

Hence $\mathfrak{P}|\mathfrak{p}$, and then $\mathfrak{P}$ is one of prime factors $\mathfrak{P}_1, \ldots, \mathfrak{P}_g$.

(3,) Assume that $\mathfrak{P}_i = \sigma\mathfrak{P}_1$ for any $i \neq 1$ and some σ. Then

$$\begin{aligned} &\mathfrak{P}_1^{e_1} \ldots \mathfrak{P}_g^{e_g} = \mathfrak{p}\mathfrak{O}_K = \sigma(\mathfrak{p}\mathfrak{O}_K) \\ &= \sigma(\mathfrak{P}_1)^{e_1} \cdots \sigma(\mathfrak{P}_g)^{e_g} = \mathfrak{P}_i^{e_1}\sigma(\mathfrak{P}_2)^{e_2} \cdots \sigma(\mathfrak{P}_g)^{e_g}. \end{aligned}$$

Clearly, $\sigma(\mathfrak{P}_j) \neq \mathfrak{P}_i$ for any $j > 1$, since otherwise $\sigma\mathfrak{P}_j = \mathfrak{P}_i = \sigma\mathfrak{P}_1$ which implies $\mathfrak{P}_j = \mathfrak{P}_1$, a contradiction. We must have $e_i = e_1$ for the unique factorization of ideals of a Dedekind domain. Therefore, $e_1 = \cdots = e_g = e$, say.

Similarly, we have, for any $i > 1$,

$$\begin{aligned} f_i &= [\mathfrak{O}_K/\mathfrak{P}_i : \mathfrak{o}_k/\mathfrak{p}] = [\mathfrak{O}_K/\sigma\mathfrak{P}_1 : \mathfrak{o}_k/\mathfrak{p}] \\ &= [\sigma(\mathfrak{O}_K)/\sigma(\mathfrak{P}_1) : \sigma(\mathfrak{o}_k)/\sigma(\mathfrak{p})] \\ &= [\mathfrak{O}_K/\mathfrak{P}_1 : \mathfrak{o}_k/\mathfrak{p}] = f_1. \end{aligned}$$

Therefore, $f_1 = \cdots = f_g = f$, say. Then $n = \sum_{i=1}^{g} e_i f_i = efg$.

(4), It is sufficient to show the conclusion for any prime ideal $\mathfrak{P}$ of K. Let $\mathfrak{p} = \mathfrak{P} \cap \mathfrak{o}_k$ and $\mathfrak{p}\mathfrak{O}_K = (\mathfrak{P}_1\mathfrak{P}_2 \cdots \mathfrak{P}_g)^e$. Since $N_{K/k}(\mathfrak{P}_i) = \mathfrak{p}^f$ for each i, we can have

$$N_{K/k}(\mathfrak{P})\mathfrak{O}_K = (\mathfrak{P}_1\mathfrak{P}_2 \cdots \mathfrak{P}_g)^{ef}.$$

On the other hand, since G acts transitively on the set $\{\mathfrak{P}_1, \mathfrak{P}_2, \ldots, \mathfrak{P}_g\}$, it follows that each $\mathfrak{P}_i$ occurs $n/g = ef$ in the family $\{\sigma\mathfrak{P} | \sigma \in G\}$ by the orbit-stabilizer theorem. Thus

$$N_{K/k}(\mathfrak{P})\mathfrak{O}_K = (\mathfrak{P}_1\mathfrak{P}_2 \cdots \mathfrak{P}_g)^{ef} = \prod_{\sigma \in G} \sigma\mathfrak{P}.$$

This completes the proof. □

In fact, this proposition implies that the following diagram commutes.

$$\begin{array}{ccc} K^\times & \xrightarrow{\alpha\mapsto(\alpha)} & J_K \\ \Big\downarrow{\scriptstyle N_{K/k}} & & \Big\downarrow{\scriptstyle N_{K/k}} \\ k^\times & \xrightarrow{\alpha\mapsto(\alpha)} & J_k \end{array}$$

In the case K/k is Galois, we shall denote the common values of the $e_i = e(\mathfrak{P}/\mathfrak{p}), f_i = f(\mathfrak{P}/\mathfrak{p})$ by the $e_\mathfrak{p}, f_\mathfrak{p}$ respectively. If we write $g_\mathfrak{p}$ instead of g, then we may reformulate (1.14), as $n = e_\mathfrak{p} f_\mathfrak{p} g_\mathfrak{p}$.

1.5.2 Decomposition and inertia groups

From now on, we fix our attention on one prime factor $\mathfrak{P}$ of $\mathfrak{p}$ in $\mathfrak{O}_K$. Let $[K : k] = n = efg$, where $e = e_\mathfrak{p} = e(\mathfrak{P}/\mathfrak{p}) = e(K/k)$.

Definition 1.47. *The stabilizer of $\mathfrak{P}$ in G is called the decomposition(splitting) group(Zerlegungs gruppe) of $\mathfrak{P}$ given by*

$$D_\mathfrak{P} = \{\sigma \in G \,|\, \sigma\mathfrak{P} = \mathfrak{P}\}.$$

Its fixed field

$$K_D = \{\alpha \in K \,|\, \sigma\alpha = \alpha, \sigma \in D\},$$

is called the decomposition(splitting) field of $\mathfrak{P}$.

By the orbit-stabilizer theorem, we have $[G : D_\mathfrak{P}] = |G\mathfrak{P}|$, where $G\mathfrak{P} = \{\sigma\mathfrak{P} \,|\, \sigma \in G\}$ is the orbit of $\mathfrak{P}$ under the action of G. Since there is only one orbit, of size g, we see that

$$|D_\mathfrak{P}| = |G|/[G : D_\mathfrak{P}] = |G|/|G\mathfrak{P}| = ef,$$

which is independent of choice of $\mathfrak{P}$.

Proposition 1.48. *Let the notations and assumptions be as above.*

(1), $e(\mathfrak{P}/\mathfrak{P}_D) = e, f(\mathfrak{P}/\mathfrak{P}_D) = f, g(\mathfrak{P}/\mathfrak{P}_D) = 1$, that is, $\mathfrak{P}$ is the only prime ideal of K lying above $\mathfrak{P}_D$.

(2), $e(\mathfrak{P}_D/\mathfrak{p}) = f(\mathfrak{P}_D/\mathfrak{p}) = 1$. Moveover, if $D_\mathfrak{P} \trianglelefteq G$, then $g(\mathfrak{P}_D/\mathfrak{p}) = g$, that is, $\mathfrak{p}$ is completely split in K_D.

(3), The subfield K_D is the smallest subfield M between k and K such that $\mathfrak{P}_M = \mathfrak{P} \cap \mathfrak{O}_M$ does not split, that is, $g(\mathfrak{P}/\mathfrak{P}_M) = 1$.

Proof. (1) and (2), We first prove that K/K_D has the property $g(\mathfrak{P}/\mathfrak{P}_D) = 1$ where $\mathfrak{P}_D = \mathfrak{P} \cap \mathfrak{O}_D$. By Galois theory, K/K_D is Galois and $\mathrm{Gal}(K/K_D) = D$. Let

$$\mathfrak{P}_D\mathfrak{O}_K = \mathfrak{P}^{e_1}\mathfrak{P}_1^{e_1}\cdots\mathfrak{P}_t^{e_1}.$$

Then for any $\mathfrak{P}_i$, there exists $\sigma \in \mathrm{Gal}(K/K_D) = D$, such that $\mathfrak{P}_i = \sigma\mathfrak{P} = \mathfrak{P}$. Hence $g(\mathfrak{P}/\mathfrak{P}_D) = 1$.

Moreover,

$$e(\mathfrak{P}/\mathfrak{P}_D)f(\mathfrak{P}/\mathfrak{P}_D) = [K : K_D] = |D_{\mathfrak{P}}| = ef$$

and

$$e(\mathfrak{P}/\mathfrak{P}_D) \le e,\ f(\mathfrak{P}/\mathfrak{P}_D) \le f$$

by the lemma (1.39). Then we obtain $e(\mathfrak{P}/\mathfrak{P}_D) = e$ and $f(\mathfrak{P}/\mathfrak{P}_D) = f$. It follows that $e(\mathfrak{P}_D/\mathfrak{p}) = f(\mathfrak{P}_D/\mathfrak{p}) = 1$. If $D_{\mathfrak{P}} \trianglelefteq G$, then K_D/k is a Galois extension. We thus get

$$g(\mathfrak{P}_D/\mathfrak{p}) = e(\mathfrak{P}_D/\mathfrak{p})f(\mathfrak{P}_D/\mathfrak{p})g(\mathfrak{P}_D/\mathfrak{p}) = [K_D : k] = g.$$

(3), Let us now prove the minimality of K_D. Assume that there exists an intermediate field M such that $g(\mathfrak{P}/\mathfrak{P}_M) = 1$. Then this unique ideal must be $\mathfrak{P}$, since by definition $\mathfrak{P}$ is above $\mathfrak{P}_M$. Then $\mathrm{Gal}(K/M)$ is a subgroup of $D_{\mathfrak{P}}$, since its elements are fixing $\mathfrak{P}$. Thus $M \supset K_D$. □

For any $\sigma \in D_{\mathfrak{P}}$, then σ induces an automorphism $\overline{\sigma}$ of $\mathfrak{O}_K/\mathfrak{P} = \mathbb{F}_{\mathfrak{P}}$ which fixes $\mathfrak{o}_k/\mathfrak{p} = \mathbb{F}_{\mathfrak{p}}$,

$$\begin{array}{rcl} \overline{\sigma} : \mathfrak{O}_K/\mathfrak{P} & \longrightarrow & \mathfrak{O}_K/\mathfrak{P} \\ \overline{\alpha} = \alpha + \mathfrak{P} & \longmapsto & \overline{\sigma\alpha} = \sigma\alpha + \mathfrak{P}, \end{array}$$

that is, we obtain the following lemma.

Lemma 1.49. *The $\overline{\sigma}$ is an automorphism of $\mathbb{F}_{\mathfrak{P}}$ which fixes $\mathbb{F}_{\mathfrak{p}}$, that is, $\overline{\sigma} \in \mathrm{Gal}(\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}})$.*

Proof. • $\overline{\sigma}$ is a mapping

It suffices to prove that $\overline{\alpha} = \overline{\beta} \Rightarrow \overline{\sigma}(\overline{\alpha}) = \overline{\sigma}(\overline{\beta})$. Clearly, the following facts

$$\begin{array}{rcl} \overline{\alpha} = \overline{\beta} & \Leftrightarrow & \alpha + \mathfrak{P} = \beta + \mathfrak{P} \Leftrightarrow \alpha - \beta \in \mathfrak{P} \\ & \Leftrightarrow & \sigma(\alpha - \beta) \in \sigma\mathfrak{P} = \mathfrak{P} \Leftrightarrow \sigma\alpha - \sigma\beta \in \mathfrak{P} \\ & \Leftrightarrow & \sigma\alpha + \mathfrak{P} = \sigma\beta + \mathfrak{P} \Leftrightarrow \overline{\sigma}(\overline{\alpha}) = \overline{\sigma}(\overline{\beta}). \end{array}$$

• $\overline{\sigma}$ is an automorphism of the finite field $\mathbb{F}_{\mathfrak{P}}$

It is easy to check that $\overline{\sigma}(\overline{\alpha} \pm \overline{\beta}) = \overline{\sigma}(\overline{\alpha}) \pm \overline{\sigma}(\overline{\beta})$ and $\overline{\sigma}(\overline{\alpha}\overline{\beta}) = \overline{\sigma}(\overline{\alpha})\overline{\sigma}(\overline{\beta})$. And

$$\begin{aligned} \ker \overline{\sigma} &= \{\overline{\alpha} \in \mathbb{F}_{\mathfrak{P}} \,:\, \overline{\sigma}(\overline{\alpha}) = 0\} \\ &= \{\overline{\alpha} \in \mathbb{F}_{\mathfrak{P}} \,:\, \sigma\alpha \in \mathfrak{P}\} \\ &= \{\overline{\alpha} \in \mathbb{F}_{\mathfrak{P}} \,:\, \alpha \in \sigma^{-1}\mathfrak{P} = \mathfrak{P}\} \\ &= \{\overline{0}\}, \end{aligned}$$

then $\overline{\sigma}$ is an automorphism.

• $\overline{\sigma}$ fixes every element of $\mathbb{F}_{\mathfrak{p}}$

For any $\overline{\alpha} = \alpha + \mathfrak{p} \in \mathbb{F}_{\mathfrak{p}}$, we have $\overline{\sigma}(\overline{\alpha}) = \overline{\sigma(\alpha)} = \sigma(\alpha) + \mathfrak{p} = \overline{\alpha}$. □

Denote a map by

$$\begin{aligned} \pi : D_{\mathfrak{P}} &\longrightarrow \mathrm{Gal}(\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}}) \\ \sigma &\longmapsto \overline{\sigma}. \end{aligned}$$

Let $I_{\mathfrak{P}}$ be the kernel of the group homomorphism π; $I_{\mathfrak{P}}$ is called the *inertia group(Trägheits gruppe)* of $\mathfrak{P}$ and its fixed field K_I is called the *inertia field* of $\mathfrak{P}$.

Proposition 1.50. *(1), The group homomorphism π is surjective.*

(2), $I_{\mathfrak{P}}$ is a normal subgroup of $D_{\mathfrak{P}}$ of order $e_{\mathfrak{p}}$ and

$$D_{\mathfrak{P}}/I_{\mathfrak{P}} \cong \mathrm{Gal}(\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}})$$

is cyclic of order $f_{\mathfrak{p}}$.

(3), $I_{\mathfrak{P}} = \{\sigma \in D_{\mathfrak{P}} \,|\, \sigma\alpha \equiv \alpha (\mathrm{mod}\mathfrak{P}),$ for any $\alpha \in \mathfrak{O}_K\}$.

Proof. (1), Let $\overline{\alpha} \in \mathbb{F}_{\mathfrak{P}}$ be an element such that $\mathbb{F}_{\mathfrak{P}} = \mathbb{F}_{\mathfrak{p}}(\overline{\alpha})$. Lift $\overline{\alpha}$ to an algebraic integer $\alpha \in \mathfrak{O}_K$, and let

$$f(x) = \prod_{\sigma \in D_{\mathfrak{P}}} (x - \sigma\alpha) \in \mathfrak{O}_D[x]$$

be the characteristic polynomial of α over K_D.

By Proposition (1.45), we see that $f(x)$ reduces mod $\mathfrak{P}_D$ to

$$\overline{f}(x) = \prod_{\sigma \in D_{\mathfrak{P}}} (x - \overline{\sigma\alpha}) \in \mathbb{F}_{\mathfrak{p}}[x]$$

because $\mathfrak{O}_D/\mathfrak{P}_D \cong \mathbb{F}_{\mathfrak{p}}$. Since the characteristic polynomial of $\overline{\alpha}$ over $\mathbb{F}_{\mathfrak{p}}$ is divided by the minimal polynomial of $\overline{\alpha}$, all the conjugates of $\overline{\alpha}$ over $\mathbb{F}_{\mathfrak{p}}$

have the form $\overline{\sigma\alpha}$. Every $\mathbb{F}_{\mathfrak{p}}$-automorphism of $\mathbb{F}_{\mathfrak{P}}$ is of the form $\overline{\sigma}$ where $\sigma \in D_{\mathfrak{P}}$. It follows that the group homomorphism π is surjective.

(2,) By Galois theory, we know that $\mathrm{Gal}(\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}})$ is cyclic, generated by the Frobenius automorphism defined by $\sigma_{\mathrm{Frob}} : \overline{\alpha} \mapsto \overline{\alpha}^{N\mathfrak{p}}$, for $\overline{\alpha} \in \mathbb{F}_{\mathfrak{P}}$. It is clear that $I_{\mathfrak{P}}$ is a normal subgroup of $D_{\mathfrak{P}}$. And the order of $I_{\mathfrak{P}}$ is $D_{\mathfrak{P}}/\mathrm{Gal}(\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}}) = e_{\mathfrak{p}}$.

(3,) Obviously, we have

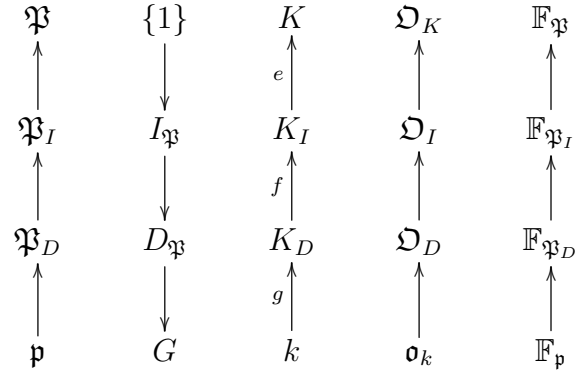
$$\begin{aligned} I_{\mathfrak{P}} &= \{\sigma \in D_{\mathfrak{P}} \ : \ \overline{\sigma} = 1\} \\ &= \{\sigma \in D_{\mathfrak{P}} \ : \ \overline{\sigma}(\overline{\alpha}) = \overline{\alpha}, \text{ for any } \overline{\alpha} \in \mathbb{F}_{\mathfrak{P}}\} \\ &= \{\sigma \in D_{\mathfrak{P}} \ : \ \sigma(\alpha) \equiv \alpha (\mathrm{mod}\mathfrak{P}), \text{ for any } \alpha \in \mathfrak{O}_K\}. \end{aligned}$$

□

Since the above theorem, we get the following exact sequence:

$$1 \to I_{\mathfrak{P}} \to D_{\mathfrak{P}} \to \mathrm{Gal}(\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}}) \to 1.$$

Let K_D, K_I be fixed fields of the subgroup $D_{\mathfrak{P}}$ and $I_{\mathfrak{P}}$ respectively. Let $\mathfrak{P}_D = \mathfrak{P} \cap \mathfrak{O}_{K_D}, \mathfrak{P}_I = \mathfrak{P} \cap \mathfrak{O}_{K_I}$ and $\mathbb{F}_{\mathfrak{P}_D} = \mathfrak{O}_{K_D}/\mathfrak{P}_D, \mathbb{F}_{\mathfrak{P}_I} = \mathfrak{O}_{K_I}/\mathfrak{P}_I$. Clearly, $K/K_I, K/K_D$ and K_I/K_D are Galois extensions with Galois groups $I_{\mathfrak{P}}, D_{\mathfrak{P}}$ and $D_{\mathfrak{P}}/I_{\mathfrak{P}}$ by Galois theory.



Theorem 1.51. *(1), (i),* $e(\mathfrak{P}/\mathfrak{P}_I) = e, f(\mathfrak{P}/\mathfrak{P}_I) = 1, g(\mathfrak{P}/\mathfrak{P}_I) = 1$, *that is,* $\mathfrak{P}_I$ *is ramified completely in* K.

(ii), $e(\mathfrak{P}_I/\mathfrak{P}_D) = 1, f(\mathfrak{P}_I/\mathfrak{P}_D) = f, g(\mathfrak{P}_I/\mathfrak{P}_D) = 1$, *that is,* $\mathfrak{P}_D$ *is unramified and inertia in* K_I.

(2), For any $\sigma \in G$, *we have* $D_{\sigma\mathfrak{P}} = \sigma D_{\mathfrak{P}} \sigma^{-1}, I_{\sigma\mathfrak{P}} = \sigma I_{\mathfrak{P}} \sigma^{-1}, K_{D_{\sigma\mathfrak{P}}} = \sigma K_{D_{\mathfrak{P}}}$, *and* $K_{I_{\sigma\mathfrak{P}}} = \sigma K_{I_{\mathfrak{P}}}$.

Proof. (1,) We first have $g(\mathfrak{P}/\mathfrak{P}_D) = 1$. For the Galois extension K/K_I with Galois groups $I_{\mathfrak{P}}$, the decomposition group and inertia group of $\mathfrak{P}$

lying above $\mathfrak{P}_I$ are both $I_{\mathfrak{P}}$. Thus $f(\mathfrak{P}/\mathfrak{P}_I) = 1$, and then $e(\mathfrak{P}/\mathfrak{P}_I) = e$. On the other hand, we have

$$\begin{aligned} e(\mathfrak{P}/\mathfrak{P}_D) &= e(\mathfrak{P}/\mathfrak{P}_I)e(\mathfrak{P}_I/\mathfrak{P}_D) = e \\ f(\mathfrak{P}/\mathfrak{P}_D) &= f(\mathfrak{P}/\mathfrak{P}_I)f(\mathfrak{P}_I/\mathfrak{P}_D) = f. \end{aligned}$$

Therefore, $e(\mathfrak{P}_I/\mathfrak{P}_D) = 1, f(\mathfrak{P}_I/\mathfrak{P}_D) = f$.

(2,) Since

$$\tau \in D_{\mathfrak{P}} \Leftrightarrow \tau\mathfrak{P} = \mathfrak{P} \Leftrightarrow \sigma\tau\sigma^{-1}(\sigma\mathfrak{P}) = \sigma\mathfrak{P} \Leftrightarrow \sigma\tau\sigma^{-1} \in D_{\sigma\mathfrak{P}}$$

we get $D_{\sigma\mathfrak{P}} = \sigma D_{\mathfrak{P}}\sigma^{-1}$. It is similar to that $I_{\sigma\mathfrak{P}} = \sigma I_{\mathfrak{P}}\sigma^{-1}$.

On the other hand,

$$\begin{aligned} \alpha \in K_{D_{\mathfrak{P}}} &\Leftrightarrow \tau\alpha = \alpha, \quad \text{for all } \tau \in D_{\mathfrak{P}} \\ &\Leftrightarrow \sigma\tau\sigma^{-1}(\sigma\alpha) = \sigma\alpha \quad \text{for all } \sigma\tau\sigma^{-1} \in D_{\sigma\mathfrak{P}} \\ &\Leftrightarrow \sigma\alpha \in K_{D_{\sigma\mathfrak{P}}} \end{aligned}$$

Thus, $K_{D_{\sigma\mathfrak{P}}} = \sigma K_{D_{\mathfrak{P}}}$. By a similar argument, we have $K_{I_{\sigma\mathfrak{P}}} = \sigma K_{I_{\mathfrak{P}}}$. □

1.5.3 The Frobenius automorphism

Let $\mathfrak{p}$ be a prime ideal of $\mathfrak{o}_k$ that is unramified in $\mathfrak{O}_K$, i.e., $e_{\mathfrak{p}} = 1$, and let $\mathfrak{P}$ be a prime ideal lying above $\mathfrak{p}$. By Proposition (1.50), then the inertia group $I_{\mathfrak{P}}$ is trivial. So $D_{\mathfrak{P}} \cong \mathrm{Gal}(\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}})$. There is a unique element $\sigma_{\mathfrak{P}}$ of $D_{\mathfrak{P}}$ that the correspondence to σ_{Frob} is called the *Frobenius automorphism* and is denoted by $[\frac{K/k}{\mathfrak{P}}]$. The Frobenius automorphism is uniquely determined as an element of G by

$$\sigma\alpha \equiv \alpha^{N\mathfrak{p}} \bmod \mathfrak{P}, \tag{1.15}$$

for all $\alpha \in \mathfrak{O}_K$. And it obviously has the property

$$\left[\frac{K/k}{\sigma\mathfrak{P}}\right] = \sigma \left[\frac{K/k}{\mathfrak{P}}\right] \sigma^{-1}$$

for every $\sigma \in G$; thus it is defined up to conjugacy by $\mathfrak{p}$.

It is natural to ask how all these objects behave under change of fields. We have the following theorem:

Theorem 1.52. *Let L be an intermediate field between k and K. Let $\mathfrak{p}$ be an unramified prime ideal of $\mathfrak{o}_k$ in $\mathfrak{O}_K$ and $\mathfrak{P}$ be prime divisor of $\mathfrak{p}$ in K. Let $H = \mathrm{Gal}(K/L)$ and $\mathfrak{P}_L = \mathfrak{P} \cap \mathfrak{O}_L$.*

(1), $e(\mathfrak{P}/\mathfrak{P}_L) = 1$ and $\left[\frac{K/L}{\sigma\mathfrak{P}}\right] = \left[\frac{K/k}{\mathfrak{P}}\right]^{f(\mathfrak{P}_L/\mathfrak{p})}$.

(2), If L/k is Galois, then $e(\mathfrak{P}_L/\mathfrak{p}) = 1$ and $\left[\frac{L/k}{\mathfrak{P}_L}\right] = \left[\frac{K/k}{\mathfrak{P}}\right]\Big|_L$.

Proof. (1), By $e(\mathfrak{P}/\mathfrak{p}) = e(\mathfrak{P}/\mathfrak{P}_L)e(\mathfrak{P}_L/\mathfrak{p}) = 1$, it gives $e(\mathfrak{P}/\mathfrak{P}_L) = 1$. It is also clear that

$$N(\mathfrak{P}_L) = |\mathfrak{O}_L/\mathfrak{P}_L| = |\mathfrak{o}_k/\mathfrak{p}|^{f(\mathfrak{P}_L/\mathfrak{p})} = N(\mathfrak{p})^{f(\mathfrak{P}_L/\mathfrak{p})}.$$

Therefore, by (1.15), for any $\alpha \in \mathfrak{O}_K$,

$$\begin{aligned}\left[\frac{K/k}{\mathfrak{P}}\right]^{f(\mathfrak{P}_L/\mathfrak{p})} \alpha &\equiv \alpha^{(N\mathfrak{p})^{f(\mathfrak{P}_L/\mathfrak{p})}} \bmod \mathfrak{P} \\ &\equiv \alpha^{N\mathfrak{P}_L} \bmod \mathfrak{P},\end{aligned}$$

and then we have $\left[\frac{K/k}{\mathfrak{P}}\right]^{f(\mathfrak{P}_L/\mathfrak{p})} = \left[\frac{K/L}{\mathfrak{P}}\right]$.

(2), Similarly, we have $e(\mathfrak{P}_L/\mathfrak{p}) = 1$. According to, for any $\alpha \in \mathfrak{O}_K$,

$$\left[\frac{K/k}{\mathfrak{P}}\right] \alpha \equiv \alpha^{N\mathfrak{p}} (\bmod \mathfrak{P}),$$

it gives, for any $\alpha \in \mathcal{O}_L$,

$$\left[\frac{K/k}{\mathfrak{P}}\right] \alpha \equiv \alpha^{N\mathfrak{p}} (\bmod \mathfrak{P}_L),$$

and thus $\left[\frac{K/k}{\mathfrak{P}}\right]\Big|_L = \left[\frac{L/k}{\mathfrak{P}_L}\right]$. □

1.5.4 The Artin map

If $\mathfrak{p}$ is ramified, we can also define the Frobenius automorphism, *the Frobenius conjugate class*, by the set of all elements of G which satisfies (1.15). This identifies the Frobenius automorphism as a left coset of $I_{\mathfrak{P}}$ in $D_{\mathfrak{P}}$. In particular, if G is abelian then the Frobenius automorphism depends only on $\mathfrak{p}$; in this case it is called the *Artin symbol* and is denoted by

$$\sigma_{\mathfrak{p}} = \left(\frac{K/k}{\mathfrak{p}}\right).$$

In this way, we obtain a correspondence between prime ideals of k that are unramified in K and elements of the abelian Galois group G. By multiplication we can now extend the Artin symbol for any fractional ideal $\mathfrak{a}$ of k which involves unramified prime ideal. Indeed, let J_k be the fractional ideal groups of k and let S be a finite set of primes of $\mathfrak{o}_k$ including all the

primes that ramify in K. Denote J_k^S by the subgroup of J_k generated by all the nonzero prime ideals outside S. An element $\mathfrak{a}$ of J_k^S has the form

$$\mathfrak{a} = \prod_{\mathfrak{p} \notin S} \mathfrak{p}^{\mathrm{ord}_{\mathfrak{p}}(\mathfrak{a})}.$$

Now we define the Artin map as the function

$$\begin{aligned} \varphi : J_k^S &\longrightarrow \mathrm{Gal}(K/k) \\ \mathfrak{a} &\longmapsto \left(\frac{K/k}{\mathfrak{a}}\right) = \prod_{\mathfrak{p} \notin S} \left(\frac{K/k}{\mathfrak{p}}\right)^{\mathrm{ord}_{\mathfrak{p}}(\mathfrak{a})}. \end{aligned}$$

The product is well defined because $\mathrm{Gal}(K/k)$ is abelian and only a finite number of exponents $\mathrm{ord}_{\mathfrak{p}}(\mathfrak{a})$ are nonzero for any given fractional ideal $\mathfrak{a}$. The Artin symbol plays a central role in class field theory. One of the major goals is to determine the image and kernel of φ. We will see that φ is surjective.

And after the first year [as an undergraduate at Gottingen] I went home with Hilbert's Zahlbericht under my arm, and during the summer vacation I worked my way through it without any previous knowledge of elementary number theory or Galois theory. These were the happiest months of my life, whose shine, across years burdened with our common share of doubt and failure, still comforts my soul.

H. Weyl (1885-1955), Bull. of AMS, 50(1944), 612-654.

Exercises

You are encouraged to collaborate on solving the problems given as homework. However, the solutions should be written on your own and in your own words. Please send me your homework to my email before the next week's class.

1, Let α, β be algebraic numbers such that β is conjugate to α. Show that α and β have the same minimal polynomial.

2, Let α be an algebraic number and let $p(x)$ be its minimal polynomial. Show that $p(x)$ has no repeated roots.

3, Let $f(x) \in \mathbb{Z}[x]$ and $g(x) \in \mathbb{Q}[x]$ be monic polynomials. If $g(x)|f(x)$. Show that $g(x) \in \mathbb{Z}[x]$. i.e., the minimal polynomial of any algebraic integer has coefficients in $\mathbb{Z}$.

4, Determine the ring of integers $\mathfrak{o}_k$ of the quadratic field $k = \mathbb{Q}[\sqrt{d}]$, where d is square-free integer. And compute the discriminant d_k.

5, $d_{K/k}(a_1, \cdots, a_n) \neq 0 \Leftrightarrow a_1, \cdots, a_n$ are k-linear independence.

6, (Dedekind)

(1), Show that $f(x) = x^3 + x^2 - 2x + 8$ is irreducible in $\mathbb{Q}[x]$.

(2), Find the discriminant of $f(x)$.

(3), Let θ be a root of $f(x)$ and $k = \mathbb{Q}(\theta)$. Compute $d_{k/\mathbb{Q}}(\theta)$.

(4), Show that $4/\theta, \frac{1}{2}(\theta^2 + \theta) \in \mathfrak{o}_k$.

(5), $\{1, \theta, 4/\theta\}$ is an integral basis of k and find the discriminant of $k = \mathbb{Q}(\theta)$.

(6), For any $\alpha \in \mathfrak{o}_k$, $\{1, \alpha, \alpha^2\}$ is not an integral basis.

(7), The prime 2 splits completely in k.

7,

8, Let $\mathfrak{a} \subset \mathfrak{o}_k$ be an ideal. Let the generalized Euler function $\phi(\mathfrak{a})$ be the number of prime residue classes modulo $\mathfrak{a}$, that is, the residue classes $\overline{\alpha} \in \mathfrak{o}_k/\mathfrak{a}$ such that $\gcd(\alpha, \mathfrak{a}) = \mathfrak{o}_k$. Then

(1), for all $\alpha \in \mathfrak{o}_k$ prime to $\mathfrak{a}$we have

$$\alpha^{\phi(\mathfrak{a})} \equiv 1 \,(\mathrm{mod}\, \mathfrak{a}).$$

(2), for any prime ideal $\mathfrak{p}$ and for any $\alpha \in \mathfrak{o}_k$

$$\alpha^{\phi(\mathfrak{a})} \equiv \alpha (\mathrm{mod}\, \mathfrak{p}).$$

(3),

$$\phi(\mathfrak{a}) = N(\mathfrak{a}) \prod_{\mathfrak{p}|\mathfrak{a}} \left(1 - \frac{1}{N\mathfrak{p}}\right).$$

9, Compute the principal ideal (6) as the product of the prime ideals in the ring of integers $\mathfrak{o}_k$where $k = \mathbb{Q}(\sqrt{-5})$.

10, Show that every nonzero prime ideal in $\mathfrak{o}_k$ contains exactly one integer prime.

11, Let $\mathfrak{a}$ be an integral ideal of $\mathfrak{o}_k$. Then (1) $Norm(\mathfrak{a}) \in \mathfrak{a}$. (2) If $Norm(\mathfrak{a})$ is a prime number; then $\mathfrak{a}$ is a prime ideal. Conversely, true or false?

12, Find a prime ideal factorization of $(2), (5)$ in $\mathbb{Z}[i]$.

13, Suppose that $\mathfrak{a}$ is an ideal of an integral domain R, then there exists an ideal $\mathfrak{b}$ such that $\mathfrak{ab}$ is a principal ideal.

14, Let R be a Dedekind domain with finitely many prime ideals. Then R is a principal ideal domain.

15, Let $a = 1 + i, b = 3 + 2i$, and $c = 3 + 4i$ as elements of $\mathbb{Z}[i]$.

(1) Prove that the ideals $\mathfrak{a} = (a), \mathfrak{b} = (b)$, and $\mathfrak{c} = (c)$ are coprime in pairs.

(2) Compute the number of the quotient ring $\mathbb{Z}[i]/(\mathfrak{abc})$.

(3) Find a single element in $\mathbb{Z}[i]$ that is congruent to 1 modulo $\mathfrak{a}$, 2 modulo $\mathfrak{b}$, and 3 modulo $\mathfrak{c}$.

16, Compute the class group and the class number of the following quadratic fields:

$$\mathbb{Q}(\sqrt{3}), \quad \mathbb{Q}(\sqrt{5}), \quad \mathbb{Q}(\sqrt{-3}), \quad \mathbb{Q}(\sqrt{-5}).$$

17, Show that $\mathbb{Q}(\sqrt{-23})$ has class number 3.

18, Compute the group W_k of roots of unity for quadratic fields $k = \mathbb{Q}(\sqrt{d})$ where d is a square-free integer.

19, Find a unit in $\mathbb{Q}(\sqrt[3]{6})$ and show that this field has class number $h = 1$.

20, Compute the fundamental unit of the real quadratic field $\mathbb{Q}(\sqrt{3})$.

21, There exist only finitely many number fields with bounded discriminant.

22, Statement and show that the ration prime p decomposes in quadratic fields $\mathbb{Q}(\sqrt{d})$.

23, Let K/k be an extension of algebraic number fields. Then, for $0 \neq \alpha \in K$,

$$N_{K/k}(\alpha\mathfrak{O}_K) = N_{K/k}(\alpha)\mathfrak{o}_k.$$

24, Let K be a finite Galois extension of $\mathbb{Q}$with Galois group G. For each prime ideal $\mathfrak{P}$ of $\mathfrak{O}_K$, let $I_{\mathfrak{P}}$ be the inertia group. Show that the groups $I_{\mathfrak{P}}$ generate G.

25, (1), Find the Galois group $\mathrm{Gal}(K/\mathbb{Q})$ where $K = \mathbb{Q}(\sqrt{-1}, \sqrt{5})$.

(2), Find the decomposition fields, inertia fields, decomposition groups and inertia groups of $(2), (5)$ for $K = \mathbb{Q}(\sqrt{-1}, \sqrt{5})$ over $\mathbb{Q}$.

26, Suppose that the extension $K/\mathbb{Q}$ is normal and has a Galois group which is simple but not cyclic. Show that there is no rational prime p such that (p) remains prime in K.

27, Let $\zeta^n = 1$ and assume that

$$\alpha = \frac{\sum_{i=1}^{m} \zeta^{n_i}}{m}$$

is an algebraic integer. Show that either $\alpha = \zeta^{n_i}$ for each i or $\alpha = 0$.

Chapter 2

Valuation Theory

There are two obvious ways of approaching algebraic number theory, one by means of ideals and the other by means of valuations. Each has its advantages, and it is desirable to be familiar with both. In this section we represent the valuation theory approach.

2.1 Valuations and Completions

2.1.1 Basic concepts

Definition 2.1. *For any field k, an absolute value(valuation) of k is a mapping*

$$\begin{aligned} |\cdot| : k &\longrightarrow \mathbb{R} \\ \alpha &\longmapsto |\alpha| \end{aligned}$$

which satisfies the following conditions, for any $\alpha, \beta \in k$,
(1), $|\alpha| \geq 0$ and $|\alpha| = 0 \Leftrightarrow \alpha = 0$.
(2), $|\alpha\beta| = |\alpha||\beta|$.
(3), $|\alpha + \beta|^a \leq |\alpha|^a + |\beta|^a$, for some $a > 0$

Clearly, we have $|1_k| = |-1_k| = 1$ and $|\alpha| = |-\alpha|$. Two valuations $|\cdot|_1$ and $|\cdot|_2$ of k are called *equivalent* if $|\alpha|_2 = |\alpha|_1^c$ form some fixed $c > 0$ and for all $\alpha \in k$. An equivalent class of valuations is called a *place* of k, or *prime divisor of k*. A valuation of k induces a metric

$$d(\alpha, \beta) = |\alpha - \beta|^a$$

under which k becomes a topological field, that is, k is Hausdorff topological space in which the field operations, i.e., addition, multiplication and inversion operations, are continuous.

Lemma 2.2. *Let $|\cdot|_1$ and $|\cdot|_2$ be valuations on a field k. The following statements are equivalent:*

(1), the valuations $|\cdot|_1$ and $|\cdot|_2$ are equivalent;

(2), the valuations $|\cdot|_1$ and $|\cdot|_2$ induce the same topology;

(3), for any $\alpha \in k$, we have $|\alpha|_1 < 1$ if and only if $|\alpha|_2 < 1$.

Proof. (1) $\Rightarrow$ (2) : If we assume (1), we get that, for any $\alpha \in k$,

$$|x - \alpha|_2 < r \Leftrightarrow |x - \alpha|_1 < r^{1/c}.$$

So that any open ball with respect to $|\cdot|_1$ is also open ball with respect to $|\cdot|_2$. This is enough to show that $|\cdot|_1$ and $|\cdot|_2$ induce the same topology.

(2) $\Rightarrow$ (3) : If $|\cdot|_1$ and $|\cdot|_2$ induce the same topology, then any sequence that converges with respect to one valuation must be also converges in the other. For given any $\alpha \in k$, we have that

$$|\alpha|_1 < 1 \Leftrightarrow |\alpha^n|_1 \to 0 \Leftrightarrow |\alpha^n|_2 \to 0 \Leftrightarrow |\alpha|_2 < 1.$$

This gives (3).

(3) $\Rightarrow$ (1) : Since $|\cdot|_1$ is not trivial, we can assume that there exists $0 \neq x_0 \in k$ such that $|x_0|_1 < 1$. Define $c > 0$, such that $|x_0|_2 = |x_0|_1^c$. For any $0 \neq x \in k$, we can assume that $|x|_1 < 1$ (otherwise just replace x by $1/x$). We now say $|x|_1 = |x_0|_1^\lambda$. If $\frac{m}{n} > \lambda$, with $m, n \in \mathbb{N}$ and $n > 0$, then

$$\left|\frac{x_0^m}{x^n}\right|_1 = \frac{|x_0|_1^m}{|x_0|_1^{\lambda n}} = |x_0|_1^{\frac{m}{\lambda n}} < 1.$$

Thus $|x_0^m/x^n|_2 < 1$, so

$$|x|_2 > |x_0|_2^{m/n}.$$

Similarly, if $\frac{m}{n} < \lambda$, with $m, n \in \mathbb{N}$ and $n > 0$, we get that

$$|x|_2 < |x_0|_2^{m/n}.$$

Therefore, we get

$$|x|_2 = |x_0|_2^\lambda = |x_0|_1^{c\lambda} = |x|_1^c,$$

for all $x \in k$. □

By the above lemma, every valuation is equivalent to a valuation for which $a = 1$ in the definition. For our purposes we can always replace a given valuation by an equivalent one. Therefore, we will henceforth assume that all valuations satisfied the usual triangle inequality

$$|\alpha + \beta| \leq |\alpha| + |\beta|. \tag{2.1}$$

Note that not all valuations satisfy the usual triangle inequality (2.1). A valuation on a field k is called *archimedean* if $|m1_k| > 1$ for some $m \in \mathbb{Z}$, and *nonarchimedean* otherwise. For nonarchimedean valuations we can radically improve the triangle inequality.

Examples 2.3. *(1), (**Trivial valuation**) $|0| = 0, |x| = 1$ for any $x \neq 0$ is called the trivial valuation of k. Henceforth we shall assume that all valuation are nontrivial. Any valuation over a finite field is trivial.*

*(2), (**Infinite valuation**) Let $|\cdot|_\infty$ be the usually absolute value over the field $k = \mathbb{Q}$, $\mathbb{R}$ or $\mathbb{C}$. Then $(k, |\cdot|_\infty)$ is an archimedean valuation.*

*(3), (**$\mathfrak{p}$-adic valuation**) Let k be a number field and $\mathfrak{p}$ be any prime ideal of $\mathfrak{o}_k$. For any $\alpha \in k$,*

$$(\alpha) = \mathfrak{p}^{\mathrm{ord}_\mathfrak{p}(\alpha)}\mathfrak{a}, \quad (\mathfrak{a}, \mathfrak{p}) = 1.$$

Here $(\mathfrak{a}, \mathfrak{p}) = 1$ means $\mathfrak{a} = \mathfrak{b}/\mathfrak{c} \in J_k$, where $\mathfrak{b}, \mathfrak{c} \subset \mathfrak{o}_k, (\mathfrak{bc}, \mathfrak{p}) = 1$. Let $c > 1$ be a fixed real number. Then we define

$$|\alpha|_\mathfrak{p} = c^{-\mathrm{ord}_\mathfrak{p}(\alpha)}.$$

$(k, |\cdot|_\mathfrak{p})$ is a nonarchimedean valuation of k. In particular, we can take $c = \mathrm{N}\mathfrak{p}$ which is called the normalized $\mathfrak{p}$-adic valuation.

Lemma 2.4. *Let $|\cdot|$ be a valuation which satisfies the triangle inequality over any field k. The following statements are equivalent:*

(1), the valuation $|\cdot|$ is nonarchimedean;

(2), the set $\{|n1_k| : n \in \mathbb{Z}\}$ is bounded.

(3), for any $\alpha, \beta \in k$,

$$|\alpha + \beta| \leq \max\{|\alpha|, |\beta|\}. \tag{2.2}$$

Proof. (1) $\Rightarrow$ (2) : If $|\cdot|$ is nonarchimedean, then we have $|n1_k| \leq 1$ for any $n \in \mathbb{N}$. Clearly, the set $\{|n1_k| : n \in \mathbb{Z}\}$ is bounded.

(2) $\Rightarrow$ (3) : Suppose that there exists $M > 0$, such that $|n1_k| \leq M$, for all $n \in \mathbb{Z}$. Then

$$\begin{aligned} |(\alpha + \beta)^n| &= \left| \sum_{i=0}^{n} C_n^i \alpha^{n-i} \beta^i \right| \\ &\leq M(n+1)(\max\{|\alpha|, |\beta|\})^n \end{aligned}$$

Taking n-th root, we have

$$|\alpha + \beta| \leq \sqrt[n]{M(n+1)}\, \max\{|\alpha|, |\beta|\}.$$

We get the result by let $n \to \infty$.

(3) $\Rightarrow$ (1) : For every $n \in \mathbb{Z}$, then $|n1_k| = |1_k + \cdots + 1_k| \leq |1_k| = 1$. Thus $|\cdot|$ is a nonzrchimedean valuation. $\square$

A metric having the property (2.2) is called an *ultrametric*. In particular, if $|\alpha| \neq |\beta|$, then we immediately obtain from an ultrametric

$$|\alpha + \beta| = \max\{|\alpha|, |\beta|\}. \tag{2.3}$$

Let $|\cdot|_v$ be a nonarchimedean valuation on any field k. Let

$$\begin{aligned}
\mathfrak{o}_{(v)} &= \{\alpha \in k \,:\, |\alpha|_v \leq 1\},\\
\mathfrak{p}_{(v)} &= \{\alpha \in k \,:\, |\alpha|_v < 1\},\\
U_{(v)} &= \{\alpha \in k \,:\, |\alpha|_v = 1\}.
\end{aligned}$$

Proposition 2.5. *Let $|\cdot|_v$ be a nonarchimedean valuation on any field k. $\mathfrak{o}_{(v)}$ is a local ring with maximal ideal $\mathfrak{p}_{(v)}$ and quotient field k. The $U_{(v)}$ is the group of units of the domain $\mathfrak{o}_{(v)}$.*

Proof. Since $|\cdot|_v$ is a non-archimedean on k, $1_k \in \mathfrak{o}_{(v)}$ and for any $\alpha, \beta \in \mathfrak{o}_{(v)}$, it follows that

$$|\alpha + \beta| \leq \max\{|\alpha|, |\beta|\} \leq 1 \text{ and } |\alpha\beta| = |\alpha||\beta| \leq 1,$$

so that $\alpha \pm \beta, \alpha\beta \in \mathfrak{o}_{(v)}$. It is easily seen that $\mathfrak{o}_{(v)}$ has no zero divisors. Therefore $\mathfrak{o}_{(v)}$ is a domain. For any nonzero element $\alpha \in k$, either $\alpha \in \mathfrak{o}_{(v)}$ or $\alpha^{-1} \in \mathfrak{o}_{(v)}$, then k is the quotient field of $\mathfrak{o}_{(v)}$.

We need to prove that $\mathfrak{p}_{(v)}$ is a maximal ideal of $\mathfrak{o}_{(v)}$. It is easily seen that $\mathfrak{p}_{(v)}$ is an ideal of $\mathfrak{o}_{(v)}$. Let $\mathfrak{m}$ be an ideal of $\mathfrak{o}_{(v)}$, which satisfies to

$$\mathfrak{p}_{(v)} \subsetneq \mathfrak{m} \subseteq \mathfrak{o}_{(v)}.$$

For every $\alpha \in \mathfrak{m}$ but not in $\mathfrak{p}_{(v)}$, we know $|\alpha| = 1$ and $|\alpha^{-1}| = 1$, then $1 = \alpha\alpha^{-1} \in \mathfrak{m}$. So $\mathfrak{m} = \mathfrak{o}_{(v)}$, that is, $\mathfrak{p}_{(v)}$ is a maximal ideal. Let $\mathfrak{a}$ be any proper ideal of $\mathfrak{o}_{(v)}$. In the similar way, we can get $\mathfrak{a} \subseteq \mathfrak{p}_{(v)}$. So $\mathfrak{o}_{(v)}$ is a local ring with maximal ideal $\mathfrak{p}_{(v)}$.

Finally, for any $\alpha \in U_{(v)}$, then $|\alpha^{-1}| = |\alpha| = 1$, so α is a unit of $\mathfrak{o}_{(v)}$. Obviously, $U_{(v)}$ is the group of units of the domain $\mathfrak{o}_{(v)}$. □

The $\mathfrak{o}_{(\mathfrak{p})}$ is called the *valuation ring of* $\mathfrak{p}$. The field $\mathfrak{o}_{(v)}/\mathfrak{p}_{(v)}$ is called the *residue class field of* $|\cdot|_v$.

2.1.2 Valuations on number fields

We find all valuations over an algebraic number field k as follows.

Proposition 2.6. *If k be an algebraic number field, the archimedean valuations on k are given by $|\alpha| = |\sigma\alpha|_\infty^c$ where $c > 0$ and σ is any embedding $k \hookrightarrow \mathbb{C}$.*

Proof. We will prove the following statements in turn.

• For any $n \in \mathbb{N}$ and $n > 1$, then $|n| > 1$.

If not, then there exists some $n_0 \in \mathbb{N}$ such that $n_0 > 1$ but $|n_0| \leq 1$. For any $n, N \in \mathbb{N}$ with $n > 1$, write n^N in the scale of n_0:

$$n^N = a_0 + a_1 n_0 + \cdots + a_r n_0^r$$

where $0 \leq a_i < n_0$ for $i = 0, 1, \ldots, r$ and $0 \leq r \leq N \log_{n_0} n$. Let A be the upper bound for $|a|$ where $0 \leq a < n_0$, then

$$\begin{aligned} |n|^N &\leq |a_0| + |a_1||n_0| + \cdots + |a_r||n_0|^r \\ &\leq A(1 + r) \leq A(1 + N \log_{n_0} n); \end{aligned}$$

taking N-th roots and letting $N \to \infty$ would give $|n| \leq 1$ for all $n > 1$, which is a contradiction with $|\cdot|$ being archimedean. Thus $|n| > 1$ for any $n \in \mathbb{N}$, $n > 1$.

• For every $m \in \mathbb{Z}$ there exists a fixed $c > 0$, such that $|m| = |m|_\infty^c$.

For any $m_1, m_2 \in \mathbb{N}$ with $m_1, m_2 > 1$, the same argument shows that

$$|m_1|^N \leq B \left(1 + N \log_{m_2} m_1\right) |m_1|^{N \log_{m_2} m_1},$$

where B is the upper bound for $|a|$ where $0 \leq a < m_2$, taking N-th roots and letting $N \to \infty$ would give

$$|m_1| \leq |m_2|^{\log_{m_1} m_2},$$

i.e.,

$$|m_1|^{\frac{1}{\log m_1}} \leq |m_2|^{\frac{1}{\log m_2}}.$$

Since m_1 and m_2 can be arbitrary, it follows that $|m|^{\frac{1}{\log m}}$ is a constant, saying e^c. Then $|m| = m^c$ for $m \in \mathbb{N}$, $m > 1$. It follows immediately that $|m| = |m|_\infty^c$ for any $m \in \mathbb{Z}$. Furthermore, we also get that $|m| = |m|_\infty^c$ for any $m \in \mathbb{Q}$.

We return to the proof of the theorem. It is clearly enough to prove the result when α is in $\mathfrak{o}_k$. Now let α be a nonzero element of $\mathfrak{o}_k$, and order the σ_i so that

$$|\sigma_1 \alpha|_\infty \geq |\sigma_2 \alpha|_\infty \geq \cdots \geq |\sigma_n \alpha|_\infty.$$

This ordering depends only on α. Let c have the value obtained above. For any $N \geq 1$, write

$$f(x) = \prod_{i=1}^{n} (x - \sigma_i \alpha^N) = x^n + a_1 x^{n-1} + \cdots + a_n \in \mathbb{Z}[X],$$

and

$$P_m = \prod_{i=1}^{m} \sigma_i \alpha^N.$$

The a_m are symmetric functions of the $\sigma_i \alpha^N$ and the largest summand in a_m is $\pm P_m$; so $|a_m|_\infty < M|P_m|_\infty$ where M depends only on n. Moreover, if $|\sigma_m \alpha|_\infty > |\sigma_{m+1}\alpha|_\infty$ then once N is large enough this summand is much larger than any other in a_m by

$$\begin{aligned}
\frac{|a_m|_\infty}{|P_m|_\infty} - 1 &= \frac{|\sum_{1\le j_1<\cdots<j_m\le n} \prod_{i=1}^m \sigma_{j_i}\alpha^N|_\infty}{|P_m|_\infty} - 1 \\
&\le \left| \frac{\sum_{j_i \neq i} \prod_{i=1}^m \sigma_{j_i}\alpha^N}{P_m} \right|_\infty \\
&\le \sum_{\substack{j_i \neq i \\ \text{for some } i}} \prod_{i=1}^{m} \left| \frac{\sigma_{j_i}\alpha}{\sigma_i \alpha} \right|_\infty^N \to 0, \quad \text{as} \quad N \to \infty,
\end{aligned}$$

which implies $|a_m|_\infty > \frac{1}{2}|P_m|_\infty$. Also $|a_m| = |a_m|_\infty^c$ because the $a_m \in \mathbb{Z}$, and hence

$$\frac{1}{2^c} < \frac{|a_m|}{|P_m|_\infty^c} < M^c,$$

where the first inequality only holds if $|\sigma_m\alpha|_\infty > |\sigma_{m+1}\alpha|_\infty$ and the second inequality holds for any m.

As follows, we shall show that

$$\begin{aligned}
&|\sigma_\mu \alpha|_\infty^c > |\alpha| > |\sigma_{\mu+1}\alpha|_\infty^c, \text{ for any } \mu, \\
&|\alpha| > |\sigma_1 \alpha|_\infty^c \text{ and } \sigma_n\alpha|_\infty^c > |\alpha|
\end{aligned}$$

all do not hold. It follows immediately that $|\alpha| = |\sigma\alpha|_\infty^c$ for some embedding σ, which completes the proof.

We need only consider the case of

$$|\sigma_\mu \alpha|_\infty^c > |\alpha| > |\sigma_{\mu+1}\alpha|_\infty^c,$$

for some μ. For two cases $|\alpha| > |\sigma_1\alpha|_\infty^c$ or $|\alpha| < |\sigma_n\alpha|_\infty^c$, the similar argument would give the same contradiction. From $f(\alpha^N) = 0$, we have that

$$\left|a_\mu \alpha^{N(n-\mu)}\right| = \left|\alpha^{Nn} + \cdots + a_{\mu-1}\alpha^{N(n-\mu+1)} + a_{\mu+1}\alpha^{N(n-\mu-1)} + \cdots + a_n\right|.$$

Using the triangle inequality of the valuation, we obtain (set $a_0 = 1$),

$$\begin{aligned}
\frac{|a_\mu|}{|P_\mu|_\infty^c} &= \left|\alpha^{-N(n-\mu)}\right| \left|\sum_{i=0}^{\mu-1} a_i\alpha^{N(n-i)} + \sum_{i=\mu+1}^{n} a_i\alpha^{N(n-i)}\right| / |P_\mu|_\infty^c \\
&= \left|\sum_{i=0}^{\mu-1} a_i\alpha^{N(\mu-i)} + \sum_{j=1}^{n-\mu} a_{\mu+j}\alpha^{-Nj}\right| / |P_\mu|_\infty^c \\
&\le \sum_{i=0}^{\mu-1} \frac{|a_i||\alpha|^{N(\mu-i)}}{|P_\mu|_\infty^c} + \sum_{j=1}^{n-\mu} \frac{|a_{\mu+j}||\alpha|^{-Nj}}{|P_\mu|_\infty^c} \\
&< \sum_{i=0}^{\mu-1} \frac{M^c|P_i|_\infty^c|\alpha|^{N(\mu-i)}}{|P_\mu|_\infty^c} + \sum_{j=1}^{n-\mu} \frac{M^c|P_{\mu+j}|_\infty^c}{|P_\mu|_\infty^c|\alpha|^{Nj}} \\
&= M^c\left(\sum_{i=0}^{\mu-1} \frac{|\alpha^N|^{\mu-i}}{|\prod_{\nu=i+1}^{\mu}\sigma_\nu\alpha^N|_\infty^c} + \sum_{j=1}^{n-\mu} \frac{|\prod_{\nu=\mu}^{\mu+j}\sigma_\nu\alpha^N|_\infty^c}{|\alpha^N|^j}\right) \\
&= M^c\left\{\sum_{i=0}^{\mu-1}\left(\prod_{\nu=i+1}^{\mu}\frac{|\alpha|}{|\sigma_\nu\alpha|_\infty^c}\right)^N + \sum_{j=1}^{n-\mu}\left(\prod_{\nu=\mu+1}^{\mu+j}\frac{|\sigma_\nu\alpha|_\infty^c}{|\alpha|}\right)^N\right\}
\end{aligned}$$

Because $|\sigma_\mu\alpha|_\infty^c > |\alpha| > |\sigma_{\mu+1}\alpha|_\infty^c$, we have

$$\prod_{\nu=i+1}^{\mu}\frac{|\alpha|}{|\sigma_\nu\alpha|_\infty^c} < 1 \quad\text{and}\quad \prod_{\nu=\mu+1}^{\mu+j}\frac{|\sigma_\nu\alpha|_\infty^c}{|\alpha|} < 1.$$

Letting $N \to \infty$, we obtain the last term of the above inequality tends to the zero which also implies $|a_\mu|/|P_\mu|_\infty^c$ tends to zero. This contradicts the fact that $|a_\mu|/|P_\mu|_\infty^c > 1/2^c$. The proof of the theorem is now completed. □

By the above proposition, there is a bijection between the archimedean places and embeddings k into $\mathbb{C}$ up to conjugation. In our case there are $r_1 + r_2$ classes the archimedean places. The archimedean places $\mathfrak{p}$ or v are often called the *infinite places* or the *infinite primes*, say $\mathfrak{p}|\infty$ or $v|\infty$. We say that $|\cdot|_\sigma$ is a *real place* if it corresponds to a real embedding σ. And $|\cdot|_\sigma$ is called a *complex place* if it corresponds to a pair of complex conjugate embeddings $\sigma = \bar{\sigma}$.

Proposition 2.7. *Let $|\cdot|$ be a nonarchimedean valuation of a number field k. Then there exists a prime ideal $\mathfrak{p}$ of $\mathfrak{o}_k$ and a constant $c > 1$ such that*

$$|\alpha| = c^{-\mathrm{ord}_\mathfrak{p}(\alpha)},$$

for every nonzero element $\alpha \in k$.

Proof. The proof will be divided into three steps.

• For any $\alpha \in \mathfrak{o}_k$, we have $|\alpha| \leq 1$.

Clearly, we have $|n| \leq 1$ for any $n \in \mathbb{Z}$. Any $\alpha \neq 0$ in $\mathfrak{o}_k$ satisfies an equation

$$\alpha^m + a_1\alpha^{m-1} + \cdots + a_m = 0$$

where $a_i \in \mathbb{Z}$ for all i. By the inequality (2.2), we obtain

$$\begin{aligned} |\alpha|^m &= |a_1\alpha^{m-1} + \cdots + a_m| \\ &\leq \max\{|a_1\alpha^{m-1}|, \ldots, |a_m|\} \\ &\leq \max\{|\alpha|^{m-1}, \ldots, 1\}. \end{aligned}$$

However if $|\alpha| > 1$, then $|\alpha|^m > \max\{|\alpha|^{m-1}, \ldots, 1\}$. It is a contradiction, so $|\alpha| \leq 1$ for all α in $\mathfrak{o}_k$.

• The set $\mathfrak{p} = \{\alpha \in \mathfrak{o}_k : |\alpha| < 1\}$ is a prime ideal of $\mathfrak{o}_k$.

If $|\alpha| = 1$ for all $\alpha \neq 0$ in $\mathfrak{o}_k$ then our valuation would be trivial; so there exists some $0 \neq \alpha \in \mathfrak{o}_k$ with $|\alpha| < 1$. Then using the inequality (2.2) again, $\mathfrak{p}$ is a ideal of $\mathfrak{o}_k$ because $\alpha, \beta \in \mathfrak{p},\ \gamma \in \mathfrak{o}_k$ implies $\alpha \pm \beta, \alpha\beta, \alpha\gamma \in \mathfrak{p}$, and $\mathfrak{p}$ is prime because $|\alpha_1\alpha_2| < 1$ implies $|\alpha_1| < 1$ or $|\alpha_2| < 1$.

• There exists $c > 1$ such that $|\alpha| = c^{-\mathrm{ord}_\mathfrak{p}(\alpha)}$ for any nonzero $\alpha \in k$.

We now choose $\pi \in \mathfrak{p}\backslash\mathfrak{p}^2$, that is, $\mathrm{ord}_\mathfrak{p}(\pi) = 1$. For any nonzero $\alpha \in k$, denote $m = \mathrm{ord}_\mathfrak{p}(\alpha)$, then

$$\mathrm{ord}_\mathfrak{p}(\alpha/\pi^m) = \mathrm{ord}_\mathfrak{p}(\alpha) - \mathrm{ord}_\mathfrak{p}(\pi^m) = 0.$$

And hence $(\mathfrak{p}, (\alpha/\pi^m)) = 1$, which means

$$\left(\frac{\alpha}{\pi^m}\right) = \frac{\mathfrak{a}_1}{\mathfrak{a}_2}, \quad \text{where} \quad \mathfrak{a}_1, \mathfrak{a}_2 \subseteq \mathfrak{o}_k,\ (\mathfrak{p}, \mathfrak{a}_1\mathfrak{a}_2) = 1.$$

According to the Chinese remainder theorem, there exists a $\beta_2 \in \mathfrak{o}_k$ such that

$$\begin{cases} \beta_2 \equiv 0 \pmod{\mathfrak{a}_2} \\ \beta_2 \equiv 1 \pmod{\mathfrak{p}} \end{cases},$$

i.e. we can find β_2 in $\mathfrak{a}_2$ and prime to $\mathfrak{p}$. Write $\beta_1 = \beta_2\alpha/\pi^m$, so that $\beta_1 \in \mathfrak{a}_1$. Neither β_1 nor β_2 is in $\mathfrak{p}$, so they both have valuation 1; thus $|\alpha| = |\pi|^m$. Let $c = 1/|\pi| > 1$, then $|\alpha| = c^{-\mathrm{ord}_\mathfrak{p}(\alpha)}$ for any nonzero $\alpha \in k$. □

Conversely, any $\mathfrak{p}$ and c determine a nonarchimedean valuation; and changing c only change the valuation within its places. Let $\mathfrak{p}$ and $\mathfrak{q}$ be two distinct prime ideals of a number field k. Then the $\mathfrak{p}$-adic valuations $|\cdot|_\mathfrak{p}$ and $|\cdot|_\mathfrak{q}$ are inequivalent, see exercise. Simply, for distinct prime numbers p and q, we have $|p|_p < 1$ but $|q|_p = 1$, it follows that the p-adic valuations

$|\cdot|_p$ and $|\cdot|_q$ are not equivalent. This place v can be identified with $\mathfrak{p}$ and will be called a *finite place*, or *finite prime*, say $\mathfrak{p} < \infty$ or $v < \infty$. In short, there is bijection between all places of k and $r_1 + r_2$ archimedean places and all prime ideals of k.

2.1.3 Product formula

Let v or $\mathfrak{p}$ be any place of an algebraic number field k including infinite places. There exists a canonical choice of valuations which is called the *normalized valuations* :

(1), v is a real place which corresponds to a real embedding σ:

$$|\alpha|_v = |\sigma\alpha|_{\mathbb{R}} = |\sigma\alpha|_\infty;$$

(2), v is a complex place which corresponds to a pair of complex embeddings $\sigma = \bar{\sigma}$:

$$|\alpha|_v = |\sigma\alpha|_{\mathbb{C}} = |\sigma\alpha|_\infty^2;$$

(3), v is a finite place which corresponds to a prime ideal $\mathfrak{p}$ of $\mathfrak{o}_k$:

$$|\alpha|_v = |\alpha|_{\mathfrak{p}} = \mathrm{N}(\mathfrak{p})^{-\mathrm{ord}_{\mathfrak{p}}(\alpha)}.$$

Theorem 2.8. *For any nonzero $\alpha \in k$, we have $|\alpha|_v = 1$ for almost all places v, i.e., for all but finitely many v and*

$$\prod_v |\alpha|_v = 1$$

where the product runs over all normalized valuations $|\cdot|_v$ of k.

Proof. For all nonzero $\alpha \in k$, we have

$$(\alpha) = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g}, \tag{2.4}$$

where $e_i = \mathrm{ord}_{\mathfrak{p}_i}(\alpha) \in \mathbb{Z}^\times$ and $S = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_g\}$ are distinct prime ideals of k. Clearly, $|\alpha|_{\mathfrak{p}} = 1$ for any $\mathfrak{p} \notin S$. We now compute $\mathrm{N}((\alpha))$ in two ways, one which will make appear the finite places, and the other the infinite places. Now take norms of the equation (2.4) to obtain

$$\mathrm{N}((\alpha)) = \mathrm{N}\mathfrak{p}_1{}^{e_1} \cdots \mathrm{N}\mathfrak{p}_g{}^{e_g} = \prod_{\mathfrak{p} \in S} |\alpha|_{\mathfrak{p}}^{-1} = \prod_{v < \infty} |\alpha|_v^{-1}.$$

And

$$\mathrm{N}((\alpha)) = |\mathrm{N}(\alpha)|_\infty = \prod_{i=1}^n |\sigma_i\alpha|_\infty = \prod_{v|\infty} |\alpha|_v.$$

Therefore,

$$\prod_v |\alpha|_v = \prod_{v|\infty} |\alpha|_v \prod_{v<\infty} |\alpha|_v = 1.$$

□

2.1.4 Completions

Let $|\cdot|_v$ be any valuation over a field k. Then the valuation induces a metric

$$d(\alpha, \beta) = |\alpha - \beta|_v,$$

such that $(k, |\cdot|_v)$ is a metric space. A sequence $\{\alpha_n\}$ of elements of k is called a *Cauchy sequence* if for any $\epsilon > 0$ there exists a positive integer N such that for any $n, m \geq N$, we have $|\alpha_n - \alpha_m|_v < \epsilon$. The sequence $\{\alpha_n\}$ *converges* to an element α of k if for any $\epsilon > 0$ there exists a positive integer N such that for any $n \geq N$, we have $|\alpha_n - \alpha|_v < \epsilon$. A *completion* of the field k with respect to the valuation $|\cdot|_v$ is a completion of k as a metric space, that is, any Cauchy sequence is convergent in the completion of k.

More specifically, let $\mathscr{R}$ denote the set of all Cauchy sequences with respect to $|\cdot|_v$ and let $\mathscr{P}$ denote the set of all null Cauchy sequences, i.e., the set of all Cauchy sequences convergent to 0.

Lemma 2.9. *$\mathscr{P}$ is a maximal ideal of the ring $\mathscr{R}$.*

Proof. It is clear that $\mathscr{P}$ is closed under addition. Let $x = (x_n) \in \mathscr{P}, y = (y_n) \in \mathscr{R}$. Then $|y_n|_v$ is a bounded sequence, so that $|x_n y_n|_v \to 0 (n \to \infty)$. Thus, $xy \in \mathscr{P}$. Thus $\mathscr{P}$ is an ideal of $\mathscr{R}$. Let $x = (x_n) \in \mathscr{R} \setminus \mathscr{P}$. By adding an element of $\mathscr{P}$ to x, we can find a sequence $y = (y_n) \in \mathscr{R} - \mathscr{P}$, such that y_n are nonzero for all n. Then $y^{-1} = (y_n^{-1}) \in \mathscr{R}$, for $|y_n|_v \geq c > 0$ for some c since $y \notin \mathscr{P}$. Then we deduce that y^{-1} is a Cauchy sequence, since

$$|y_n^{-1} - y_m^{-1}|_v \leq c^{-2} |y_n - y_m|_v \to 0,$$

as $m, n \to \infty$. Then $y^{-1}y$ is contained in the ideal generated by x and $\mathscr{P}$. Thus, $(x, \mathscr{P}) = \mathscr{R}$, and $\mathscr{P}$ is maximal. □

There is a natural injective map ρ from k to $\mathscr{R}/\mathscr{P}$ sending an element to the constant Cauchy sequence. We now extend the valuation on k to $\mathscr{R}/\mathscr{P}$ by, still denote by $|\cdot|_v$,

$$|\alpha|_v = |(\alpha_n)|_v = \lim_{n\to\infty} |\alpha_n|_v$$

for any $\alpha = (\alpha_n)_{n=1}^{\infty} \in \mathscr{R}/\mathscr{P}$. This limit exists because $\big||\alpha|_v - |\beta|_v\big|_\infty \leq |\alpha-\beta|_v$ implies that $\{|\alpha_n|_v\}$ is a Cauchy sequence of real numbers. Obviously this limit does not depend on the choice of the representative (α_n) of α. We have the following fundamental facts:

(1), The valuation $|\cdot|_v$ of k is also a valuation on the field $\mathscr{R}/\mathscr{P}$;
(2), The field $\mathscr{R}/\mathscr{P}$ is complete with respect to the valuation $|\cdot|_v$;
(3), $\rho(k)$ is dense in $\mathscr{R}/\mathscr{P}$; furthermore,
(4), $\mathscr{R}/\mathscr{P}$ is unique up to a unique isomorphism fixing k.

The detailed proof is left as an exercise to the reader. Define k_v to be the completion of k with respect to the metric defined by $|\cdot|_v$. Then

$$k_v = \mathscr{R}/\mathscr{P}.$$

We shall denote the natural embedding of k into k_v by ρ_v. Whenever confusion will not arise, we shall identify k with $\rho_v(k)$ and consider k as a subfield of k_v, that is, we shall identify α and (α) for any $\alpha \in k$.

Proposition 2.10. *The valuation $|\cdot|$ is nonarchimedean on k_v if and only if it is so on k. If $|\cdot|$ is nonarchimedean, then the set of values taken by $|\cdot|$ on k and k_v are the same.*

Proof. The first part follows from Lemma (2.4) which asserts that a valuation is non-archimedean if and only if $|n1_k| < 1$ for all integers n. Since the valuation on k_v extends the valuation on k, the first statement follows.

For the second, we only need to find $\beta \in k$ such that $|\beta| = |\alpha|$ for any $\alpha \in k_v$. Since k is dense in k_v, there exists $\beta \in k$ such that

$$|\beta - \alpha| < |\alpha|.$$

According to the formula (2.3), we have $|\beta| = \max\{|\alpha|, |\beta-\alpha|\} = |\alpha|$, which completes the second part of the theorem. □

2.2 Local Fields

A *global field* k is an algebraic number field, or a finite extension of $\mathbb{F}_p(t)$, i.e., the field of rational functions in one variable over the finite field. The completions k_v of a global field k at any place v are called *local fields*. Obviously, if v is a real place, then $k_v = \mathbb{R}$; if v is a complex place, then $k_v = \mathbb{C}$. In what follows, We will mainly consider local fields of an algebraic number field at a finite place.

2.2.1 The structure of local fields: $\mathfrak{p}$-number fields

Let $v_\mathfrak{p}$ be a fixed finite place associated to a prime ideal $\mathfrak{p}$ of $\mathfrak{o}_k$ with the normalized valuation. The completion $k_\mathfrak{p}$ of k with respect to a nonarchimedean valuation $v_\mathfrak{p}$ is called $\mathfrak{p}$-*adic number field*. Set

$$\begin{aligned}\mathfrak{o}_\mathfrak{p} &= \{\alpha \in k_\mathfrak{p} \,:\, |\alpha|_\mathfrak{p} \leq 1\},\\ \mathfrak{p}_\mathfrak{p} &= \{\alpha \in k_\mathfrak{p} \,:\, |\alpha|_\mathfrak{p} < 1\},\\ U_\mathfrak{p} &= \{\alpha \in k_\mathfrak{p} \,:\, |\alpha|_\mathfrak{p} = 1\}.\end{aligned}$$

The $\mathfrak{o}_\mathfrak{p}$ is called *the ring of* $\mathfrak{p}$-*adic integers*. The field $\mathfrak{o}_\mathfrak{p}/\mathfrak{p}_\mathfrak{p}$ is also called the *residue class field of* $\mathfrak{p}$. The group $U_\mathfrak{p}$ is called the $\mathfrak{p}$-*adic units group* of the domain $\mathfrak{o}_\mathfrak{p}$.

Proposition 2.11. *(1), Then* $\mathfrak{o}_\mathfrak{p}$ *is a local ring with maximal ideal* $\mathfrak{p}_\mathfrak{p}$ *and quotient field* $k_\mathfrak{p}$.

(2),

$$\mathfrak{o}_\mathfrak{p}/\mathfrak{p}_\mathfrak{p} \cong \mathfrak{o}_k/\mathfrak{p} \cong \mathfrak{o}_{(\mathfrak{p})}/\mathfrak{p}_{(\mathfrak{p})}. \tag{2.5}$$

Proof. (1), The proof is similar to Proposition (2.5). Left as an exercise for the reader.

(2) We could define a mapping

$$\varphi : \mathfrak{o}_\mathfrak{p} \longrightarrow \mathfrak{o}_k/\mathfrak{p},$$

as for any Cauchy sequence (a_n) in $\mathfrak{o}_\mathfrak{p}$, via

$$\varphi((a_n)) = a_N (\mathrm{mod}\, \mathfrak{p}),$$

where $N \in \mathbb{N}$ such that when $n, m \geq N, a_n \equiv a_m (\mathrm{mod}\, \mathfrak{p})$. Obviously it is surjective because constant sequences are all in $\mathfrak{o}_\mathfrak{p}$. Its kernel is the set of Cauchy sequences whose elements are eventually all in $\mathfrak{p}$, which is exactly $\mathfrak{p}_\mathfrak{p}$. This completes the first part of the proof. A slight change the the proof actually shows that the second isomorphism, which proves the theorem. □

Example 2.12. *For the rational number field $\mathbb{Q}$, we obtain*

$$\mathbb{Z}_{(p)}/p\mathbb{Z}_{(p)} \cong \mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{Z}/p\mathbb{Z}.$$

Let π be in $\mathfrak{p}$ but not in $\mathfrak{p}^2$ and $\varpi_\mathfrak{p}$ be the image of π in $k_\mathfrak{p}$. Then $\mathrm{ord}_\mathfrak{p}(\pi) = 1$ and $|\varpi_\mathfrak{p}|_\mathfrak{p} = |\pi|_\mathfrak{p} = (\mathrm{N}\mathfrak{p})^{-1}$ and $\mathfrak{p}_\mathfrak{p} = \varpi_\mathfrak{p}\mathfrak{o}_\mathfrak{p} = (\varpi_\mathfrak{p})$. The element $\varpi_\mathfrak{p}$ is called the *uniformizer*, or the *prime element* of $\mathfrak{p}$. Every nonzero element $\alpha \in k_\mathfrak{p}$ can be written uniquely in the form

$$\alpha = u\varpi_\mathfrak{p}^m,\ m \in \mathbb{Z},\ u \in U_\mathfrak{p}. \tag{2.6}$$

The integer m is independent of the choice of $\varpi_\mathfrak{p}$. We may define $\mathrm{ord}_\mathfrak{p}(\alpha) = m$ and $\mathrm{ord}_\mathfrak{p}(0) = \infty$. By the Proposition (2.10), we have the surjective map $\mathrm{ord}_\mathfrak{p}$

$$\begin{aligned} \mathrm{ord}_\mathfrak{p} : k_\mathfrak{p} &\longrightarrow \mathbb{Z} \cup \{\infty\} \\ \alpha &\longmapsto \mathrm{ord}_\mathfrak{p}(\alpha). \end{aligned}$$

The map $\mathrm{ord}_\mathfrak{p}$ is said to be *additive valuation* satisfies

$$\begin{aligned} \mathrm{ord}_\mathfrak{p}(\alpha\beta) &= \mathrm{ord}_\mathfrak{p}(\alpha) + \mathrm{ord}_\mathfrak{p}(\beta), \\ \mathrm{ord}_\mathfrak{p}(\alpha+\beta) &\geq \min\{\mathrm{ord}_\mathfrak{p}(\alpha), \mathrm{ord}_\mathfrak{p}(\beta)\}, \end{aligned}$$

and specifically, if $\mathrm{ord}_\mathfrak{p}(\alpha) \neq \mathrm{ord}_\mathfrak{p}(\beta)$,

$$\mathrm{ord}_\mathfrak{p}(\alpha+\beta) = \min\{\mathrm{ord}_\mathfrak{p}(\alpha), \mathrm{ord}_\mathfrak{p}(\beta)\}.$$

Then we have

$$\begin{aligned} \mathfrak{o}_\mathfrak{p} &= \{\alpha \in k_\mathfrak{p} : |\alpha|_\mathfrak{p} \leq 1\} = \{\alpha \in k_\mathfrak{p} : \mathrm{ord}_\mathfrak{p}(\alpha) \geq 0\}, \\ \mathfrak{p}_\mathfrak{p} &= \{\alpha \in k_\mathfrak{p} : |\alpha|_\mathfrak{p} < 1\} = \{\alpha \in k_\mathfrak{p} : \mathrm{ord}_\mathfrak{p}(\alpha) > 0\}, \\ U_\mathfrak{p} &= \{\alpha \in k_\mathfrak{p} : |\alpha|_\mathfrak{p} = 1\} = \{\alpha \in k_\mathfrak{p} : \mathrm{ord}_\mathfrak{p}(\alpha) = 0\}. \end{aligned}$$

Since (2.6), it is also straightforward to show that

$$k_\mathfrak{p}^\times = U_\mathfrak{p} \times \langle \varpi_\mathfrak{p} \rangle.$$

Actually, we have the following disjoint unions

$$k_\mathfrak{p}^\times = \bigcup_{m\in\mathbb{Z}} \varpi_\mathfrak{p}^m U_\mathfrak{p},\ \mathfrak{o}_\mathfrak{p} = \bigcup_{m=0}^{\infty} \varpi_\mathfrak{p}^m U_\mathfrak{p},\ \mathfrak{p}_\mathfrak{p} = \bigcup_{m=1}^{\infty} \varpi_\mathfrak{p}^m U_\mathfrak{p}.$$

Proposition 2.13. *(1), Every ideal of $\mathfrak{o}_\mathfrak{p}$ is of the form $\mathfrak{p}_\mathfrak{p}^m (m \geq 1)$. Moreover, $\mathfrak{p}_\mathfrak{p}^m = (\varpi^m)$, so that $\mathfrak{o}_\mathfrak{p}$ is a principal ideal domain.*

(2), $\mathfrak{o}_\mathfrak{p}$ and $\mathfrak{p}_\mathfrak{p}$ are the closure of $\mathfrak{o}_k$ and $\mathfrak{p}$, respectively.

Proof. (1) For any ideal $\mathfrak{a}$ of $\mathfrak{o}_\mathfrak{p}$, let

$$r = \min\{\mathrm{ord}_\mathfrak{p}(x) \,:\, 0 \neq x \in \mathfrak{a}\}.$$

Then there exist $\alpha \in \mathfrak{a}$ such that $\mathrm{ord}_\mathfrak{p}(\alpha) = r$. From $\varpi^r/\alpha \in U_\mathfrak{p}$, we obtain $\varpi^r \in \mathfrak{a}$, and hence $(\varpi^r) \subset \mathfrak{a}$.

Furthermore, for any $\beta \in \mathfrak{a}$, we conclude from $\mathrm{ord}_\mathfrak{p}(\beta/\varpi^r) \geq 0$ that $\beta/\varpi^r \in \mathfrak{o}_\mathfrak{p}$, hence that $\beta \in (\varpi^r)$, and finally that $\mathfrak{a} \subset (\varpi^r)$, which proves $\mathfrak{a} = (\varpi^r) = \mathfrak{p}_\mathfrak{p}^r$.

(2) We may view $\mathfrak{o}_\mathfrak{p}$ as the set of equivalent classes of Cauchy sequences (α_n) in k such that $\alpha_n \in \mathfrak{o}_k$ for n sufficiently large. Clearly, we have that $\mathfrak{o}_k \subset \mathfrak{o}_\mathfrak{p}$. For any $\alpha = (\alpha_n) \in \mathfrak{o}_\mathfrak{p}$ and any $0 < \epsilon < 1$, there exist a positive integer N such that $|\alpha_n - \alpha_m| < \epsilon$ for $n, m \geq N$. Take the constant sequence $\beta = (\beta) \in \mathfrak{o}_k$ with $\beta = x_M \in \mathfrak{o}_k$ and $M > N$. Then

$$|\alpha - \beta|_\mathfrak{p} = \lim_{n\to\infty} |\alpha_n - \alpha_N| \leq \epsilon.$$

It immediately follows that $\mathfrak{o}_\mathfrak{p}$ is the closure of $\mathfrak{o}_k$. We conclude similarly that $\mathfrak{p}_\mathfrak{p}$ is the closure of $\mathfrak{p}$. □

Remarks 2.14. *By the above the Proposition, for any $\alpha \in \mathfrak{o}_\mathfrak{p}$, there exist $\beta \in \mathfrak{o}_k$ such that $|\alpha - \beta|_\mathfrak{p} < 1$, i.e., $\alpha - \beta \in \mathfrak{p}_\mathfrak{p}$. Hence $\mathfrak{o}_\mathfrak{p} = \mathfrak{o}_k + \mathfrak{p}_\mathfrak{p}$. It is clear that $\mathfrak{p} = \mathfrak{o}_k \cap \mathfrak{p}_\mathfrak{p}$. According to the second isomorphism theorem, we have*

$$\mathfrak{o}_\mathfrak{p}/\mathfrak{p}_\mathfrak{p} = (\mathfrak{o}_k + \mathfrak{p}_\mathfrak{p})/\mathfrak{p}_\mathfrak{p} \cong \mathfrak{o}_k/(\mathfrak{o}_k \cap \mathfrak{p}_\mathfrak{p}) = \mathfrak{o}_k/\mathfrak{p}.$$

We gave another proof of the isomorphism (2.5) of residue class fields.

Let $\mathscr{A} = \{r_0 = 0, r_1, \ldots, r_{q-1}\}$ be a complete system of representatives of the residue class field $\mathfrak{o}_\mathfrak{p}/\mathfrak{p}_\mathfrak{p}$ where $q = \mathrm{N}\mathfrak{p}$ such that if $r_i \neq r_j$ then $r_i \neq r_j (\mathrm{mod}\, \mathfrak{p})$ and for any $\alpha \in \mathfrak{o}_\mathfrak{p}$, there exists an element $r_i \in \mathscr{A}$ such that $\alpha \equiv r_i (\mathrm{mod}\, \mathfrak{p})$. The set $\varpi^n \mathscr{A}$ is a system of representatives for $\mathfrak{p}_\mathfrak{p}^n/\mathfrak{p}_\mathfrak{p}^{n+1}$.

Proposition 2.15. *Every element $\alpha \in \mathfrak{o}_\mathfrak{p}$ can be written uniquely as*

$$\alpha = \sum_{n=0}^{\infty} a_n \varpi_\mathfrak{p}^n = a_0 + a_1 \varpi_\mathfrak{p} + a_2 \varpi_\mathfrak{p}^2 + \cdots \tag{2.7}$$

with $a_i \in \mathscr{A}$. An element of $\alpha \in k_\mathfrak{p}$ can be written as

$$\alpha = \sum_{n=r}^{\infty} a_n \varpi_\mathfrak{p}^n = a_r \varpi_\mathfrak{p}^r + a_{r+1} \varpi_\mathfrak{p}^{r+1} + \cdots \tag{2.8}$$

form some $r \in \mathbb{Z}$. Moveover, if $a_r \neq 0$, then $\mathrm{ord}_\mathfrak{p}(\alpha) = r$.

Proof. Let $\alpha \in \mathfrak{o}_\mathfrak{p}$. Let $a_0 \in \mathscr{A}$ be the representative if the class $\alpha + \mathfrak{p}_\mathfrak{p}$ in $\mathfrak{o}_\mathfrak{p}/\mathfrak{p}_\mathfrak{p}$. We set $\alpha_1 = (\alpha - a_0)/\varpi_\mathfrak{p}$. Clearly $\alpha_1 \in \mathfrak{o}_\mathfrak{p}$ since $|\alpha_1| \leq 1$, then we could get $a_1 \in \mathscr{A}$ such that $a_1 \equiv \alpha_1 (\mathrm{mod}\mathfrak{p}_\mathfrak{p})$. Keep on this progress for k times, we could get

$$\alpha = a_0 + a_1\varpi_\mathfrak{p} + \cdots + a_{k-1}\varpi_\mathfrak{p}^{k-1} + \alpha_k\varpi_\mathfrak{p}^k$$

with $a_0, a_1, \ldots, a_{k-1} \in \mathscr{A}$ and $\alpha_k \in \mathfrak{o}_\mathfrak{p}$. From the progress we could know that the representation is unique. This completes the first part of the proof.

If $\alpha \in k_\mathfrak{p}$, let $r = \mathrm{ord}_\mathfrak{p}(\alpha) \in \mathbb{Z}$. Then $|\alpha\varpi_\mathfrak{p}^{-r}|_\mathfrak{p} = 1$, it follows that $\alpha\varpi_\mathfrak{p}^r \in U_\mathfrak{p} \subset \mathfrak{o}_\mathfrak{p}$. So we have

$$\alpha\varpi_\mathfrak{p}^{-r} = \sum_{n=0}^{\infty} a_n\varpi_\mathfrak{p}^n = a_0 + a_1\varpi_\mathfrak{p} + a_2\varpi_\mathfrak{p}^2 + \cdots$$

with $a_i \in \mathscr{A}$ and $a_0 \neq 0$. Then $\alpha \in k_\mathfrak{p}$ can be written as

$$\alpha = \sum_{n=r}^{\infty} a_{n-r}\varpi_\mathfrak{p}^n = a_0\varpi_\mathfrak{p}^r + a_1\varpi_\mathfrak{p}^{r+1} + \cdots .$$

□

Examples 2.16. *(1), Let p be a fixed prime number and $\mathbb{Q}_p$ be the local field with respect to the p-adic valuation. Then $\mathscr{A} = \{0, 1, \ldots, p-1\}$. We have the following p-adic expansions*

$$\begin{aligned} -1 &= \sum_{n=0}^{\infty}(p-1)p^n = (p-1) + (p-1)p + (p-1)p^2 + \cdots , \\ \frac{1}{1-p} &= \sum_{n=0}^{\infty} p^n = 1 + p + p^2 + \cdots . \end{aligned}$$

(2), By the series (2.8), write $\alpha = (a_r, a_{r+1}, \ldots)$. For $\mathbb{Q}_3$, we have

$$\begin{aligned} -5 &= (1,1,2,2,...) = (1,1,\overline{2},...) \\ 1/5 &= (2,0,1,2,1,0,1,2,1,...) = (2,\overline{0,1,2,1},...) \\ \sqrt{7} &= (1,1,1,0,2,...). \end{aligned}$$

Recall: Topological Groups (1), A *topological group* is a group G which is also a topological space with the property that the multiplication map and the inversion map are continuous with respect to the topology.

(2), A topological space is *locally compact* if every point has a neighborhood which is itself contained in a compact set. A *locally compact group* is a topological group

which is locally compact as a topological space. By homogeneity, local compactness for a topological group need only be checked at the identity. That is, a group G is locally compact if and only if the identity element has a compact neighborhood. Every closed subgroup of a locally compact group is locally compact. Locally compact groups are important because they have a natural measure called the *Haar measure*. This allows one to define integrals of functions on G.

(3), A topological space is said to be *disconnected* if it is the union of two disjoint nonempty open sets. Otherwise, it is said to be *connected*. The maximal connected subsets (ordered by inclusion) of a nonempty topological space are called the *connected components* of the space. A Hausdorff topological space is *totally disconnected* if the connected components are the one-point sets. Equivalently, each point has a basis for its neighborhoods which consists of sets that are both open and closed.

(4), A *profinite group* is a Hausdorff, compact, and totally disconnected topological group. Equivalently, one can define a profinite group to be a topological group that is isomorphic to the *inverse limit* of an inverse system of discrete finite groups.

For the proofs we refer the reader to [12] or [18].

Theorem 2.17. *The $\mathfrak{p}$-adic integer ring $\mathfrak{o}_\mathfrak{p}$ is the maximum compact open subring of k with respect to the $|\cdot|_\mathfrak{p}$ topology. In particular, $k_\mathfrak{p}$ is a locally compact topological field.*

Proof. Let $\{U_\lambda : \lambda \in \Lambda\}$ be any open cover of $\mathfrak{o}_\mathfrak{p}$. We must show that there is a finite subcover. We suppose not. Since

$$\mathfrak{o}_\mathfrak{p} = \bigcup_{a \in \mathscr{A}} (a + \varpi \mathfrak{o}_\mathfrak{p}),$$

there is an $a_0 \in \mathscr{A}$ such that $a_0 + \varpi\mathfrak{o}_\mathfrak{p}$ is not covered by finitely many of the U_λ. Similarly, by

$$a_0 + \varpi \mathfrak{o}_\mathfrak{p} = \bigcup_{a \in \mathscr{A}} (a_0 + a\varpi + \varpi^2 \mathfrak{o}_\mathfrak{p}),$$

there is an $a_1 \in \mathscr{A}$ such that $(a_0 + a_1\varpi + \varpi^2\mathfrak{o}_\mathfrak{p})$ is not finitely covered. And so on, one has

$$\alpha = a_0 + a_1\varpi + a_2\varpi^2 + \cdots \in \mathfrak{o}_\mathfrak{p}.$$

Then $\alpha \in U_{\lambda_0}$ for some $\lambda_0 \in \Lambda$. Since U_{λ_0} is open, there is a neighborhood

$$\alpha + \varpi^N \mathfrak{o}_\mathfrak{p} = a_0 + a_1\varpi + \cdots + a_{N-1}\varpi^{N-1} + \varpi^N \mathfrak{o}_\mathfrak{p}$$

of α such that $\alpha + \varpi^N \mathfrak{o}_\mathfrak{p} \subset U_{\lambda_0}$. This is a contradiction because we constructed α so that none of the sets $\alpha + \varpi^n \mathfrak{o}_\mathfrak{p}$, for each n, are not covered by any finite subset of the U_λ.

It R is an arbitrary compact open subring of k, we have

$$\alpha \in R \Rightarrow \alpha R \subset R \Rightarrow |\alpha|_\mathfrak{p} \leq 1 \Rightarrow \alpha \in \mathfrak{o}_\mathfrak{p},$$

whence $R \subset \mathfrak{o}_\mathfrak{p}$. Therefre $\mathfrak{o}_\mathfrak{p}$ is the maximum compact open subring of k. $\square$

▶ **Additive structure**

We extend the fractional ideal of the number field k to the local field $k_\mathfrak{p}$. A subset $\mathfrak{a}$ of $k_\mathfrak{p}$ is called a *fractional ideal* if there exists $\alpha \in k_\mathfrak{p}^\times$ such that $\alpha\mathfrak{a}$ is an ideal of $\mathfrak{o}_\mathfrak{p}$. By Proposition (2.13), $\alpha\mathfrak{a} = (\varpi_\mathfrak{p}^n) = \mathfrak{p}_\mathfrak{p}^n (n \geq 0)$. Suppose that $\alpha = \varpi_\mathfrak{p}^m u (m \in \mathbb{Z}, u \in U_\mathfrak{p})$, then

$$\mathfrak{a} = \alpha^{-1}(\varpi_\mathfrak{p}^n) = (\varpi_\mathfrak{p}^{n-m}) = \mathfrak{p}_\mathfrak{p}^{n-m}.$$

On the other hand, $\mathfrak{a} = \mathfrak{p}_\mathfrak{p}^m (m \in \mathbb{Z})$ is a fractional ideal of $k_\mathfrak{p}$, because there is $\varpi_\mathfrak{p}^{-m} \in k_\mathfrak{p}^\times$ such that $\varpi^{-m}\mathfrak{a} = \mathfrak{o}_\mathfrak{p}$. Therefore, all fractional ideals of $k_\mathfrak{p}$ are $\{\mathfrak{p}_\mathfrak{p}^n : n \in \mathbb{Z}\}$. We also have a chain of additive subgroups:

$$k \supset \cdots \supset \mathfrak{p}_\mathfrak{p}^{-2} \supset \mathfrak{p}_\mathfrak{p}^{-1} \supset \mathfrak{p}_\mathfrak{p}^0 = \mathfrak{o}_\mathfrak{p} \supset \mathfrak{p}_\mathfrak{p} \supset \mathfrak{p}_\mathfrak{p}^2 \supset \cdots \supset \{0\}.$$

It is obvious that $\{\mathfrak{p}_\mathfrak{p}^n : n \geq 1\}$ is a fundamental system of neighborhoods of the zero in $k_\mathfrak{p}$ with both open and closed sets $\mathfrak{p}_\mathfrak{p}^n$. In particular, $k_\mathfrak{p}$ is a locally compact and totally disconnected topological field.

For any $n, m \in \mathbb{Z}$, we have an isomorphism as additive groups from $\mathfrak{p}_\mathfrak{p}^n$ to $\mathfrak{p}_\mathfrak{p}^m$ via $\alpha \mapsto \alpha\varpi_\mathfrak{p}^{m-n}$. For $r \in \mathbb{N}, m \in \mathbb{Z}$, there is a surjective mapping

$$\begin{array}{rccc} \phi: & \mathfrak{o}_\mathfrak{p} & \longrightarrow & \mathfrak{p}_\mathfrak{p}^m/\mathfrak{p}_\mathfrak{p}^{m+r} \\ & \alpha & \longmapsto & \alpha\varpi_\mathfrak{p}^m, \end{array}$$

which its kernel is $\mathfrak{p}_\mathfrak{p}^r$. Then $\mathfrak{o}_\mathfrak{p}/\mathfrak{p}_\mathfrak{p}^r \cong \mathfrak{p}_\mathfrak{p}^m/\mathfrak{p}_\mathfrak{p}^{m+r}$. In particular,

$$\mathfrak{p}_\mathfrak{p}^m/\mathfrak{p}_\mathfrak{p}^{m+1} \cong \mathfrak{o}_\mathfrak{p}/\mathfrak{p}_\mathfrak{p} \cong \mathfrak{o}_k/\mathfrak{p} = \mathbb{F}_\mathfrak{p}.$$

▶ **Multiplicative structure**

For $r \geq 1$, write

$$\begin{aligned} U_\mathfrak{p}^{(r)} &= 1 + \mathfrak{p}_\mathfrak{p}^r \\ &= \{\alpha \in k_\mathfrak{p}^\times : \mathrm{ord}_\mathfrak{p}(\alpha - 1) \geq r\} \\ &= \{\alpha \in k_\mathfrak{p}^\times : |\alpha - 1|_\mathfrak{p} \leq (N\mathfrak{p})^{-r}\}. \end{aligned}$$

It is easily seen that $U_\mathfrak{p}^{(r)}$ is a multiplicative subgroup of $k_\mathfrak{p}^\times$ and is called the *r-th higher unit group.* In particular, $U^{(1)} = 1 + \mathfrak{p}_\mathfrak{p}$ is called the *group of principal units* and any element of it is called a *principal unit.* The higher unit groups provide a decreasing *filtration* of the unit group:

$$k_\mathfrak{p}^\times \supset U_\mathfrak{p} \supset U_\mathfrak{p}^{(1)} \supset U_\mathfrak{p}^{(2)} \supset \cdots \supset \{1\}.$$

We conclude similarly that $\{1+\mathfrak{p}_\mathfrak{p}^r : r \geq 1\}$ is a fundamental system of neighborhoods of 1 in $k_\mathfrak{p}^\times$. In particular, $k_\mathfrak{p}^\times$ is a locally compact and totally disconnected topological field. Denote a mapping ψ by

$$\begin{array}{rcl} U_\mathfrak{p} & \longrightarrow & (\mathfrak{o}_\mathfrak{p}/\mathfrak{p}_\mathfrak{p})^\times \\ \alpha & \longmapsto & \alpha \bmod \mathfrak{p}_\mathfrak{p}. \end{array}$$

It is a surjective homomorphism of groups, which its kernel is $U_\mathfrak{p}^{(1)}$. Hence, we actually have an exact sequence:

$$1 \to U_\mathfrak{p}^{(1)} \to U_\mathfrak{p} \to (\mathfrak{o}_\mathfrak{p}/\mathfrak{p}_\mathfrak{p})^\times \to 1.$$

Similarly, denote the mapping $\varphi : U_\mathfrak{p}^{(r)} \to \mathfrak{o}_\mathfrak{p}/\mathfrak{p}_\mathfrak{p}$ via $1+\alpha\varpi^r \mapsto \alpha \bmod \mathfrak{p}_\mathfrak{p}$, which induces the isomorphism $U_\mathfrak{p}^{(r)}/U_\mathfrak{p}^{(r+1)} \cong \mathfrak{o}_\mathfrak{p}/\mathfrak{p}_\mathfrak{p}$. Therefore, we have

$$[U_\mathfrak{p} : U_\mathfrak{p}^{(r)}] = [U_\mathfrak{p} : U_\mathfrak{p}^{(1)}] \cdots [U_\mathfrak{p}^{(r-1)} : U_\mathfrak{p}^{(r)}] = (N\mathfrak{p})^{r-1}(N\mathfrak{p}-1).$$

2.2.2 Hensel's lemma

Lemma 2.18. *(First Hensel's Lemma) Let $f(x) \in \mathfrak{o}_\mathfrak{p}[X]$ and let $\overline{f}(x)$ be the reduction of $f(x)$ modulo $\mathfrak{p}$ its coefficients. Let $\overline{f}(x) = \phi_1(x)\phi_2(x)$ where $\phi_1, \phi_2 \in \mathbb{F}_\mathfrak{p}[X]$ are coprime. Then there exist polynomials f_1 and f_2 in $\mathfrak{o}_\mathfrak{p}[X]$ such that*

$$f(x) = f_1(x)f_2(x), \text{ and } \overline{f}_1 = \phi_1, \overline{f}_2 = \phi_2.$$

Proof. We construct polynomials $f_1^{(n)}, f_2^{(n)}$ in $\mathfrak{o}_\mathfrak{p}[X]$ for $n = 1, 2, \ldots$, whose reductions mod$\mathfrak{p}$ are ϕ_1, ϕ_2 and which have the properties $\deg f_1^{(n)} = \deg\phi_1$, $\deg f_2^{(n)} \leq \deg f - \deg\phi_1$, and

$$\mathfrak{p}^n | (f - f_1^{(n)} f_2^{(n)}) \text{ and } \mathfrak{p}^n | (f_1^{(n+1)} - f_2^{(n)}) \text{ for } \nu = 1, 2.$$

Then $f_\nu = \lim f^{(n)}$ will exist and have the required properties.

For the $f_\nu^{(1)}$, we lift ϕ_ν to $\mathfrak{o}_\mathfrak{p}$ in any way. To construct the $f_\nu^{(n+1)}$ from the $f_\nu^{(n)}$, we proceed as follows. By hypothesis

$$f = f_1^{(n)} f_2^{(n)} + \pi^n h^{(n)} \text{ for same } h^{(n)} \text{ in } \mathfrak{o}_\mathfrak{p}[X] \text{ with } \deg h^{(n)} \leq \deg f.$$

If we choose $f_\nu^{(n+1)} = f_\nu^{(n)} + \pi^n g_\nu^n$ with g_ν^n in $\mathfrak{o}_\mathfrak{p}[X]$, then the second condition on the fourth line will certainly be satisfied, and the first one will be equivalent to

$$h^{(n)} \equiv f_1^{(n)} g_2^{(n)} + f_2^{(n)} g_1^{(n)} \pmod{\mathfrak{p}}$$

therefore

$$\overline{h^{(n)}} = \phi_1 \overline{g_2^{(n)}} + \phi_2 \overline{g_1^{(n)}}.$$

Since ϕ_1, ϕ_2 are coprime and $\mathbb{F}_\mathfrak{p}[X]$ is a principal ideal domain, there are polynomial ψ_1, ψ_2 in $\mathbb{F}_\mathfrak{p}[X]$ such that $\phi_1\psi_2 + \phi_2\psi_1 = \overline{h^{(n)}}$ and $\deg\psi_1 < \deg\phi_1$ and we can take $g_\nu^{(n)}$ be any lifts of ψ_ν. □

Corollary 2.19. *If $\alpha \in \mathfrak{O}_\mathfrak{P}$ then α is integral over $\mathfrak{o}_\mathfrak{p}$; in particular $\mathrm{Tr}_{K_\mathfrak{P}/k_\mathfrak{p}}\alpha$ and $\mathrm{N}_{K_\mathfrak{P}/k_\mathfrak{p}}\alpha$ are in $\mathfrak{o}_\mathfrak{p}$.*

Proof. Suppose that $\mathfrak{P}^e || \mathfrak{p}$ and choose Π in $\mathfrak{P}$ so that $\mathfrak{P} || \Pi$. Let $B_1, B_2, \ldots, B_n$ be a base for $\mathfrak{O}_\mathfrak{P}$ as an $(\mathfrak{o}/\mathfrak{p})$-vector space. The representation on privious pages implies that the $\Pi^\mu B_\nu$ with $0 \le \mu < e$ form a base for $\mathfrak{O}_\mathfrak{P}$ as an $\mathfrak{o}_\mathfrak{p}$-module. Hence $K_\mathfrak{P}$ is algebraic over $k_\mathfrak{p}$. In what follows, we use the absolute value associated with $\mathfrak{P}$, which clearly induces an absolute value on k associated with $\mathfrak{p}$. Let

$$f(X) = c_0 x^m + c_1 x^{m-1} + \cdots + c_m \quad (c_0 = 1)$$

be the minimal monic polynomial for α over $k_\mathfrak{p}$. We assume that the c_μ are not all in $\mathfrak{o}_\mathfrak{p}$ and obtain a contradiction. Let b in $\mathfrak{o}_\mathfrak{p}$ such that bc_μ are all in $\mathfrak{o}_\mathfrak{p}$ but not all divisible by $\mathfrak{p}$. If bc_m is the only one of the bc_μ not in $\mathfrak{p}$, then bc_m would have strictly larger absolute value than any of the other terms in $f(\alpha) = 0$, contradicting the ultrametric law. In any other case, we use the above lemma to lift the factorization $\overline{bf(X)} \cdot 1$ to a non-trivial factorization of $bf(X)$ over $\mathfrak{o}_\mathfrak{p}$, and f would not be minimal. □

The problem of finding good approximations to the roots may sometimes be handled on the basis of our the following result.

Lemma 2.20. *(Newton's method) Let $f(x) \in \mathfrak{o}_\mathfrak{p}[X]$ be a monic polynomial with formal derivative $f'(x)$. Assume that there exists $\alpha \in \mathfrak{o}_\mathfrak{p}$ such that $|f(\alpha)|_\mathfrak{p} < |f'(\alpha)|_\mathfrak{p}^2$. Then there uniquely exists $\beta \in \mathfrak{o}_\mathfrak{p}$ such that $f(\beta) = 0$ and*

$$|\beta - \alpha|_\mathfrak{p} \le \frac{|f(\alpha)|_\mathfrak{p}}{|f'(\alpha)|_\mathfrak{p}} < |f'(\alpha)|_\mathfrak{p}. \tag{2.9}$$

Theorem 2.21. *Every finite algebraic extension of $k_\mathfrak{p}$ lies in some $K_\mathfrak{P}$ where K is a finite algebraic extension of the number field k and $\mathfrak{P}$ is a prime ideal of K above $\mathfrak{p}$.*

2.2.3 Weak approximation theorem

In the language of valuations we can restate the Chinese remainder theorem as follows. Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$ be distinct prime ideals in $\mathfrak{o}_k$ and $\alpha_1, \ldots, \alpha_m$ any elements of $\mathfrak{o}_k$. Then for any $\epsilon > 0$ we can find $\alpha \in \mathfrak{o}_k$ such that $|\alpha - \alpha_i|_{\mathfrak{p}_i} < \epsilon$ for each i.

In this subsection we shall observe the behavior of distinct places of a field. For this purpose we shall first prove the following lemma.

Lemma 2.22. *Let $|\cdot|_1, \ldots, |\cdot|_m$ be distinct places of k. There exists an element α of k such that*

$$|\alpha|_1 > 1, |\alpha|_2 < 1, \ldots, |\alpha|_m < 1.$$

Proof. When $m = 2$, as $|\cdot|_1$ and $|\cdot|_2$ are distinct places of k, we could find $\alpha, \beta \in k$ such that $|\alpha|_1 \geq 1$, $|\alpha|_2 < 1$ and $|\beta|_1 < 1$, $|\beta|_2 \geq 1$. Let $\gamma = \alpha\beta^{-1}$. Then we have $|\gamma|_1 > 1$, $|\gamma|_2 < 1$. The lemma is right.

Suppose that when $m = t-1 (t \geq 3)$ the lemma is right. Then for $m = t$, we could find $\alpha, \beta \in k$ such that

$$|\alpha|_1 > 1, |\alpha|_j < 1, j = 2, 3, \ldots, t-1, |\beta|_1 \geq 1, |\beta|_t < 1.$$

If $|\alpha|_n \leq 1$, then set $\gamma = \alpha^r \beta$, with r large enough we could get

$$|\gamma|_1 > 1, |\gamma|_j < 1, j = 2, 3, \ldots, t;$$

if $|\alpha|_n > 1$, then set $\gamma = \alpha^r \beta/(1 + \alpha^r)$, with r large enough we could get the same result. □

Theorem 2.23. *Let $|\cdot|_1, \ldots, |\cdot|_m$ be distinct places of k and $\alpha_1, \ldots, \alpha_m$ any elements of k. For any $\epsilon > 0$, we can find α in k such that*

$$|\alpha - \alpha_i|_i < \epsilon$$

for each i.

Proof. Thus by the lemma we could find $\beta_l \in k, 1 \leq l \leq m$ such that $|\beta_l|_l > 1$ and $|\beta_l|_j < 1 (l \neq j)$. Then let

$$\alpha = \sum_{i=1}^{m} \frac{\alpha_i \beta_i^r}{1 + \beta_i^r},$$

we could have that

$$\begin{aligned} |\alpha - \alpha_i|_i &\leq \frac{|\alpha|_i}{|1 + \beta_i^r|_i} + \sum_{j=1, j\neq i}^{m} \frac{|\alpha|_i |\beta_i^r|_i}{|1 + \beta_i^r|_{v_i}} \\ &\leq \frac{|\alpha|_i}{|\beta_i|_i^r - 1} + \sum_{j=1, j\neq i}^{m} \frac{|\alpha|_i |\beta_i|_i^r}{1 - |\beta_i|_i^r}. \end{aligned}$$

Then when $r \to \infty$, we have $|\alpha - \alpha_i|_i \to 0$ for each i. Thus for all $\epsilon > 0$, with r large enough, we obtion

$$|\alpha - \alpha_i|_i < \epsilon$$

for each i. □

The week approximation theorem asserts that inequivalent valuations are in fact almost totally independence. Let us now state two corollaries of week approximation theorem.

Corollary 2.24. *(Independence Theorem) Let $|\cdot|_1, \ldots, |\cdot|_m$ be distinct places of k. Then for $1 \leq r \leq m$ there exists $\alpha \in k$ such that*

$$|\alpha|_1 > 1, \ldots, |\alpha|_r > 1, |\alpha|_{r+1} < 1, \ldots, |\alpha|_m < 1.$$

Corollary 2.25. *Let $|\cdot|_1, \ldots, |\cdot|_m$ be distinct places of k. If*

$$|\alpha|_1^{r_1} \cdots |\alpha|_m^{r_m} = 1,$$

for all $\alpha \in k^\times$, where r_i are real constants, then $r_1 = \cdots = r_m = 0$.

2.3 Extensions of Valuations

Let k be a field with valuation $|\cdot|$ and let V be a vector space over k. A real valued functions $\|\cdot\|$ on V is called a norm if

- $\|v\| > 0$ for all nonzero $v \in V$ (positivity);
- $\|v + w\| \leq \|v\| + \|w\|$ for all $v, w \in V$ (triangle inequality);
- $\|\alpha v\| = |\alpha|\|v\|$ for all $\alpha \in k$ and $v \in V$ (homogeneity).

Two norms $\|\cdot\|_1$ and $\|\cdot\|_2$ on the same space V are *equivalent* if there exist positive real numbers c_1 and c_2 such that for all $v \in V$,

$$c_1\|\cdot\|_1 \leq \|\cdot\|_2 \leq c_2\|\cdot\|_1.$$

This is clearly an equivalence relation.

Lemma 2.26. *Suppose that k is complete with respect to $|\cdot|$ and that V is an n-dimensional normed vector space over k. Then any two norms on V are equivalent. Let $\{v_1, \ldots, v_n\}$ be a basis of V over k. In particular, V is complete with respect to a norm and the vector space homomorphism*

$$\begin{array}{rcl} \phi: \ k^n & \longrightarrow & V \\ (\alpha_1, \ldots, \alpha_n) & \longmapsto & \displaystyle\sum_{i=1}^{n} \alpha_i v_i \end{array}$$

is a homeomorphism.

Proof. The proof of the lemma is similar to the case for $k = \mathbb{R}$. The details are left to the reader. See any good *Functional Analysis* textbook. □

2.3.1 Extensions of valuations

Suppose $K \supset k$ is a finite extension of fields, and that $|\cdot|$ and $\|\cdot\|$ are valuations on k and K, respectively. We say that $\|\cdot\|$ *extends* $|\cdot|$ if $\|\alpha\| = |\alpha|$ for all $\alpha \in k$.

Theorem 2.27. *Suppose that k is a field that is complete with respect to the nonarchimedean valuation $|\cdot|$ and that K is a finite extension $\|\cdot\|$ of k of degree $n = [K : k]$. Then there is precisely one extension of $|\cdot|$ to K, namely*

$$\|\alpha\| = |N_{K/k}(\alpha)|^{\frac{1}{n}}. \tag{2.10}$$

Proof. Let us first prove that the existence of the extended valuation. Define $\|\cdot\|$ on K by

$$\|\alpha\| = |N_{K/k}(\alpha)|^{\frac{1}{n}}$$

for $\alpha \in K$. Clearly, it satisfies the conditions *(1)* and *(2)* in the definition of valuation. It remains to show that $\|\alpha+\beta\| \leq \max(\|\alpha\|, \|\beta\|)$ for all $\alpha, \beta \in K$. By the exercise, it suffices to show that if $\alpha \in K$ is such that $|N_{K/k}(\alpha)| \leq 1$, then

$$|N_{K/k}(1+\alpha)| \leq 1.$$

Consider the irreducible polynomial

$$f(x) = x^m + a_{m-1}x^{m-1} + \cdots + a_0$$

of α over k. By the Viete's theorem and the proposition (1.3), we have

$$(-1)^n (a_0)^{n/m} = N_{K/k}(\alpha)$$

and then $|a_0| \leq 1$. In other words, $a_0 \in \mathfrak{o}_k = \{\alpha \in k : |\alpha| \leq 1\}$. Since

$$\begin{aligned} f(-1) &= (-1)^m N_{k(\alpha)/k}(1+\alpha) \\ &= (-1)^m + (-1)^{m-1}a_{m-1} + \cdots + a_0, \end{aligned}$$

if we can show that all coefficients $a_i \in \mathfrak{o}_k$, then so does $N_{k(\alpha)/k}(1+\alpha)$ and hence $N_{K/k}(1+\alpha)$, implying that $|N_{K/k}(1+\alpha)| \leq 1$. Indeed, we have the following lemma. See exercise.

Claim: *Let the polynomial* $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in k_{\mathfrak{p}}[X]$ *be irreducible. Then*

$$\max\{|a_i|_{\mathfrak{p}} : 0 \leq i \leq n\} = \max\{|a_0|_{\mathfrak{p}}, |a_n|_{\mathfrak{p}}\}.$$

It remains to prove that the uniqueness of the extended valuation. View K as an n-dimensional vector space over k. Any valuation $\|\cdot\|$ on K extending $|\cdot|$ defines a norm on K satisfying $\|\alpha x\| = |\alpha|\|x\|$ for $\alpha \in k$ and $x \in K$. By Lemma (2.26), any two valuations on K extending $|\cdot|$ are equivalent. It follows that the uniqueness of the extended valuation $\|\cdot\|$. □

Corollary 2.28. *Let k be a complete field with a nonarchimedean valuation $|\cdot|$ and K/k be a Galois extension with the Galois group G. Let $\|\cdot\|$ be a valuation of K. Then, for any $\alpha \in K$ and $\sigma \in G$, we have $\|\sigma\alpha\| = \|\alpha\|$.*

Proof. It is clear that $N(\sigma\alpha) = N(\alpha)$ for any $\alpha \in K$ and $\sigma \in G$. Hence we have $\|\sigma\alpha\| = \|\alpha\|$ follows from Theorem (2.27). □

From now on, we only consider the case of number fields. Let K/k be an extension of algebraic number fields with $[K:k]=n$. Let $\mathfrak{p}$ be a prime ideal of $\mathfrak{o}_k$ with the decomposition

$$\mathfrak{p}\mathfrak{O}_K = \mathfrak{P}_1^{e_1}\cdots\mathfrak{P}_g^{e_g}, \tag{2.11}$$

for some prime ideals $\mathfrak{P}_1,\ldots,\mathfrak{P}_g$ in $\mathfrak{O}_K$. Let $k_\mathfrak{p}$ and $K_{\mathfrak{P}_i}$ be the local fields at the prime ideals $\mathfrak{p}$ and $\mathfrak{P}_i$, respectively. Let w and v be the places of K and k corresponding to $\mathfrak{P}$ and $\mathfrak{p}$, so that w lies above v, say $w|v$. Let π and Π be uniformizers at $\mathfrak{p}$ and $\mathfrak{P}$, respectively. Let the nations

$$K_w = K_\mathfrak{P}, \mathfrak{O}_K, \mathfrak{O}_\mathfrak{P}, \mathfrak{P}_\mathfrak{P}, \mathbb{F}_w = \mathfrak{O}_\mathfrak{P}/\mathfrak{P}_\mathfrak{P} \cong \mathfrak{O}_K/\mathfrak{P} = \mathbb{F}_\mathfrak{P}, U_\mathfrak{P}, \Pi$$

and

$$k_v = k_\mathfrak{p}, \mathfrak{o}_k, \mathfrak{o}_\mathfrak{p}, \mathfrak{p}_\mathfrak{p}, \mathbb{F}_v = \mathfrak{o}_\mathfrak{p}/\mathfrak{p}_\mathfrak{p} \cong \mathfrak{o}_k/\mathfrak{p} = \mathbb{F}_\mathfrak{p}, U_\mathfrak{p}, \pi$$

be as above. For fixed $\mathfrak{P}|\mathfrak{p}$, set $e(\mathfrak{P}/\mathfrak{p})=e$ and $f(\mathfrak{P}/\mathfrak{p})=f$.

Lemma 2.29. *For any $\alpha\in k_\mathfrak{p}$, we have*

$$\mathrm{ord}_\mathfrak{P}(\alpha) = e\mathrm{ord}_\mathfrak{p}(\alpha), \quad \textit{and} \ |\alpha|_\mathfrak{P} = |\alpha|_\mathfrak{p}^{ef}.$$

Proof. According to $\pi\in\mathfrak{p}\setminus\mathfrak{p}^2$ and $\Pi\in\mathfrak{P}\setminus\mathfrak{P}^2$, thus $\pi\mathfrak{o}_k=\mathfrak{p}\mathfrak{a}$ where $\mathfrak{a}$ is an ideal coprime to $\mathfrak{p}$. If we lift π in $\mathfrak{O}_K$, we get

$$\pi\mathfrak{O}_K = \mathfrak{p}\mathfrak{a}\mathfrak{O}_K = \mathfrak{a}\mathfrak{O}_K\prod_{\mathfrak{P}|\mathfrak{p}}\mathfrak{P}^e,$$

where $\mathfrak{a}\mathfrak{O}_K$ is coprime to the $\mathfrak{P}$. Now $\mathrm{ord}_\mathfrak{P}(\pi)=e$, thus we see immediately that $\pi=u\Pi^e$, where $u\in U_\mathfrak{P}$. For any $\alpha\in k_\mathfrak{p}$, we have

$$v\Pi^{\mathrm{ord}_\mathfrak{P}(\alpha)} = \alpha = w\pi^{\mathrm{ord}_\mathfrak{p}(\alpha)} = uw\Pi^{e\mathrm{ord}_\mathfrak{p}(\alpha)},$$

where $v\in U_\mathfrak{P}$ and $w\in u_\mathfrak{p}$. Taking the valuation $|\cdot|_\mathfrak{P}$ to both sides of the last equation, we complete the proof of the lemma. □

Proposition 2.30. *With the nations above,*

$$[K_\mathfrak{P}:k_\mathfrak{p}] = ef. \tag{2.12}$$

Proof. Let $\mathscr{A}$ be any set of representatives of the residue class field $\mathfrak{O}_\mathfrak{P}/\mathfrak{P}_\mathfrak{P}$ in $\mathfrak{O}_\mathfrak{P}$. We know that for any $\alpha\in K_\mathfrak{P}$,

$$\alpha = \sum_{i=m}^{\infty} a_i\Pi^i, \quad \text{where } a_i\in\mathscr{A} \text{ and } m\in\mathbb{Z}$$

and $\Pi^i = u_j\Pi^t\pi^s, u_j \in U_{\mathfrak{P}}$ where $1 \le t \le e-1$. Obviously we have that $a_iu_j \in \mathscr{A}$. Hence we have that $\alpha = \sum_{i=0}^{e-1}\sum_{m>-\infty} s_{im}\Pi^i\pi^m$ such that $s_{im} \in \mathscr{A}$. Let S be a set of representatives of the residue field $\mathfrak{o}_{\mathfrak{p}}/\mathfrak{p}$ in $\mathfrak{o}_{\mathfrak{p}}$ and let $w_1, \ldots, w_f$ be elements in $\mathfrak{O}_{\mathfrak{P}}$ such that modulo $\mathfrak{P}$ they form a basis over $\mathfrak{o}_{\mathfrak{p}}/\mathfrak{p}$. Then we choose $\mathscr{A} = \{\sum_{j=1}^{f} s_jw_j : s_j \in S\}$. This shows that $w_j\Pi^i, 1 \le j \le f, 0 \le i \le e-1$, generate $K_{\mathfrak{P}}$ over $k_{\mathfrak{p}}$.

It remains to show that $w_j\Pi^i, 1 \le j \le f, 0 \le i \le e-1$ are linearly independent over $k_{\mathfrak{p}}$. Suppose otherwise. Let $\sum_{i,j} a_{ij}w_j\Pi^i = 0$ be a non-trivial linear relation over $k_{\mathfrak{p}}$, where $1 \le j \le f, 0 \le i \le e-1$. We may assume that all a_{ij} are in $\mathfrak{O}_{\mathfrak{P}}$ and some a_{ij} is a unit. Let i_0 be the smallest index m such that a_{mj} is a unit for some j. Then $a_{ij} \in \mathfrak{p}$ for $i < i_0$ and all j so that $\sum_{i\neq i_0,j} a_{ij}w_j\Pi^i \in \mathfrak{P}^{i_0+1}$. Consequently, $\sum_{1\le j\le f} a_{i_0j}w_j\Pi^i \in \mathfrak{P}^{i_0+1}$, which implies that $\sum_{1\le j\le f} a_{i_0j}w_j \in \mathfrak{P}$, or equivalently, modulo $\mathfrak{P}$, $\sum_{1\le j\le f} \overline{a_{i_0j}w_j} = \overline{0}$ in $\mathfrak{O}_{\mathfrak{P}}/\mathfrak{P}$. That's in contradict with the linear independency of $\{\overline{w_j}\}$ over $\mathfrak{o}_{\mathfrak{p}}/\mathfrak{p}$. Therefore $w_j\Pi^i, 1 \le j \le f, 0 \le i \le e-1$, form a basis of $K_{\mathfrak{P}}$ over $k_{\mathfrak{p}}$. □

Corollary 2.31. *With the nations above. Then*

$$\mathfrak{O}_{\mathfrak{P}} = \oplus_{\substack{1\le i\le f\\ 0\le j\le e-1}} \omega_i\Pi^j\mathfrak{o}_{\mathfrak{p}},$$

that is, the set $\{\omega_i\Pi^j : 1 \le i \le f, 0 \le j \le e-1\}$ *constitutes a basis of the ring* $\mathfrak{O}_{\mathfrak{P}}$ *over the ring* $\mathfrak{o}_{\mathfrak{p}}$.

Proof. Since the set $\{\omega_i\Pi^j : 1 \le i \le f, 0 \le j \le e-1\}$ constitutes a basis of $K_{\mathfrak{P}}$ over $k_{\mathfrak{p}}$, it suffices to show that for given elements $c_{ij} \in k_{\mathfrak{p}}$, if the sum $\sum c_{ij}\omega^i\Pi^j$ is contained in the ring $\mathfrak{O}_{\mathfrak{P}}$, then all c_{ij} are elements of the ring $\mathfrak{o}_{\mathfrak{p}}$. Firstly, we claim that

- Let $\alpha = a_1\omega_1 + \cdots + a_f\omega_f$ with any $a_i \in k_{\mathfrak{p}}$. Then

$$\mathrm{ord}_{\mathfrak{P}}(\alpha) = \min\{\mathrm{ord}_{\mathfrak{P}}(a_i) : 1 \le i \le f\}.$$

Proof. Without loss of generality, we assume that not all a_i are zero and $\mathrm{ord}_{\mathfrak{P}}(a_1) = \min\{\mathrm{ord}_{\mathfrak{P}}(a_i) : 1 \le i \le f\}$. It gives that $a_i/a_1 \in \mathfrak{o}_{\mathfrak{p}}$ and

$$\alpha = a_1\{\omega_1 + \cdots + (a_f/a_i)\omega_f\} = a_1\beta.$$

By the choice of $\{\omega_i\}$, we obtain $\overline{\beta} \neq \overline{0}$, so $\mathrm{ord}_{\mathfrak{P}}(\beta) = 0$, and then $\mathrm{ord}_{\mathfrak{P}}(\alpha) = \mathrm{ord}_{\mathfrak{P}}(a_1\beta) = \mathrm{ord}_{\mathfrak{P}}(a_1)$.

We can now turn to prove the corollary. For $1 \le i \le f, 0 \le j \le e-1$,

$$\begin{aligned}\sum c_{ij}\omega^i\Pi^j \in \mathfrak{O}_\mathfrak{P} &\Rightarrow \operatorname{ord}_\mathfrak{P}(\sum c_{ij}\omega^i\Pi^j) \ge 0\\ &\Rightarrow \operatorname{ord}_\mathfrak{P}(c_{ij}\Pi^j) \ge 0\\ &\Rightarrow \operatorname{ord}_\mathfrak{P}(c_{ij}) \ge -j\\ &\Rightarrow \operatorname{ord}_\mathfrak{p}(c_{ij}) \ge 0\\ &\Rightarrow c_{ij} \in \mathfrak{o}_\mathfrak{p}.\end{aligned}$$

□

Corollary 2.32. *There exists $\alpha \in \mathfrak{O}_\mathfrak{P}$ such that $\mathfrak{O}_\mathfrak{P} = \mathfrak{o}_\mathfrak{p}[\alpha]$ and $K_\mathfrak{P} = k_\mathfrak{p}(\alpha)$. In particular, $\mathfrak{O}_\mathfrak{P}$ is a free $\mathfrak{o}_\mathfrak{p}$-module of rank ef.*

Proof. Take $\alpha \in \mathfrak{O}_K$ such that the residue class $\bar{\alpha}$ generates $\mathbb{F}_w$, i.e., $\mathbb{F}_w = \mathbb{F}_v(\bar{\alpha})$. Let $f(x)$ be a polynomial in $\mathfrak{o}_\mathfrak{p}[X]$ such that $\bar{f}(x)$ is an irreducible polynomial with $\bar{f}(\bar{\alpha}) = 0$. Then we have $\operatorname{ord}_\mathfrak{P} f(\alpha) \ge 1$, and $\operatorname{ord}_\mathfrak{P} f'(\alpha) = 0$. We may assume that $\operatorname{ord}_\mathfrak{P} f(\alpha) = 1$. In fact, if $\operatorname{ord}_\mathfrak{P} f(\alpha) > 1$, we may replace α by $\beta = \alpha + \Pi$. By

$$f(\beta) = f(\alpha + \Pi) \equiv f(\alpha) + \Pi f'(\alpha) \mod \mathfrak{P}_\mathfrak{P}^2,$$

we get $\operatorname{ord}_\mathfrak{P} f(\beta) = 1$. We may therefore assume that $f(\alpha)$ is prime element of $K_\mathfrak{P}$. Hence, by Corollary (2.31), the set $\{\alpha^i f(\alpha)^j \,:\, 0 \le i \le f-1, 0 \le j \le e-1\}$ constitutes an $\mathfrak{o}_\mathfrak{p}$-base of $\mathfrak{O}_\mathfrak{P}$, and therefore the set $\{1, \alpha, \ldots, \alpha^{ef-1}\}$ constitutes an $\mathfrak{o}_\mathfrak{p}$-base of $\mathfrak{O}_\mathfrak{P}$. □

Let K/k be an extension of any field of finite degree $[K : k] = n$. Let $\omega_1, \ldots, \omega_n$ be a basis of K over k. Then

$$\omega_i\omega_j = \sum_{k=1}^{n} a_{ijk}\omega_k, \quad \textit{with} \;\; a_{ijk} \in k,$$

and this relation determines K up to isomorphism. Let A be a ring containing k. The tensor product denote by

$$K \otimes_k A = \left\{ \sum_{i=1}^{n} c_i(1 \otimes \omega_i) \,:\, c_i \in A \right\}. \tag{2.13}$$

Algebraically, it is a ring with the componentwise addition and with multiplication table given by (2.13). Note that both A and K are imbedded in

$K \otimes_k A$. If there is a topology on A, then we put on $K \otimes_k A$ the topology coming from the product topology on A^n via the isomorphism

$$\begin{aligned} A^n &\longrightarrow K \otimes_k A \\ (c_1, \ldots, c_n) &\longmapsto \sum_{i=1}^{n} c_i (1 \otimes \omega_i). \end{aligned}$$

One checks easily that both algebraic and topological structure on $K \otimes_k A$ are independent of the choice of a basis $\{\omega_1, \ldots, \omega_n\}$ of K over k. Clearly, we have $[K \otimes_k A : A] = [K : k]$.

Theorem 2.33. *Let $K = k(\alpha)$ be an algebraic number field with $[K : k] = n$ and $\alpha \in \mathfrak{O}_K$, and let $f(x)$ be the minimal polynomial of α over k. Let $f(x) = \prod_{i=1}^{h} f_i(x)$ where the $f_i(x)$ are irreducible and distinct in $k_\mathfrak{p}[X]$. Then $h = g$. After renumbering,* $\deg f_i(x) = e_i f_i$ *and $K_{\mathfrak{P}_i} \cong k_\mathfrak{p}[X]/(f_i(x))$. There is a natural isomorphism*

$$K \otimes_k k_\mathfrak{p} \cong K_{\mathfrak{P}_1} \oplus \cdots \oplus K_{\mathfrak{P}_g} \tag{2.14}$$

both algebraically and topologically.

Proof. By assumption, we have an isomorphism $K = k(\alpha) \cong k[X]/(f(x))$. Hence

$$K \otimes_k k_\mathfrak{p} \cong (k[X]/(f(x))) \otimes_k k_\mathfrak{p} \cong k_\mathfrak{p}[X]/(f(x)).$$

Because K/k is separable, the minimal polynomial $f(x)$ has distinct roots. Therefore $f(x)$ factors in $k_\mathfrak{p}[X]$ into monic irreducible polynomials

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

that are relatively prime in pairs. Algebraically, we have, by the Chinese reminder theorem,

$$k_\mathfrak{p}[x]/(f(x)) \cong \prod_{i=1}^{r} k_\mathfrak{p}[x]/(f_i(x)).$$

Here each $k_\mathfrak{p}[x]/(f_i(x))$ is a finite field extension of $k_\mathfrak{p}$ of degree $\deg f_i$, say K_i. As k is dense in $k_\mathfrak{p}$, $K = K \otimes_k k$ is dense in $K \otimes_k k_\mathfrak{p}$, hence K is dense in each K_i. So $|\cdot|_i$ restricts to K corresponds to a place $\mathfrak{P}_i$ of K. By Theorem (2.21), we have $K_i = K_{\mathfrak{P}_i}$ for some prime ideal $\mathfrak{P}_i$ lying above $\mathfrak{p}$. According to

$$[K \otimes_k k_\mathfrak{p} : k_\mathfrak{p}] = [K : k] = \sum_{i=1}^{g} e_i f_i = \sum_{i=1}^{g} [K_{\mathfrak{P}_i} : k_\mathfrak{p}],$$

the theorem follows. □

Corollary 2.34. *For any element $\alpha \in K$,*

$$\begin{aligned} \mathrm{Tr}_{K/k}\alpha &= \sum_{i=1}^{g} \mathrm{Tr}_{K_{\mathfrak{P}_i}/k_{\mathfrak{p}}}\alpha, \\ \mathrm{N}_{K/k}\alpha &= \prod_{i=1}^{g} \mathrm{N}_{K_{\mathfrak{P}_i}/k_{\mathfrak{p}}}\alpha \end{aligned}$$

Proof. As shown in the above proof, we have $\sum_{i=1}^{g}[K_{\mathfrak{P}_i}/k_{\mathfrak{p}}] = n = [K:k]$, hence Corollary holds for $\alpha \in k$. Next assume $K = k(\alpha)$. Let $f(x)$ and $f_i(x)$ be as in the proof above; we have $\mathrm{N}_{K/k}(\alpha) = (-1)^n f(0)$ and $\mathrm{N}_{K_{\mathfrak{P}_i}/k_{\mathfrak{p}}}(\alpha) = (-1)^{[K_{\mathfrak{P}_i}:k_{\mathfrak{p}}]} f_i(0)$, and $\mathrm{Tr}_{K/k}(\alpha) = -$coefficient of x^{n-1} in f and $\mathrm{Tr}_{K_{\mathfrak{P}_i}/k_{\mathfrak{p}}}(\alpha) = -$coefficient of $x^{[K_{\mathfrak{P}_i}:k_{\mathfrak{p}}]-1}$ in $f_i(x)$. As $f(x) = f_1(x)\cdots f_g(x)$, the global norm and trace of α are related to local norm and trace of α as stated. Finally, for any element $\alpha \in K$, suppose $M = k(\alpha)$ is an intermediate field. Let $\mathcal{P}_1, \cdots, \mathcal{P}_s$ be the prime ideals of M dividing $\mathfrak{p}$. Then $\mathfrak{P}_1, \cdots, \mathfrak{P}_g$ are the prime ideals of K dividing one of $\mathcal{P}_1, \cdots, \mathcal{P}_s$. Fix an prime ideal $\mathcal{P}_i$ of M. We have

$$\begin{aligned} \prod_{\mathfrak{P}_j|\mathcal{P}_i} \mathrm{N}_{K_{\mathfrak{P}_j}/k_{\mathfrak{p}}}(\alpha) &= \prod_{\mathfrak{P}_j|\mathcal{P}_i} \mathrm{N}_{M_{\mathcal{P}_i}/k_{\mathfrak{p}}} \circ \mathrm{N}_{K_{\mathfrak{P}_j}/M_{\mathcal{P}_i}}(\alpha) \\ &= \mathrm{N}_{M_{\mathcal{P}_i}/k_{\mathfrak{p}}}(\alpha)^{\sum_{\mathfrak{P}_j/\mathcal{P}_i}[K_{\mathfrak{P}_j}:M_{\mathcal{P}_i}]} \\ &= \mathrm{N}_{M_{\mathcal{P}_i}/k_{\mathfrak{p}}}(\alpha)^{[K:M]}. \end{aligned}$$

Therefore

$$\begin{aligned} \prod_{\mathfrak{P}_j} \mathrm{N}_{K_{\mathfrak{P}_j}/k_{\mathfrak{p}}}(\alpha) &= \prod_{\mathcal{P}_i|\mathfrak{p}} \prod_{\mathfrak{P}_j|\mathcal{P}_i} \mathrm{N}_{K_{\mathfrak{P}_j}/k_{\mathfrak{p}}}(\alpha) = \prod_{\mathcal{P}_i} \mathrm{N}_{M_{\mathcal{P}_i}/k_{\mathfrak{p}}}(\alpha)^{[K:M]} \\ &= \mathrm{N}_{M/k}(\alpha)^{[K:M]} = \mathrm{N}_{K/k}(\alpha). \end{aligned}$$

Similar proof shows $\mathrm{Tr}_{K/k}(\alpha) = \sum_{i=1}^{g} \mathrm{Tr}_{K_{\mathfrak{P}_i}/k_{\mathfrak{p}}}(\alpha)$. □

2.3.2 Unramified and ramified extensions

In the subsection, let E/F be an extension of nonarchimedean local fields of an algebraic number field k with respect to prime ideals $\mathfrak{P}|\mathfrak{p}$. Let $e = e(\mathfrak{P}/\mathfrak{p})$ and $f = f(\mathfrak{P}/\mathfrak{p})$ be the ramification index and the residue class fields degree, respectively, which implies that $[E:F] = n = ef$. Let p be the characteristic of the finite field $\bar{F}$. The extension E/F of local fields is called *unramified extension* if $e = 1$ and *totally ramified extension* if $f = 1$. The finite extension E/F is said to *tamely ramified* and *wildly ramified* if

$p \nmid e$ and $p|e$, respectively. By the above definitions, we obtain an unramified extension is tamely ramified and E/F is both totally and tamely ramified if and only if $p \nmid e = [E : F]$.

Let $\mathfrak{O}_F, \mathfrak{P}_F, U_F, \bar{F}, \pi_F$ denote respectively the $\mathfrak{p}$-adic integers ring, the maximal prime ideal, the unit group, the residue class field and the uniformizer of F. For a finite extension E of F, then $\mathfrak{O}_E, \mathfrak{P}_E, U_E, \bar{E}, \pi_E$ will be above with respect to E.

Unramified Extensions:

Theorem 2.35. *(1), Suppose that the extension E/F is unramified and $\bar{E} = \bar{F}(\bar{\alpha})$ where $\alpha \in \mathfrak{O}_F$. Then $E = F(\alpha)$ and $\tilde{f}(x) = f(x) \mod \mathfrak{P}_F$ is the minimal polynomial of $\bar{\alpha}$ over $\bar{F}$ where $f(x)$ is the minimal polynomial of α over F.*

(2), Suppose $f(x) \in \mathfrak{O}_F[X]$ is a monic polynomial such that $\tilde{f}(x)$ is irreducible and separable. If α is root of $f(x)$ then $E = F(\alpha)$ is unramified.

Proof. (1) As we have that $\alpha \in \mathfrak{O}_F$, hence $f(x)$ is monic and $\deg\tilde{f}(x) = \deg f(x)$, $\tilde{f}(\bar{\alpha}) = 0$. Hence we have that

$$\begin{aligned} \deg\tilde{f} &\geq [\bar{F}(\bar{\alpha}) : \bar{F}] = [\bar{E} : \bar{F}] = [E : F], \\ \deg f &= [F(\alpha) : F] \leq [E : F] \end{aligned}$$

As $\deg\tilde{f}(x) = \deg f(x)$, hence the inequality signs can be turned into equal ones. Hence we have $E = F(\alpha)$ and $\tilde{f}(x)$ is the minimal polynomial of $\bar{\alpha}$ over $\bar{F}$.

(2) As $f(x)$ is monic, we have that $\deg\tilde{f}(x) = \deg f(x)$. We also have that $\tilde{f}(\bar{\alpha}) = 0$. Hence we have that

$$\begin{aligned} \deg f &= [F(\alpha) : F] = [E : F] \\ \deg\tilde{f} &= [\bar{F}(\bar{\alpha}) : \bar{F}] \leq [\bar{E} : \bar{F}] \leq [E : F] \end{aligned}$$

Hence we have $[\bar{E} : \bar{F}] = [E : F]$, $E = F(\alpha)$ is unramified. □

Theorem 2.36. *Let E/F be an extension of nonarchimedean local fields. Then there is a unique local field K with $F \subset K \subset F$ such that E/K is totally ramified with $[E : K] = e$ and K/F is unramified with $[K : F] = f$.*

Proof. Let $e = e(E/F)$, $f = f(E/F)$. Then we can let κ^f be the number of elements in the residue of E. By Hensel's lemma, the $(\kappa^f - 1)$-th roots of unity are in E. Let $K = F(\zeta)$ where ζ is a primitive $(\kappa^f - 1)$-th root of unity. Let g be the monic minimal polynomial of ζ over F. By the corollary of Hensel's lemma, g is over $\mathfrak{O}_F$. Since $g(x)|(x^{\kappa^f} - x)$, one has that g is

prime to g' over the residue field of F. Therefore g is also irreducible over the residue field of F by Hensel's lemma and $[K:F] = \deg(g) = f$.

It is clear that any element in K can be written as $\frac{x}{b}$ where $x \in \mathfrak{O}_F[\zeta]$ and $b \in \mathfrak{O}_F$. Furthermore there are $a_{ij} \in \mathfrak{O}_F^\times$ or $a_{ij} = 0$ such that

$$x = \sum_{i=0}^{n} \left(\sum_{j=0}^{f-1} a_{ij} \zeta^j \right) \pi_F^i.$$

It is clear that

$$\sum_{j=0}^{f-1} a_{ij} \zeta^j = 0 \ \text{ or } \ \mathrm{ord}_p \left(\sum_{j=1}^{f-1} a_{ij} \zeta^j = 0 \right),$$

since $\{1, \zeta, \cdots, \zeta^{f-1}\}$ are linearly independent over the residue field of F. Let i_0 be the smallest integer such that $a_{i_0 j} \neq 0$ for some $0 \leq j \leq (f-1)$. Then

$$\mathrm{ord}_p(x) = \mathrm{ord}_p(\pi_F^{i_0}).$$

This implies that $\mathrm{ord}_p(K^\times) = \mathrm{ord}_p(F^\times)$ and K/F is unramified.

Since the residue of K is the same as the residue field of E, E/K is totally ramified. Let π_E be a uniformizer of E. Then

$$\pi_E^e = a_0 \pi_F \ \text{ with } \ a_0 \in \mathfrak{O}_E^\times,$$

and

$$a_0 = b_0^{(0)} + b_1^{(0)} \pi_E + \cdots + b_{e-1}^{(0)} \pi_E^{e-1} + a_1 \pi_F$$

where $b_0^{(0)} \in \mathfrak{O}_K^\times$ and $b_1^{(0)}, \cdots, b_{e-1}^{(0)} \in \mathfrak{O}_K$ and $a_1 \in \mathfrak{O}_E$. Consider

$$a_1 = b_0^{(1)} + b_1^{(1)} \pi_E + \cdots + b_{e-1}^{(1)} \pi_E^{e-1} + a_2 \pi_F$$

where $b_1^{(1)}, \cdots, b_{e-1}^{(1)} \in \mathfrak{O}_K$ and $a_2 \in \mathfrak{O}_E$.

. . . . . .

Let

$$c_i = \sum_{j=0}^{\infty} b_i^{(j)} \pi_F^j \in \mathfrak{O}_K \text{ for } 1 \leq i \leq (e-1).$$

Then $c_0 \in \mathfrak{O}_K^\times$ and π_E satisfies the following Eisenstein polynomial over $\mathfrak{O}_K$

$$h(x) = x^e - c_{e-1} \pi_F x^{e-1} - \cdots - c_1 \pi_F x - c_0 \pi_F.$$

One also has that $\mathfrak{O}_E^\times \subseteq \mathfrak{O}_K[\pi_E]$ by the above argument. Therefore

$$E = K(\pi_E) \text{ and } [E:K] = \deg(h) = e.$$

Now we show the uniqueness of K. Suppose there is another intermediate field K' satisfying the conditions of this proposition. It is clear that $K' \supseteq K$ by our construction. Then K'/K is both unramified and totally ramified. Therefore $K = K'$. □

Theorem 2.37. *Let $\bar{L}$ be a finite extension of the residue field $\bar{F}$. Then there exists a unique unramified extension L/F with the residue field $\bar{L}$. Such a field L is Galois over F, and the Galois group of L/K is isomorphic to the Galois groups of $\bar{L}/\bar{F}$.*

Proof. Let a be a generator of $\bar{L}/\bar{F}$ with a minimal polynomial $f(x)$ over $\bar{F}$. Choose a monic polynomial $E(x)$ over F such that

$$E(x)(\text{mod } \mathfrak{p}) = f(x)$$

and put $L = F(b)$, where b is any root of $E(x)$, taken as usual from a fixed algebraic closure of Q_p, we obtain

$$[L : F] = \text{deg}b \text{ over } K \leq \text{deg}E = \text{deg}f = [\bar{L} : \bar{F}] \leq [\bar{L}_L : \bar{F}] \leq [L : F]$$

because the image of b in $\bar{L}_L$ is a root of $f(x)$, and so $\bar{L}$ is contained in $\bar{L}_L$. The resulting chain of inequalities shows that $[\bar{L}_L : \bar{F}] = [L : F]$; thus L/F is unramified and $[\bar{L} : \bar{F}] = [\bar{L}_L : \bar{F}]$; hence $\bar{L} = \bar{L}_L$. Thus L/F satisfies our first assertion. It remains to prove its uniqueness and normality. Let L_1 be another field, unramified over K and with $\bar{L}_{L_1} = \bar{L}$. By Hensel's lemma the polynomial $E(x)$ has a root b_1 in L_1 and we have

$$F(b_1) \cong F(b) = L,$$

but

$$[F(b_1) : F] = [\bar{L} : \bar{F}] = [L_1 : F];$$

thus $L_1 = F(b_1)$ and L_1 is indeed isomorphic to L.

Now let's turn to the normality. The extension $\bar{L}/\bar{F}$ is normal and thus $\bar{L}$ is a splitting field of some polynomial $h(x)$ over $\bar{L}$. Choose $H(x)$ over F so that

$$H(x) = h(x)(\text{mod } \mathfrak{p}).$$

By Hensel's lemma $H(x)$ splits into linear factors in L, and the preceding argument shows that one of its roots generates L over K, i.e. that L is the splitting field of $H(x)$ over F and so is normal.

If g is any element of the Galois group G of L/F and for any a in S we donate by $\bar{a}$ its image in $\bar{L}$, then the formula $\bar{g}(\bar{x}) = \overline{g(x)}$ defines an automorphism $\bar{g}$ of $\bar{L}/\bar{F}$. We shall prove that the mapping $g \to \bar{g}$ is

bijective. Since the groups of L/F and $\bar{L}/\bar{F}$ have the same number of elements, it suffices to show that this mapping is surjective. Let $a, b, f(x)$ and $E(x)$ have the same meaning as at the beginning of the prove and let $\bar{b} = a$. If s is an element of the Galois group $G(\bar{L}/\bar{F})$, then $s(a) = a_1$ is again a root of $f(x)$, and Hensel's lemma implies the existence of b_1 in S such that $F(b_1) = 0$ and $\bar{b_1} = a_1$. Such an element is unique because f has in $\bar{L}$ as many roots as F has in L, and so all roots of F have distinct images in $\bar{L}$. Now if g is an element of G which takes b into b_1, then $\bar{g} = s$; hence the required surjectivity follows. □

Ramified Extensions:

A monic polynomial

$$e(x) = x^m + a_{m-1}x^{m-1} + \cdots + a_0 \in \mathfrak{o}_\mathfrak{p}[X]$$

is said to be an *Eisenstein polynomial* if $\mathrm{ord}_\mathfrak{p}(a_0) = 1$ and $\mathrm{ord}_\mathfrak{p}(a_i) \geq 1$ for $1 \leq i \leq m-1$, that is, $a_0 \in \mathfrak{p} \setminus \mathfrak{p}^2$ and $a_i \in \mathfrak{p}$ for $1 \leq i \leq m-1$. It is clear that an Eisenstein polynomial $e(x)$ is irreducible.

Theorem 2.38. *(1), If $E = F(\alpha)$ and the minimal polynomial $E(x)$ of α is an Eisenstein polynomial, then E/F is totally ramified and* $\mathrm{ord}_E(\alpha) = 1$.

(2), If E is totally ramified over F and α is a uniformizer, then the minimal polynomial of α over F is an Eisenstein polynomial and $E = F(\alpha)$.

Proof. (1) Let $f(x) = x^n + a_1x^{n-1} + \cdots + a_n$ be the minimum polynomial of α over F. Then f is Eisenstein, that is, $\mathrm{ord}_{\mathfrak{p}_F}(a_i) \geq 1$ for $1 \leq i \leq n$ and $\mathrm{ord}_{\mathfrak{p}_F}(a_n) = 1$. Hence, the Newton polygon of $f(x)$ is the line joining $(n, \mathrm{ord}_{\mathfrak{p}_F}) = (n, 0)$ with $(0, \mathrm{ord}_{\mathfrak{p}_F}) = (0, 1)$.

Thus, we have

$$\mathrm{ord}(\alpha) = 1/n,$$

where $\mathrm{ord}(\cdot)$ is the extension of $\mathrm{ord}_{\mathfrak{p}_F}(\cdot)$ on the algebraic closure of F and since

$$E(\alpha) = 0, \quad a_i \equiv 0 \mod \mathfrak{p}_F,$$

$$\alpha \equiv 0 \mod \mathfrak{P}_E, \quad e(E/F)\mathrm{ord}_{\mathfrak{p}_F}(\alpha) = \mathrm{ord}_{\mathfrak{P}_E}(\alpha) \geq 1.$$

This means that $e = n$, and that E/F is totally ramified. Furthermore, $\mathrm{ord}_E(\alpha) = \mathrm{ord}_{\mathfrak{P}_E}(\alpha) = e\mathrm{ord}_{\mathfrak{p}_F}(\alpha) = 1$.

(2) Let $f(x) = x^m + a_1x^{m-1} + \cdots$ be the minimum polynomial of α over $\mathcal{O}_F[X]$ and $\mathrm{ord}(\cdot)$ be the extension of $\mathrm{ord}_{\mathfrak{p}_F}(\cdot)$ on the algebraic closure of F. Since E/F is totally ramified, $1 = \mathrm{ord}_{\mathfrak{P}_E}(\alpha) = n\mathrm{ord}(\alpha)$ with $n = [E : F]$.

Suppose that $\alpha_1, \cdots, \alpha_m$ are m roots of $f(x)$. Then $\text{ord}(\alpha_i), 1 \leq i \leq m$ are all equal. Hence,

$$\begin{aligned}\text{ord}_{\mathfrak{p}_F}(a_m) &= \text{ord}(a_m) = \text{ord}(\alpha_1) + \cdots + \text{ord}(\alpha_m) \\ &= m\text{ord}(\alpha) = \frac{m}{n}.\end{aligned}$$

However, $\text{ord}_{\mathfrak{p}_F}(a_m) \in \mathbb{Z}$. So $m \geq n$.

On the other hand, $n = [E : F] \geq [F(\alpha) : F] = m$, meaning that $n = m$ and $E = F(\alpha)$. Since a_i are polynomials of $\alpha_1, \cdots, \alpha_m$ and $\text{ord}(\alpha_i) = \text{ord}(\alpha) > 0$, $\text{ord}_{\mathfrak{p}_F}(a_i) = \text{ord}(a_i) \geq 1$ for $1 \leq i \leq m$. From $\text{ord}_{\mathfrak{p}_F}(a_m) = \frac{m}{n} = 1$, we have $f(x)$ is Einsenstein polynomial. □

2.3.3 Galois extensions: Local Hilbert theory

Let K/k be a Galois extension of number fields with the Galois group $G = \text{Gal}(K/k)$ and $[K : k] = n$. Let $\mathfrak{p}$ be a fixed prime ideal of $\mathfrak{o}_k$ and $\mathfrak{P}$ be prime ideal above $\mathfrak{p}$ in $\mathfrak{O}_K$. Let w and v be the places of K and k corresponding to $\mathfrak{P}$ and $\mathfrak{p}$, so that w lies above v, say $w|v$.

By the global Hilber theory, the decomposition group of $\mathfrak{P}$ is $D_{\mathfrak{P}}$ with the order ef. The elements of $D_{\mathfrak{P}}$ acts as isometries of K in the norm $|\cdot|_{\mathfrak{P}}$. Consequently $\sigma \in D_{\mathfrak{P}}$ extends to an automorphism of $K_{\mathfrak{P}}$, and we can thin in terms of an inclusion.

Theorem 2.39. *There is a natural embedding* $\text{Gal}(K_{\mathfrak{P}}/k_{\mathfrak{p}})$ *into* G *such that* $\text{Gal}(K_{\mathfrak{P}}/k_{\mathfrak{p}}) \cong D_{\mathfrak{P}}$ *and the extension of local fields* $K_{\mathfrak{P}}/k_{\mathfrak{p}}$ *is also Galois.*

Proof. Let $K_{\mathfrak{P}} = k_{\mathfrak{p}}(\alpha)$ where α is generator of the extension K/k. The conjugates of α over $k_{\mathfrak{p}}$ from a subset of the set of conjugates of α over k, and so they all lie in $K \subset K_{\mathfrak{P}}$. Denote the mapping ϕ by

$$\phi : \text{Gal}(K_w/k_v) \longrightarrow G.$$

By Corollary, $\sigma \in \text{Gal}(K_w/k_v)$ is an isometry with respect to the metric induced by $|\cdot|_{\mathfrak{P}}$. In particular, $\sigma\mathfrak{O}_{\mathfrak{P}} = \mathfrak{O}_{\mathfrak{P}}$ and $\sigma\mathfrak{P}_{\mathfrak{P}} = \mathfrak{P}_{\mathfrak{P}}$. It follows that $\sigma\mathfrak{P} = \mathfrak{P}$. Then $Im(\phi) \subset D_{\mathfrak{P}}$. On the other hand, for any $\tau \in D_{\mathfrak{P}}$, denote the mapping by $\sigma\alpha = \sigma(\alpha_n) = (\tau\alpha_n)$, where the Cauchy sequence $(\alpha_n) \in K_{\mathfrak{P}}$. We have $\sigma \in \text{Gal}(K_w/k_v)$. Then $Im(\phi) = D_{\mathfrak{P}}$.

It remains to prove that ϕ is injective. If $\phi(\sigma)$ is the identity map over K, then σ is also the identity map one the whole field $K_{\mathfrak{P}}$ because K is dense in $K_{\mathfrak{P}}$. This proves the theorem. □

In global Hilbert theory, we have the following exact sequence:

$$1 \to I_{\mathfrak{P}} \to D_{\mathfrak{P}} \to \text{Gal}(\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}}) \to 1.$$

Similarly, we can define a local mapping

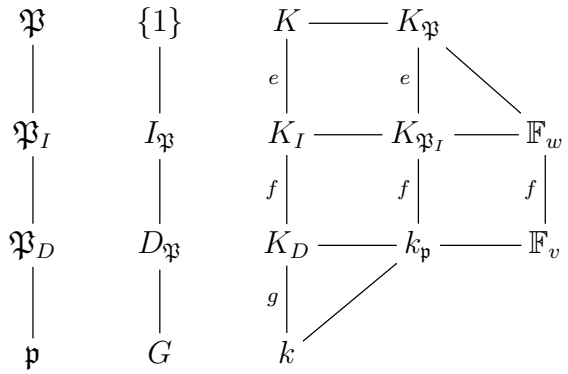
$$\begin{aligned} \pi : \ \mathrm{Gal}(K_w/k_v) &\longrightarrow \mathrm{Gal}(\mathbb{F}_w/\mathbb{F}_v) \\ \sigma &\longmapsto \overline{\sigma}, \end{aligned}$$

via $\overline{\sigma}(\alpha \bmod \mathfrak{P}_{\mathfrak{P}}) = \sigma(\alpha) \bmod \mathfrak{P}_{\mathfrak{P}}$. It is clear that this mapping is a surjective homomorphism. The kernel I_w of the homomorphism is given by

$$I_w = \{\sigma \in \mathrm{Gal}(K_w/k_v) \ : \ \sigma\alpha \equiv \alpha \bmod \mathfrak{P}_{\mathfrak{P}} \text{ for all } \alpha \in \mathfrak{O}_{\mathfrak{P}}\}.$$

A slight change in the proof actually show that we have also the same exact sequence:

$$1 \to I_w \to \mathrm{Gal}(K_w/k_v) \to \mathrm{Gal}(\mathbb{F}_w/\mathbb{F}_v) \to 1.$$



Let us define the sequence of subgroups of I_w

$$R_i = \{\sigma \in I_w \ : \ \sigma\alpha \equiv \alpha (\bmod \mathfrak{P}_{\mathfrak{P}}^{i+1}), \text{ for all } \alpha \in \mathfrak{O}_{\mathfrak{P}}\}.$$

It's clear that R_i is subgroup of G, and is called the *ith ramification group* of G at $\mathfrak{P}$ and

$$\mathrm{Gal}(K_w/k_v) \supset I_w = R_0 \supset R_1 \supset R_2 \supset \cdots .$$

Corresponding to this decreasing sequence of subgroups, we have the increasing sequence of subfields:

$$k_v \subset K_1 \subset K_2 \subset \cdots \subset K_w.$$

Proposition 2.40. *(1), Let Π be an element of $\mathfrak{P}$ with not in $\mathfrak{P}^2$. Then*

$$R_i = \{\sigma \in I_{\mathfrak{P}} \ : \ \sigma\Pi \equiv \Pi (\bmod \mathfrak{P}^{i+1})\},$$

and is a normal subgroup of $D_{\mathfrak{P}}$.

(2), R_1 is the unique Sylow p-subgroup of $I_{\mathfrak{P}}$ where p is the restrict of $\mathfrak{p}$ to $\mathbb{Z}$. R_0/R_1 is cyclic and its order divides $N\mathfrak{P} - 1$.

(3), $R_i/R_{i+1}, i \geq 1$ is an elementary p-group.

Proof. (1), For a fixed $\Pi \in \mathfrak{P} \setminus \mathfrak{P}^2$, denote

$$R_i' = \{\sigma \in I_{\mathfrak{P}} \,|\, \sigma\Pi \equiv \Pi (\mathrm{mod} \mathfrak{P}^{i+1})\}.$$

According to Equation (2.6), any nonzero $\alpha \in \mathfrak{O}_{\mathfrak{P}}$ can be written uniquely as

$$\alpha = u\Pi^{\mathrm{ord}_{\mathfrak{P}}\alpha}, \text{ where } u \in \mathfrak{O}_{\mathfrak{P}} \setminus \mathfrak{P}_{\mathfrak{P}} = U_{\mathfrak{P}}.$$

If $\sigma \in R_i'$, then there exists a $\beta, \beta' \in \mathfrak{O}_{\mathfrak{P}}$ such that $\sigma\Pi = \Pi + \beta\Pi^{i+1}$ and $\sigma u = u + \beta'\Pi$. Thus

$$\begin{aligned} |\sigma\alpha - \alpha|_{\mathfrak{P}} &= |\alpha|_{\mathfrak{P}} \cdot |\sigma\alpha/\alpha - 1|_{\mathfrak{P}} \\ &\leq |\frac{\sigma u}{u} \cdot \left(\frac{\sigma\Pi}{\Pi}\right)^{\mathrm{ord}_{\mathfrak{P}}\alpha} - 1|_{\mathfrak{P}} \\ &= |(1+\beta' u^{-1}\Pi)(1+\beta\Pi^i)^{\mathrm{ord}_{\mathfrak{P}}\alpha} - 1|_{\mathfrak{P}} \\ &= \max\{|\beta' u^{-1}\Pi|_{\mathfrak{P}}, |\beta\Pi^i|_{\mathfrak{P}}\} \\ &\leq \end{aligned}$$

So $\sigma \in R_i$. And clearly $\sigma \in R_i \Rightarrow \sigma \in R_i'$. Hence

$$R_i = \{\sigma \in I_{\mathfrak{P}} \,|\, \sigma\Pi \equiv \Pi (\mathrm{mod} \mathfrak{P}^{i+1})\}.$$

For any $\tau \in D_{\mathfrak{P}}$, $\sigma \in R_i$, $\alpha \in \mathfrak{O}_{\mathfrak{P}}$,

$$|\tau^{-1}\sigma\tau\alpha - \alpha|_{\mathfrak{P}} = |\tau^{-1}(\sigma\tau\alpha - \tau\alpha)|_{\mathfrak{P}} = |\sigma(\tau\alpha) - (\tau\alpha)|_{\mathfrak{P}} \leq N\mathfrak{P}^{-(i+1)}.$$

Then $\tau^{-1}\sigma\tau \in R_i$, which means R_i is a normal subgroup of $D_{\mathfrak{P}}$.

(2), If σ is an element of R_1 other than identity, then we can choose a $\Pi \in \mathfrak{P} \setminus \mathfrak{P}^2$ so that $\sigma\Pi \neq \Pi$. Thus $\sigma\Pi \equiv \Pi + u\Pi^m \mod \mathfrak{P}^{m+1}$ for some $m > 1$ and $u \in U_{\mathfrak{P}}$. By iterating we obtain $\sigma^r\Pi \equiv \Pi + ru\Pi^m \mod \mathfrak{P}^{m+1}$. Suppose that r is the order of σ, then $\sigma^r\Pi = \Pi$, which means $ru\Pi^m \in \mathfrak{P}^{m+1}$. Thus σ cannot have order prime to p where p is the rational prime underlying $\mathfrak{P}$, and the same happens for any power of σ other than the identity. So any element of R_1 has order a power of p.

Let $\sigma \in R_0$; then $\sigma\Pi$ is also a prime element and so $\sigma\Pi = u\Pi$ with u a unit in $\mathfrak{O}_{\mathfrak{P}}$. Then the map

$$\begin{aligned} \varphi_0 : R_0 &\longrightarrow U_{\mathfrak{P}}/(1+\mathfrak{P}_{\mathfrak{P}}) \\ \sigma &\longmapsto u \mod (1+\mathfrak{P}_{\mathfrak{P}}) \end{aligned}$$

is a group homomorphism with kernel R_1. So R_1 is normal in R_0, and R_0/R_1 is isomorphic to a subgroup of $U_{\mathfrak{P}}/(1+\mathfrak{P}_{\mathfrak{P}}) \cong \mathbb{F}_w^{\times} = (\mathfrak{O}_{\mathfrak{P}}/\mathfrak{P}_{\mathfrak{P}})^{\times}$,

a cyclic group of order $N\mathfrak{P}-1$. And thus R_0/R_1 is cyclic and its order divides $N\mathfrak{P}-1$.

Since $N\mathfrak{P}$ is a power of p, $|R_0/R_1|$ is relatively prime to p. So R_1 is a Sylow p-subgroup of $R_0 = I_{\mathfrak{P}}$. What's more, we know that all Sylow p-subgroups of an arbitrary finite group are conjugate, and R_1 is normal in R_0. So R_1 is the unique Sylow p-subgroup.

(3), For $i \geq 1$, if $\sigma \in R_i$, then $\sigma\Pi - \Pi \in \mathfrak{P}^{i+1}$, that is, $\sigma\Pi/\Pi - 1 \in \mathfrak{P}^i$. Consider the mapping

$$\begin{aligned} \varphi_i : \ R_i &\longrightarrow U_{\mathfrak{P}}^{(i)}/U_{\mathfrak{P}}^{(i+1)} \\ \sigma &\longmapsto \frac{\sigma\Pi}{\Pi} \mod U_{\mathfrak{P}}^{(i+1)} \end{aligned}$$

where

$$\begin{aligned} U_{\mathfrak{P}}^{(i)} &= 1+\mathfrak{P}_{\mathfrak{P}}^i \\ &= \{\alpha \in K_{\mathfrak{P}}^{\times} \,:\, \mathrm{ord}_{\mathfrak{P}}(\alpha-1) \geq i\} \\ &= \{\alpha \in K_{\mathfrak{P}}^{\times} \,:\, |\alpha-1|_{\mathfrak{P}} \leq (N\mathfrak{P})^{-i}\}. \end{aligned}$$

Then φ_i is a group homomorphism with kernel R_{i+1}. So R_i/R_{i+1} is isomorphic to a subgroup of $U_{\mathfrak{P}}^{(i)}/U_{\mathfrak{P}}^{(i+1)}$. We have already known that $U_{\mathfrak{P}}^{(i)}/U_{\mathfrak{P}}^{(i+1)} \cong \mathfrak{O}_{\mathfrak{P}}/\mathfrak{P}_{\mathfrak{P}}$ via $1+\alpha\Pi^i \mapsto \alpha \bmod \mathfrak{P}_{\mathfrak{P}}$, and $\mathfrak{O}_{\mathfrak{P}}/\mathfrak{P}_{\mathfrak{P}}$ is a additive group of order $N\mathfrak{P}$, which is an elementary p-group, being a vector space over $\mathbb{Z}/(p)$. So R_i/R_{i+1} is an elementary p-group. □

Corollary 2.41. *The Galois group of any finite normal extension of a $\mathfrak{p}$-adic field is solvable.*

For a Galois extension, it is clear that $K_{\mathfrak{P}}/k_{\mathfrak{p}}$ is unramified if and only if $R_0 = \{1\}$ and $K_{\mathfrak{P}}/k_{\mathfrak{p}}$ is tamely ramified if and only if $R_1 = \{1\}$.

2.4 Ramification Theory

Many number-theoretic objects give rise to an ideal which identifies the bad primes for that object and measures how bad they are. Such an ideal is important primarily because it has this this property.

2.4.1 The different

Let E/F be a finite separable extension of local fields or global fields with the integral domain $O_E \supset O_F$ and $[L:K] = n$. Let M be a nonzero subset of E. The *complementary set* M' of M is denoted by

$$M' = \{\alpha \in E : Tr_{E/F}(\alpha M) \subset O_F\}.$$

Our first major result will state that if M is a fractional ideal of E, then so is M'.

Lemma 2.42. *If $\omega_1, \ldots, \omega_n$ is a basis of E over F and*

$$M = O_F\omega_1 + \cdots + O_F\omega_n.$$

Then

$$M' = O_F\omega_1' + \cdots + O_F\omega_n',$$

where $\{\omega_1', \ldots, \omega_n'\}$ is the dual basis relative to the trace, that is, $Tr_{E/F}(\omega_i\omega_j') = \delta_{ij}$. In particular, if $\mathfrak{a}$ is a fractional ideal of O_E, then $\mathfrak{a}'$ is also a fractional ideal. Furthermore $O_E \subset O_E'$.

Proof. Let $\alpha \in M'$ and write

$$\alpha = a_1\omega_1' + \cdots + a_n\omega_n'$$

with $a_i \in F$. Then $Tr(\alpha\omega_i) = a_i$, whence $a_i \in O_F$ for all i. This proves $M' \subset O_F\omega_1' + \cdots + O_F\omega_n'$.

Conversely,

$$Tr(O_F\omega_i'M) = O_F Tr(\omega_i'M) \subset o_F.$$

So $O_F\omega_1' + \cdots + O_F\omega_n' \subset M'$.

Since every a fractional ideal of E is squeezed between two O_F-modules of type $O_F\omega_1 + \cdots + O_F\omega_n$ for suitable bases $\{\omega_i\}$ of E over F, and since O_F is noetherian. We get that if $\mathfrak{a}$ is a fractional ideal of O_E, then $\mathfrak{a}'$ is also a fractional ideal. □

The integral ideal $O_E'^{-1}$ of O_E is called the *different* of E/F and is denoted by $\mathfrak{D}_{E/F}$, i.e.,

$$\mathfrak{D}_{E/F}^{-1} = \{\alpha \in E \,:\, Tr_{E/F}(\alpha O_E) \subset O_F\}.$$

We prove now the following transitivity properties of the different.

Proposition 2.43. *For a tower of fields $F \subset E \subset K$, one has*

$$\mathfrak{D}_{K/F} = \mathfrak{D}_{K/E}\mathfrak{D}_{E/F}.$$

Proof. It is easy to see that $(\mathfrak{D}_{E/F}O_K)^{-1} = \mathfrak{D}_{E/F}^{-1}O_K$, and therefore

$$\mathfrak{D}_{K/F} = \mathfrak{D}_{K/E}\mathfrak{D}_{E/F} \Longleftrightarrow \mathfrak{D}_{K/F}^{-1} = \mathfrak{D}_{K/E}^{-1}\mathfrak{D}_{E/F}^{-1}.$$

Now, for any $\alpha \in K$ we have

$$\begin{aligned}
\alpha \in \mathfrak{D}_{K/F}^{-1} &\iff Tr_{K/F}(\alpha O_K) \subset O_F \\
&\iff Tr_{E/F}(Tr_{K/E}(\alpha O_K)) \subset O_F \\
&\iff Tr_{K/E}(\alpha O_K) \subset \mathfrak{D}_{E/F}^{-1} \\
&\iff Tr_{K/E}(\alpha \mathfrak{D}_{E/F} O_K) \subset O_E \\
&\iff \alpha \mathfrak{D}_{E/F} \subset \mathfrak{D}_{K/E}^{-1} \\
&\iff \alpha \subset \mathfrak{D}_{K/E}^{-1}\mathfrak{D}_{E/F}^{-1}.
\end{aligned}$$

This completes the proof. □

Lemma 2.44. *(Euler lemma) Let $E = F(\alpha)$ be a finite separable extension of degree n. Let $f(x)$ be the irreducible polynomial of α over F and $f'(x)$ be its formal derivative. Write*

$$\frac{f(x)}{x-\alpha} = b_{n-1}x^{n-1} + \cdots + b_1 x + b_0.$$

Then the dual basis of $\{1, \alpha, \ldots, \alpha^{n-1}\}$ is

$$\frac{b_0}{f'(\alpha)}, \ldots, \frac{b_{n-1}}{f'(\alpha)}.$$

Proof. For if $\alpha_1, ..., \alpha_n$ are the roots of f, then one has

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

as the difference of the two sides is a polynomial of degree $\leq n-1$ with roots $\alpha_1, ..., \alpha_n$, so is identically zero. We may write this equation in the form

$$Tr_{E/F}\left[\frac{f(x)}{x-\alpha}\frac{\alpha^r}{f'(\alpha)}\right] = x^r.$$

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

$$Tr_{E/F}\left(\alpha^i \frac{b_j}{f'(\alpha)}\right) = \delta_{ij}$$

and the lemma follows. □

Corollary 2.45. *If $O_E = O_F[\alpha]$. Then $\mathfrak{D}_{E/F} = (f'(\alpha))$.*

Proof. As $O_E = O_F[\alpha] = O_F + O_F\alpha + \cdots + O_F\alpha^{n-1}$, we get

$$\mathfrak{D}_{E/F}^{-1} = O_E' = f'(\alpha)^{-1}(O_F b_0 + \cdots + O_F b_{n-1}).$$

Considering the coefficient of each of the powers of x of $f(x)$, we get

$$b_{n-i} = \alpha^{i-1} + a_{n-1}\alpha^{i-2} + \cdots + a_{n-i+1},$$

so that

$$O_F b_0 + \cdots + O_F b_{n-1} = O_F[\alpha] = O_E.$$

Then $\mathfrak{D}_{E/F}^{-1} = f'(\alpha)^{-1}O_E$, and thus $\mathfrak{D}_{E/F} = f'(\alpha)O_E = (f'(\alpha))$. □

2.4.2 The discriminant

For a finite extension $k/\mathbb{Q}$, we have defined the absolute discriminant d_k of k. The definition of the discriminant of a general algebraic number field K/k was given by Dedekind. Let $[K : k] = n$ and let $\alpha_1, \ldots, \alpha_n$ be n elements of $\mathfrak{O}_K$ linearly independent over k. We write

$$d_{K/k}(\alpha_1, \ldots, \alpha_n) = \det(\mathrm{Tr}_{K/k}(\alpha_i\alpha_j));$$

then the *relative discriminant* $d_{K/k}$ of K/k is the ideal in k generated by all the $d_{K/k}(\alpha_1, \ldots, \alpha_n)$. Note that $d_{K/k}$ is an integral ideal of $\mathfrak{o}_k$.

Lemma 2.46. *(1), For a extension of $k/\mathbb{Q}$, we have $N_{k/\mathbb{Q}}(\mathfrak{D}_{k/\mathbb{Q}}) = |d_k|$.*
(2), $d_{K/k} = N_{K/k}(\mathfrak{D}_{K/k})$.

Proof. (1), Let $\alpha_1, \ldots, \alpha_n$ be an integral basis of k, that is,

$$\mathfrak{o}_k = \mathbb{Z}\alpha_1 + \cdots + \mathbb{Z}\alpha_n.$$

Then

$$\mathfrak{D}_{k/\mathbb{Q}}^{-1} = \mathbb{Z}\beta_1 + \cdots + \mathbb{Z}\beta_n,$$

where $Tr(\alpha_i\beta_j) = \delta_{ij}$. Assume that $\beta_j = \sum_{i=1}^n c_{ij}\alpha_s$ with $c_{ij} \in \mathbb{Q}$. Then

$$\begin{aligned}(Tr(\alpha_i\alpha_j))(c_{ij}) &= \Big(\sum_{s=1}^n Tr(\alpha_i\alpha_s)c_{sj}\Big) \\ &= \Big(Tr\big(\alpha_i \sum_{s=1}^n c_{sj}\alpha_s\big)\Big) \\ &= (Tr(\alpha_i\beta_j)) \\ &= I.\end{aligned}$$

It implies that $|d_k| \det(c_{ij}) = 1$. According the definition of norm of ideals, we obtain

$$\mathrm{N}_{k/\mathbb{Q}}(\mathfrak{D}_{k/\mathbb{Q}}) = \Big\{\mathrm{N}_{k/\mathbb{Q}}(\mathfrak{D}_{k/\mathbb{Q}}^{-1})\Big\}^{-1} = \{\det(c_{ij})\}^{-1} = |d_k|.$$

□

Let K/k be a extension of number fields with $[K : k] = n$. Let $\mathfrak{p}$ be a fixed prime ideal of $\mathfrak{o}_k$ and $\mathfrak{P}$ be prime ideal above $\mathfrak{p}$ in $\mathfrak{O}_K$. For any extension of local fields $K_\mathfrak{P}/k_\mathfrak{p}$ with the degree ef, we also can define the local discriminant for $K_\mathfrak{P}/k_\mathfrak{p}$. Let

$$\mathfrak{D}_{K_\mathfrak{P}/k_\mathfrak{p}}^{-1} = \mathfrak{O}_\mathfrak{P}'^{-1} = \{\alpha \in K_\mathfrak{P} \,:\, Tr_{K_\mathfrak{P}/k_\mathfrak{p}}(\alpha\mathfrak{O}_\mathfrak{P}) \subset \mathfrak{o}_\mathfrak{p}\}$$

be the local different for the extension $K_\mathfrak{P}/k_\mathfrak{p}$. Then $\mathfrak{D}_{K_\mathfrak{P}/k_\mathfrak{p}}$ is an integral ideal of $\mathfrak{o}_\mathfrak{p}$, say $\mathfrak{P}_\mathfrak{P}^d$ where d is called the *differential exponent*. Let $\omega_1, \ldots, \omega_{ef}$ be a basis of $K_\mathfrak{P}$ over $k_\mathfrak{p}$ satisfying

$$\mathfrak{O}_\mathfrak{P} = \mathfrak{o}_\mathfrak{p}\omega_1 + \cdots + \mathfrak{o}_\mathfrak{p}\omega_{ef}.$$

We have

$$D_{K_\mathfrak{P}/k_\mathfrak{p}}^{-1} = (\Pi^{-d}) = \mathfrak{o}_\mathfrak{p}\omega_1' + \cdots + \mathfrak{o}_\mathfrak{p}\omega_{ef}',$$

where $\{\omega_1', \ldots, \omega_{ef}'\}$ is the dual basis relative to the trace. We define the *local discriminant* by

$$d_{K_\mathfrak{P}/k_\mathfrak{p}} = \det(Tr_{K_\mathfrak{P}/k_\mathfrak{p}}(\omega_i\omega_j)).$$

It is easy check that $d_{K_\mathfrak{P}/k_\mathfrak{p}} \in \mathfrak{o}_\mathfrak{p}$ and the ideal $(d_{K_\mathfrak{P}/k_\mathfrak{p}})$ of $\mathfrak{o}_\mathfrak{p}$ is independent the choice of the basis $\{\omega_1, \ldots, \omega_n\}$.

Lemma 2.47. *With notations and assumptions as above. Then* $\mathrm{ord}_{\mathfrak{p}}(d_{K_{\mathfrak{P}}/k_{\mathfrak{p}}}) = fd$ *and* $d_{K_{\mathfrak{P}}/k_{\mathfrak{p}}}\mathfrak{o}_{\mathfrak{p}} = N_{K_{\mathfrak{P}}/k_{\mathfrak{p}}}(\mathfrak{D}_{K_{\mathfrak{P}}/k_{\mathfrak{p}}})$.

Proof. If S is a multiplicative subset of $K_{\mathfrak{P}}$, then clearly $d_{S^{-1}K_{\mathfrak{P}}/S^{-1}k_p} = S^{-1}d_{K_{\mathfrak{P}}/k_p}$ and $\mathfrak{D}_{S^{-1}K_{\mathfrak{P}}/S^{-1}k_p} = S^{-1}\mathfrak{D}_{K_{\mathfrak{P}}/k_p}$. Assume that $K_{\mathfrak{P}}$ has an integral basis $\alpha_1, \ldots, \alpha_n$. So we have $d_{K_{\mathfrak{P}}/k_p} = (d(\alpha_1, \ldots, \alpha_n))$. Dedekind's Complementary module $\mathfrak{C}_{K_{\mathfrak{P}}/k_p}$ is generated by the dual basis $\alpha_1^{'}, \ldots, \alpha_n^{'}$ which satisfies $Tr_{K_{\mathfrak{P}}/k_p}(\alpha_i\alpha_j^{'}) = \delta_{ij}$. On the other hand, $\mathfrak{C}_{K_{\mathfrak{P}}/k_p}$ is a principal ideal (β) and admits the k_p- basis $\beta\alpha_1, \ldots, \beta\alpha_n$ of discriminant

$$d(\beta\alpha_1, \ldots, \beta\alpha_n) = N_{K_{\mathfrak{P}}/k_p}(\beta)^2 d(\alpha_1, \ldots, \alpha_n).$$

But $(N_{K_{\mathfrak{P}}/k_p}(\beta)) = N_{K_{\mathfrak{P}}/k_p}(\mathfrak{C}_{K_{\mathfrak{P}}/k_p}) = N_{K_{\mathfrak{P}}/k_p}(\mathfrak{D}^{-1}_{K_{\mathfrak{P}}/k_p}) = N_{K_{\mathfrak{P}}/k_p}(\mathfrak{D}_{K_{\mathfrak{P}}/k_p})^{-1}$, and $(d(\alpha_1, \ldots, \alpha_n)) = d_{K_{\mathfrak{P}}/k_p}$. One has $d(\alpha_1, \ldots, \alpha_n) = det((\sigma_i\alpha_j))^2$, $d(\alpha_1^{'}, \ldots, \alpha_n^{'}) = det((\sigma_i\alpha_j^{'}))^2$, and $Tr(\alpha_i\alpha_j^{'}) = \delta_{ij}$. Then $d(\alpha_1, \ldots, \alpha_n) \cdot d(\alpha_1^{'}, \ldots, \alpha_n^{'}) = 1$. Combining these yields

$$d^{-1}_{K_{\mathfrak{P}}/k_p} = (d(\alpha_1, \ldots, \alpha_n)^{-1}) = (d(\alpha_1^{'}, \ldots, \alpha_n^{'})) = (d(\beta\alpha_1, \ldots, \beta\alpha_n))$$

$$= N_{K_{\mathfrak{P}}/k_p}(\mathfrak{D}_{K_{\mathfrak{P}}/k_p})^{-2} d_{K_{\mathfrak{P}}/k_p},$$

and hence $N_{K_{\mathfrak{P}}/k_p}(\mathfrak{D}_{K_{\mathfrak{P}}/k_p}) = d_{K_{\mathfrak{P}}/k_p}$. □

2.4.3 Ramification theory

With notations and assumptions as above. We identify $\mathfrak{D}_{K_{\mathfrak{P}}/k_{\mathfrak{p}}}$ with a power of $\mathfrak{P}$, though strictly speaking it is a power of $\mathfrak{P}_{\mathfrak{P}}$.

Proposition 2.48. *(1), The global different is the product of the local differents, i.e.,*

$$\mathfrak{D}_{K/k} = \prod_{\mathfrak{P}} \mathfrak{D}_{K_{\mathfrak{P}}/k_{\mathfrak{p}}}.$$

(2), The global relative discriminant is the product of the local discriminants, i.e.,

$$d_{K/k} = \prod_{\mathfrak{P}} d_{K_{\mathfrak{P}}/k_{\mathfrak{p}}}.$$

Proof. Let $x \in \mathfrak{D}^{-1}_{K_{\mathfrak{P}}/k_{\mathfrak{p}}}$, we choose $y \in K$, which's very close to x at $\mathfrak{P}$, very close to 0 at all other prime divisors of $\mathfrak{p}$ in K, and of value at most 1 at

all other finite K-primes. Then by Corollary 2.35, for all k-primes $\mathfrak{p}$ and $z \in \mathfrak{O}_K$

$$\begin{aligned} &\mathrm{Tr}_{K/k}(yz) = \sum_{\mathfrak{P}|\mathfrak{p}} \mathrm{Tr}_{K_{\mathfrak{P}}/k_{\mathfrak{p}}}(yz) \in \mathfrak{o}_{\mathfrak{p}} \\ &\Rightarrow \mathrm{Tr}_{K/k}(yz) \in \mathfrak{o}_k \end{aligned}$$

Therefore

$$\begin{aligned} &y \in \mathfrak{d}_{K/k}^{-1} \\ &\Rightarrow x \in \mathfrak{d}_{K/k}^{-1} \\ &\Rightarrow \mathfrak{D}_{K/k} \subseteq \mathfrak{D}_{K_{\mathfrak{P}}/k_{\mathfrak{p}}} \end{aligned}$$

Conversely, we assume that $x \in \mathfrak{D}_{K/k}^{-1}$, and choose $y \in K$, which's very close to x at $\mathfrak{P}$, very close to 0 at other prime divisors of $\mathfrak{p}$ in K, and of valve at most 1 at all other finite K-primes. Reasoning as above, we see that for all $z \in \mathfrak{O}_K$

$$\begin{aligned} &\mathrm{Tr}_{K_{\mathfrak{P}}/k_{\mathfrak{p}}}(yz) \in \mathfrak{o}_{\mathfrak{p}} \\ &\Rightarrow \mathrm{Tr}_{K_{\mathfrak{P}}/k_{\mathfrak{p}}}(x\mathfrak{O}_{\mathfrak{P}}) \subseteq \mathfrak{o}_{\mathfrak{p}} \\ &\Rightarrow x \in \mathfrak{D}_{K_{\mathfrak{P}}/k_{\mathfrak{p}}}^{-1} \\ &\Rightarrow \mathfrak{D}_{K/k} \supseteq \mathfrak{D}_{K_{\mathfrak{P}}/k_{\mathfrak{p}}} \end{aligned}$$

This shows $\mathfrak{D}_{K/k}$ is dense in $\mathfrak{D}_{K_{\mathfrak{P}}/k_{\mathfrak{p}}}$, that is, $\mathfrak{D}_{K/k}\mathfrak{O}_{K_{\mathfrak{P}}} = \mathfrak{D}_{K_{\mathfrak{P}}/k_{\mathfrak{p}}}$. Then $\mathfrak{D}_{K/k} = \prod_{\mathfrak{P}} \mathfrak{D}_{K_{\mathfrak{P}}/k_{\mathfrak{p}}}$. □

Theorem 2.49. *Let $e = e(\mathfrak{P}/\mathfrak{p})$ and $\mathrm{ord}_{\mathfrak{P}}(\mathfrak{D}_{K/k}) = m$. Then $\mathfrak{P}^{e-1}|\mathfrak{D}_{K/k}$. In particular, we have*

(1), $\mathfrak{P}$ is ramified in K/k if and only if $\mathfrak{P}|\mathfrak{D}_{K/k}$.

(2), $\mathfrak{P}$ is tamely ramified in K/k if and only if $m = e - 1$.

(3), $\mathfrak{P}$ is wildly ramified in K/k if and only if $e \leq m \leq \mathrm{ord}_{\mathfrak{P}}(e) + e - 1$.

Corollary 2.50. *The prime ideal $\mathfrak{p}$ of k is ramified in K/k if and only if $\mathfrak{p}|d_{K/k}$.*

Corollary 2.51. *For any finite extension $k/\mathbb{Q}$ at least one prime p ramifies.*

Proof. It follows immediately that $|d_k| > 1$ for any number field $k \neq \mathbb{Q}$ by Corollary (1.32) and the above theorem. □

Exercises

1, The $\mathfrak{p}$-adic valuation is nonarchimedean.

2,Let $|\cdot|$ be any valuation over any field k and $|\cdot|_\infty$ be the usual absolute value over $\mathbb{R}$. Then, for any $\alpha, \beta \in k$,

$$||\alpha| - |\beta||_\infty \leq |\alpha - \beta|.$$

3, A field of nonzero characteristic has only nonarchimedean valuations.

4, Let $|\cdot|$ be any valuation over any field k. Then the following statements are equivalent:

(1), the valuation $|\cdot|$ is nonarchimedean;

(2), for any $|\alpha| < 1$, we have $|1 + \alpha| < 1$;

(3), for any $|\alpha| \leq 1$, we have $|1 + \alpha| \leq 1$.

5, Let $\sigma_1, \ldots, \sigma_{r_1}, \sigma_{r_1+1} = \bar{\sigma}_{r_1+r_2+1}, \ldots, \sigma_{r_1+r_2} = \bar{\sigma}_n$ be embeddings of k. Let $|\cdot|_1, \ldots, |\cdot|_{r_1+r_2}$ be archimedean valuations induce by $\sigma_1, \ldots, \sigma_{r_1+r_2}$. Then $|\cdot|_1, \ldots, |\cdot|_{r_1+r_2}$ are pairwise inequivalent.

6, Let $\mathfrak{p}$ and $\mathfrak{q}$ be two distinct prime ideals of a number field k. Then the $\mathfrak{p}$-adic valuations $|\cdot|_\mathfrak{p}$ and $|\cdot|_\mathfrak{q}$ are inequivalent.

7, Find $\alpha \in \mathbb{Q}$, such that $v_2(\alpha - 1/3) \geq 2, v_3(\alpha - 1/2) \geq 3$, and $|\alpha - 1|_\infty < 1/2$.

8, If a sequence α_n converges a nonzero element α withe respect to any nonarchimedean valuation over a field k, then we have $|\alpha| = |\alpha_n|$ for sufficiently large n.

9,

$$\begin{aligned} \mathrm{ord}_\mathfrak{p} : k &\longrightarrow \mathbb{Z} \\ \alpha &\longmapsto \mathrm{ord}_\mathfrak{p}(\alpha). \end{aligned}$$

Then it is surjective.

10,

11, A valuation $|\cdot|$ on a field k is *discrete* if there is a $\delta > 0$ such that for any $\alpha \in k$

$$1 - \delta < |\alpha| < 1 + \delta \Longrightarrow |\alpha| = 1.$$

A non-archimedean valuation $|\cdot|$ on any field k is discrete if and only if $\mathfrak{p} = \{\alpha \in k : |\alpha| < 1\}$ is a principal ideal.

12, Let $|\cdot|_1, \ldots, |\cdot|_m$ be distinct places of k. If

$$|\alpha|_1^{r_1} \cdots |\alpha|_m^{r_m} = 1,$$

for all $\alpha \in k^\times$, where r_i are real constants, then $r_1 = \cdots = r_m = 0$.

13, (1), Let the polynomial $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in k_\mathfrak{p}[X]$ be irreducible. Then

$$\max\{|a_i|_\mathfrak{p} \,:\, 0 \le i \le n\} = \max\{|a_0|_\mathfrak{p}, |a_n|_\mathfrak{p}\}.$$

In particular, if $f(x) = x^n + a_1 x^{n-1} + \cdots + a_n \in k_\mathfrak{p}[X]$ is irreducible and $a_n \in \mathfrak{o}_\mathfrak{p}$, then all $a_i \in \mathfrak{o}_\mathfrak{p}$, i.e., $f(x) \in \mathfrak{o}_\mathfrak{p}[X]$.

(2), Let $\bar{f}(x) \in \mathbb{F}_\mathfrak{p}[X]$ be the polynomial obtained from $f(x)$ by reducing the coefficients of $f(x)$ modulo $\mathfrak{p}_\mathfrak{p}$. If $f(x) \in \mathfrak{o}_k[X]$ is monic and irreducible over $k_\mathfrak{p}$, then $\bar{f}(x)$ is a power of an irreducible polynomial in $\mathbb{F}_\mathfrak{p}[X]$.

14, Show that for any prime p, there are $p-1$ distinct $(p-1)$-th roots of unity in $\mathbb{Z}_p$.

15, $\mathfrak{o}_k = \bigcap_{\text{all prime ideals } \mathfrak{p}} \mathfrak{o}_\mathfrak{p}$.

15, Show that Fermat equation $x^n + y^n = 1$ has infinitely many solutions over $\mathbb{Z}_p$ for any integer $n \ge 1$.

16, Write power series of the number $2/3$ and $-2/3$ as 5-adic numbers.

17, Show that the equation $x^2 = 2$ has a solution in $\mathbb{Z}_7$.

18, Show that the exponential series

$$e^x = \sum_{n=0}^{\infty} \frac{x^n}{n!}$$

converges for $\mathrm{ord}_p(x) > \frac{1}{p-1}$ in $\mathbb{Q}_p$ and diverges elsewhere.

19, (Krasner's Lemma) Let F be a local field and α, β be two elements of the algebraic closure of F. Assume that α is separable over $F(\beta)$ and assume that for all isomorphisms σ of $F(\alpha)$, $\sigma \ne 1$, we have

$$|\beta - \alpha| < |\sigma\alpha - \alpha|.$$

Then $F(\alpha) \subset F(\beta)$.

20, Suppose that $f(x) \in \mathbb{Z}[X]$, then $f(x) = 0$ has a solution in $\mathbb{Z}_p$ iff for any $n \ge 1$, the equation $f(x) \equiv 0(\mod p^n)$ has solutions in $\mathbb{Z}$.

21, Let $K_\mathfrak{P} \supset k_\mathfrak{p}$ be local fields. If $x \in K_\mathfrak{P}$, then $|x|_\mathfrak{P} = |N_{K_\mathfrak{P}/k_\mathfrak{p}} x|_\mathfrak{p}^{1/[K_\mathfrak{P}:k_\mathfrak{p}]}$, and $\mathrm{ord}_\mathfrak{p}(N(x)) = f(\mathfrak{P}/\mathfrak{p})\mathrm{ord}_\mathfrak{P}(x)$.

22, Show that $x^2 - 82y^2 = \pm 2$ has solutions in every $\mathbb{Z}_p$ but not in $\mathbb{Z}$. What conclusion can you draw about $\mathbb{Q}(\sqrt{82})$?

23, Let $k = \mathbb{Q}(\alpha)$ with α a root of $f(x) = x^4 - 14$.

(1), Show that the prime 11 has three extensions to prime $\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3$ of k and $k_{\mathfrak{p}_1} = k_{\mathfrak{p}_2} = \mathbb{Q}_{11}$ while $[k_{\mathfrak{p}_3} : \mathbb{Q}_{11}] = 2$.

(2), The prime 13 has four extensions to primes of k.

(3), Show the prime 5 has two extensions to primes $\mathfrak{p}_1, \mathfrak{p}_2$ of k and $[k_{\mathfrak{p}_1} : \mathbb{Q}] = [k_{\mathfrak{p}_2} : \mathbb{Q}] = 2$.

24, Let E/F be a finite separable extension of local fields or global fields with the integral domain $O_E \supset O_F$ and $[L : K] = n$. Let I be a fractional ideal of E. Then

(1), $Tr(I) \subset O_F$ if and only if $I \subset O'_E$.

(2), I is an integral ideal if and only if ${I'}^{-1} \subset {O'_E}^{-1}$.

(3), $(I')' = I$.

(4), $Tr(O'_E) = O_F$,

(5), $I' = O'_E I^{-1}$.

25, Prove that if $[k_v : \mathbb{Q}_p] = n$ and $\mathfrak{D}_v = \mathfrak{D}_{k_v/\mathbb{Q}_p}$, then $k_v/\mathfrak{D}_v$ and $(\mathbb{Q}_p/\mathbb{Z}_p)^n$ are topologically isomorphic.

Chapter 3

Adele, Idele and Harmonic Analysis

In this chapter, we saw how we could associate various locally compact groups to an algebraic number field, and we saw how the topological properties of these groups translate into arithmetic properties of the field.

3.1 Adeles and Ideles

In discussing "local-to-global" problems it is often necessary to consider several different v-adic fields simultaneously, where each v may be either a finite or an infinite place. The natural language for this is that of adeles and ideles.

Recall: Some fundamental facts on any topological group Let G be a topological group and H be its subgroup, and let A be any subset of G.

(1), $\prod G_i$ is compact if and only if G_i is compact for every i.
(2), $\prod G_i$ is locally compact iff G_i is locally compact for every i and G_i is compact for almost all i.
(3), if H is open, then xH, Hx, H^{-1}, AH and HA are open.
(4), every open subgroup H is also closed, and every closed subgroup with the finite index is open.
(5), the quotient map $\rho : G \to G/H$ is open.
(6), the subgroup H is open if and only if the quotient space G/H is discrete.
(7), if $H \lhd G$, then G/H is a topological group.
(8), if G is compact and H is a closed subgroup, then H is compact.
(9), if G is compact, then the topological space G/H is compact.
(10), If H is compact and the quotient space G/H is compact, then G is compact.
For detailed proof, see [12].

3.1.1 Restricted direct products

Let $\{G_v : v \in \Lambda\}$ be a family of locally compact topological groups where Λ is a set of indices; let Λ_∞ be a finite subset of Λ. For each $v \in \Lambda \setminus \Lambda_\infty$, we fix a compact open subgroup H_v of G_v. We say a condition holds for *almost*

all elements of a set if it holds for all but finitely many elements. We define the *restricted direct product* of the G_v with respect to the H_v as follows

$$G = \prod_{v\in\Lambda}{}' G_v = \{(x_v) \,:\, x_v \in G_v \text{ with } x_v \in H_v \text{ for almost all } v\}.$$

We give G a topology by taking as a basis of open sets the sets $\prod N_v$ where the open sets $N_v \subset G_v$ for all v, and $N_v = H_v$ for almost all v. It is clear that the restricted topological product G of G_v is locally compact. For the detailed proof, see [12].

Let S be any finite subset of Λ containing Λ_∞ and consider the subgroup G_S defined by

$$G_S = \prod_{v\in S} G_v \prod_{v\notin S} H_v.$$

Then G_S is an open subset of G and the topology induced on G_S as a subset of X is the same as the product of a finite family of locally compact groups with a compact group; hence G_S is locally compact in the product topology.

3.1.2 The adele ring

Let k be an algebraic number field and v be any place. Let k_v be the completion of k with respect to the normalized valuation at the place v. For each nonarchimedean place v of k, let $\mathfrak{o}_v$ denote the ring of integers of k_v and U_v denote the unit group of k_v. The *adele ring* $\mathbb{A}_k$ is the restricted direct product of the k_v with respect to the $\mathfrak{o}_v$, that is

$$\mathbb{A}_k = \left\{(\alpha_v) \in \prod k_v \,:\, \alpha_v \in \mathfrak{o}_v \text{ for almost all } v\right\}.$$

The adele ring form a commutative ring under componentwise addition and multiplication. For any $\alpha \in k$, there is a natural continuous ring inclusion which is called the *diagonal map*

$$\begin{array}{ccc} k & \longrightarrow & \mathbb{A}_k \\ a & \longmapsto & (\alpha). \end{array}$$

We see at once that the diagonal map is injective because each map $k \to k_v$ is an inclusion. It enables us to identify k with a subring of $\mathbb{A}_k$. The image of the diagonal map is called the ring of *principal adeles*. Write $S_f = \{v \,:\, v < \infty\}$ all finite places and $S_\infty = \{v \,:\, v|\infty\}$ all infinite places of k. Let S be a finite set of places of k containing S_∞. The

$$\mathbb{A}_k^S = \prod_{v\in S} k_v \prod_{v\notin S} \mathfrak{o}_v$$

is called the *S-adeles.*

Lemma 3.1. *The field k is the discrete subring of $\mathbb{A}_k$.*

Proof. On account of the additive group structure of $\mathbb{A}_k$ it suffices to find a neighborhood U of 0 in $\mathbb{A}_k$ which contains no elements of k other than 0. Denote the set U by

$$\begin{aligned} U &= \prod_{v|\infty} N_v \prod_{v<\infty} \mathfrak{o}_v \\ &= \{(\alpha_v) : |\alpha_v|_v < 1 \text{ for } v|\infty \text{ and } \alpha_v \in \mathfrak{o}_v \text{ for } v < \infty\}, \end{aligned}$$

is an open set containing 0; and it contains no other elements of k by the Product Formula. □

Theorem 3.2. *$\mathbb{A}_k/k$ is compact.*

Proof. In order to prove this important result, we require the following preliminary result, which will be useful in its own right.

- $\mathbb{A}_k^{S_\infty} \cap k = \mathfrak{o}_k$ and $\mathbb{A}_k^S + k = \mathbb{A}_k$.

That $\mathbb{A}_k^{S_\infty} \cap k = \mathfrak{o}_k$ follows immediately from the fact that $\alpha \in k$ lies in $\mathfrak{o}_k$ if and only if $\mathrm{ord}_{\mathfrak{p}}(\alpha) \geq 0$ for all nonzero prime ideals $\mathfrak{p}$ in $\mathfrak{o}_k$.

Let $\alpha = (\alpha_v) \in \mathbb{A}_k$ and $T = \{v < \infty : \alpha_v \notin \mathfrak{o}_v\}$. Then T is finite set of places of k. By the approximation theorem, there exists $\beta \in k$ such that $|\beta - \alpha_v|_v \leq 1$ for $v \in T$ and $|\beta|_v \leq 1$ for $v \notin T \cup S_\infty$. It follows that $|\beta - \alpha_v| \leq \max\{|\beta|_v, |\alpha_v|_v\} \leq 1$ for $v \notin T \cup S_\infty$. We conclude that $(\beta - \alpha_v) \in \mathfrak{o}_v$ for $v \in S_f$, hence that $\beta - (\alpha_v) \in \mathbb{A}_k^S$, and finally that $\alpha \in \mathbb{A}_k^S + k$.

Now we turn to prove the theorem. We first have

$$\Big(\prod_{v\in S_\infty} k_v\Big)/\mathfrak{o}_k \cong \mathbb{R}^n/\mathfrak{o}_k$$

is compact because $\mathfrak{o}_k$ is a lattice. Therefore, we get that

$$\begin{aligned} \mathbb{A}_k/k &= (\mathbb{A}_k^{S_\infty} + k)/k \cong \mathbb{A}_k^{S_\infty}/(\mathbb{A}_k^{S_\infty} \cap k) \\ &= \mathbb{A}_k^{S_\infty}/\mathfrak{o}_k = \Big(\prod_{v\in S_\infty} k_v\Big)/\mathfrak{o}_k \prod_{v\in S_f} \mathfrak{o}_v \\ &= \big(\mathbb{R}^n/\mathfrak{o}_k\big) \prod_{v\in S_f} \mathfrak{o}_v \end{aligned}$$

is compact. □

• **Recall: Fundamental domain** Given a topological space X and a group G acting on it, the images of a single point under the group action form an orbit of the action. A fundamental domain D is a subset of the space which contains exactly one point from each of these orbits, i.e., for each $x \in X$, there exists $\alpha \in D$ and $g \in G$ such that $gx = \alpha$ and the choice of α is unique.

Corollary 3.3. *(Strong approximation theorem for adeles) The fundamental domain D for $k \setminus \mathbb{A}_k$ is given by*

$$D = D_\infty \prod_{v \in S_f} \mathfrak{o}_v,$$

where

$$D_\infty = \left\{ \sum_{i=1}^{n} a_i \omega_i \,:\, 0 \le a_i < 1 \right\}$$

with $\{\omega_i \,:\, 1 \le i \le n\}$ being integral basis of k. In particular, the $D = [0,1) \prod \mathbb{Z}_p$ is called the fundamental domain for $\mathbb{Q} \setminus \mathbb{A}_\mathbb{Q}$. That is, we have a disjoint union

$$\mathbb{A}_\mathbb{Q} = \bigcup_{\alpha \in \mathbb{Q}} (\alpha + D).$$

Proof. This corollary is to say that every element $\alpha \in \mathbb{A}_k$ could be expressed uniquely in the form $\beta + \gamma$, where $\beta \in k, \gamma \in \mathbb{A}_k^{S_\infty}$, and where the infinite component of γ is of the form

$$\sum_{i=1}^{n} a_i \omega_i, 0 \le a_i < 1.$$

From the proof of theorem 3.2 we know that every α could be expressed like that. Then we only need to prove the uniqueness.

If $\beta_1 + \gamma_1 = \beta_2 + \gamma_2$, then we know $\beta_1 - \beta_2 = \gamma_1 - \gamma_2$. Hence we know $\gamma_1 - \gamma_2 \in k$. As we know $\gamma_1 - \gamma_2 \in \mathbb{A}_k^{S_\infty}$, then we could have that $\gamma_1 - \gamma_2 \in \mathfrak{o}_k$. Hence we know $\gamma_1 = \gamma_2$ by the infinite component. Hence $\beta_1 = \beta_2$. □

3.1.3 The idele group

The *idele group* $\mathbb{I}_k$ is the restricted direct product of the $k_v^\times$ with respect to the U_v, that is

$$\mathbb{I}_k = \left\{ (\alpha_v) \in \prod k_v^\times \,:\, \alpha_v \in U_v \text{ for almost all } v \right\}.$$

It follows easily that the idele group $\mathbb{I}_k$ is the group of invertible elements of the adele ring $\mathbb{A}_k$. But although $\mathbb{I}_k$ is a subset of $\mathbb{A}_k$ we must not give it

the subspace topology, for $\alpha \mapsto \alpha^{-1}$ would not continuous in that topology. By the restricted direct product, a basis for the open sets in $\mathbb{I}_k$ is given by $\prod N_v$ where each N_v is open in $k_v^\times$ and $N_v = U_v$ for almost all v. For the convenience, we set $U_v = \{\pm 1\}$ if v is a real place and $U_v = S^1$ if v is a complex place.

As with adele, there is *diagonal map* $k^\times \longrightarrow \mathbb{I}_k$ defined by $a \longmapsto (\alpha)$. Thus we can identify $k^\times$ with a subset of $\mathbb{I}_k$ and its image are called the *principal ideles*. This map induces on $k^\times$ the subspace topology; and we can form $\mathbb{I}_k/K^\times$ and endow it with the quotient topology. The

$$\mathbb{I}_k^S = \prod_{v \in S} k_v^\times \prod_{v \notin S} U_v$$

is called the *S-ideles* where $S \supset S_\infty$ is a finite set of places of k. In particular, the element $\alpha \in \mathbb{I}_k^{S_\infty}$ is called the *unit ideles*.

Lemma 3.4. *The group $k^\times$ is the discrete subgroup of $\mathbb{I}_k$.*

Proof. Set $U = \{(\alpha_v) : |x_v - 1|_v < 1 \text{ for } v|\infty \text{ and } |x_v - 1|_v \leq 1 \text{ for } v < \infty\}$. Then U is an open neighborhood of 1 and $U \cap k^\times = \{1\}$. □

The factor group $\mathbb{A}_k/k$ is called the *adele class group*, and similarly the group $\mathbb{I}_k/k^\times$ is called the *idele class group*.

If $\alpha = (\alpha_v) \in \mathbb{I}_k$, define the *content* of the idele α by

$$|\alpha| = \prod_v |\alpha_v|_v.$$

It is clearly well-defined because $\alpha_v \in U_v$ for almost all v.

Lemma 3.5. *The map $\phi : \mathbb{I}_k \to \mathbb{R}_+^\times$ as above is continuous epimorphism where $\mathbb{R}_+^\times$ is the multiplicative group of positive real numbers. There is an exact sequence*

$$1 \to \mathbb{I}_k^1 \to \mathbb{I}_k \xrightarrow{\phi} \mathbb{R}_+^\times \to 1,$$

where $\mathbb{I}_k^1 = \ker \phi = \{\alpha \in \mathbb{I}_k : |\alpha| = 1\}$.

Proof. By the definition of the content map ϕ, we easily see ϕ is a homomorphisms. Define the two subgroups

$$\begin{aligned} I_1 &= \prod_{v \in S_\infty} k_v^\times \\ I_2 &= \{(\alpha_v) \in \prod_{v \in S_f} k_v^\times : \alpha_v \in U_v \text{ for almost all } v \in S_f\} \end{aligned}$$

considered as closed subgroup of $\mathbb{I}_k$ in the obvious way. Let $\phi_i (i = 1, 2)$ be the restriction of ϕ to $\mathbb{I}_k$. It suffices to show that ϕ_i is continuous, since $\mathbb{I}_k = I_1 \times I_2, \phi = \phi_1\phi_2$. But the map

$$\begin{array}{ccc} k_v^\times & \longrightarrow & \mathbb{R}_+^\times \\ \alpha & \longmapsto & |\alpha|_{v|\infty} \end{array}$$

are continuous and surjective, so ϕ_1 is continuous and surjective. The map ϕ_2 contains the open subgroup $\prod_{v\in S_f} U_v$ in its kernel, and is therefore continuous. The surjectivity of ϕ follows from the surjectivity of ϕ_1.

On the other hand, by the definition of $\mathbb{I}_k^1$, we know $\ker(\phi) = \mathbb{I}_k^1$. So there is an exact sequence

$$1 \to \mathbb{I}_k^1 \to \mathbb{I}_k \xrightarrow{\phi} \mathbb{R}_+^\times \to 1.$$

□

Lemma 3.6. *$\mathbb{I}_k^1/k^\times$ is closed both as a subset of $\mathbb{I}_k$ and as a subset of $\mathbb{A}_k$, and the two induced topologies on it coincide.*

Proof. To prove that $\mathbb{I}_k^1$ is closed in $\mathbb{A}_k$, it suffices to show that there exists $\mathbb{A}_k-$neighborhood W of α which does not meet $\mathbb{I}_k^1$ for any $\alpha = (\alpha_v) \in \mathbb{A}_k - \mathbb{I}_k^1$. Since $|\alpha| \neq 1$, there are two cases to consider.

First suppose that $|\alpha| > 1$. Then there is a finite set S including all infinite places and those finite prime $\mathfrak{p}$ which either Norm$\mathfrak{p} \leq 2|\alpha|$ or $|\alpha_\mathfrak{p}|_\mathfrak{p} > 1$. We can choose ε so small that $|w_v - \alpha_v|_v < \varepsilon$ for $v \in S$ implies $1 < \prod_{v\in S} |w_v|_v < 2|\alpha|$. Then define

$$W = \{w = (w_v) \,:\, |w_v - \alpha_v|_v < \varepsilon \text{ for } v \in S, w_v \in \mathfrak{o}_v \text{ for any others}\}.$$

This works because if $w \in W$, then either $|w_v|_v = 1$ for all $v \notin S$, in which case $|w| > 1$, i.e. $w \notin \mathbb{I}_k^1$, either $|w_{v_0}|_{v_0} < 1/2|alpha|$ for some $v_0 \notin S$, in which case

$$|w| = (\prod_{v\in S} |w_v|_v) \cdot |w_{v_0}| \cdots < 2|\alpha| \cdot 1/(2|\alpha|) \cdots < 1,$$

so $w \notin \mathbb{I}_k^1$.

If instead $|\alpha| < 1$. Then there is a finite set S including all infinite places and those finite prime $\mathfrak{p}$ with $|\alpha_\mathfrak{p}|_\mathfrak{p} > 1$, such that $\prod_{v\in S} |\alpha_v|_v < 1$. We can choose ε so small that $|w_v - \alpha_v|_v < \varepsilon$ for $v \in S$ implies $\prod_{v\in S} |w_v|_v < \frac{1}{2}(\prod_{v\in S} |\alpha_v|_v + 1) < 1$. Then define

$$W = \{w = (w_v) \,:\, |w_v - \alpha_v|_v < \varepsilon \text{ for } v \in S, w_v \in \mathfrak{o}_v \text{ for any others}\}.$$

Obviously, W does not meet $\mathbb{I}_k^1$.

Thus $\mathbb{I}_k^1$ is closed in $\mathbb{A}_k$. It is closed in $\mathbb{I}_k$, because the idelic topology on $\mathbb{I}_k$ is finer than he restriction of the adelic topology.

For the last assertion in the lemma it suffices to show that any $\mathbb{I}_k-$open subset of $\mathbb{I}_k^1$ is $\mathbb{A}_k-$open, the converse being trivial. Now let $W = \prod W_v$ be any basic $\mathbb{I}_k-$open set; we need to find a $\mathbb{A}_k-$open set W' such that $W \bigcap \mathbb{I}_k^1 = W' \bigcap \mathbb{I}_k^1$. By writing W as a union of smaller basic open sets if necessary, we can assume that each W_v is bounded; since for all but finitely many v we have $W_v = \mathfrak{o}_k^\times$ and therefore $|\alpha_v|_v = 1$ for all α_v in W_v, there is a constant C such that $|\alpha| = \prod |\alpha_v|_v < C$ for all α in W. Now write

$$W_v' = \begin{cases} \mathfrak{o}_\mathfrak{p} & \text{if } \mathfrak{p} \text{ is finite, } W_\mathfrak{p} = \mathfrak{o}_\mathfrak{p}^\times \text{ and } \mathrm{Norm}\mathfrak{p} > 2C \\ W_v & \text{otherwise} \end{cases} \tag{3.1}$$

Since the first of these happens for all but finitely many $\mathfrak{p}, W' = \prod W_v'$ open in $\mathbb{A}_k$; and $W' \bigcap \mathbb{I}_k^1 = W \bigcap \mathbb{I}_k^1$ as in the first part of the proof. □

There is a natural homomorphism map of $\mathbb{I}_k$ to the fractional ideals J_k of $\mathfrak{o}_k$. Indeed, given an idele $\alpha = (\alpha_v) \in \mathbb{I}_k$,

$$\eta : \alpha = (\alpha_v) \longmapsto (\alpha) = \prod_{v \in S_f} \mathfrak{p}_v^{\mathrm{ord}_\mathfrak{p}(\alpha_v)},$$

where $\mathfrak{p}_v$ is the prime ideal of $\mathfrak{o}_k$ with respect to the finite place v. It is easily seen that this map is onto and its kernel is

$$\ker \eta = \{(\alpha_v) \,:\, \mathrm{ord}_v(\alpha_v) = 0 \text{ for all finte } v\} = \mathbb{I}_k^{S_\infty}.$$

Thus we have an isomorphism

$$\mathbb{I}_k / k^\times \mathbb{I}_k^{S_\infty} \cong J_k / P_k = \mathcal{C}_k,$$

where P_k is the principal fractional ideals group and $\mathcal{C}_k$ is the ideal class group. By the product formula we have that $k^\times \subset \mathbb{I}_k^1$. The following result is of vital importance in class field theory.

Theorem 3.7. *$\mathbb{I}_k^1 / k^\times$ is compact.*

Proof. Let the map η be as above. Then it induces a homomorphism of $\mathbb{I}_k^1 / k^\times$ onto $\mathcal{C}_k$ whose kernel consists of the idele classes $\mathbb{I}_\infty^1 = H \times \prod_{v<\infty} U_v$ where

$$H = \Big\{ (\alpha_v) \in \prod_{v|\infty} k_v^\times \,:\, \prod_{v|\infty} |\alpha_v|_v = 1 \Big\}.$$

Indeed, the map η restricts only the nonarchimedean co0rdinates and we can adjust the archimedean coordinates to obtain $|\alpha| = 1$. Then we have the exact sequence

$$1 \to k^\times \mathbb{I}_\infty^1/k^\times \to \mathbb{I}_k^1/k^\times \to J_k/P_k \to 1.$$

Clearly, $\mathbb{I}_\infty^1 \cap k^\times = U_k$, and thus

$$\begin{aligned} k^\times \mathbb{I}_\infty^1/k^\times &= k^\times \Big(H \times \prod_{v<\infty} U_v\Big)/k^\times \\ &\cong \Big(H \times \prod_{v<\infty} U_v\Big)/\Big(H \times \prod_{v<\infty} U_v\Big) \cap k^\times \\ &= \Big(H \times \prod_{v<\infty} U_v\Big)/U_k \\ &\cong \Big(H/U_k\Big) \times \prod_{v<\infty} U_v. \end{aligned}$$

By Dirichlet unit theorem (1.12), we have the map

$$\lambda : H \to \mathbb{R}^{r_1+r_2}, \ \ (\alpha_v)_{v|\infty} \mapsto (\log |\alpha_v|_v)_{v|\infty}.$$

It follows that $\ker \lambda = \prod_{v|\infty} U_v$ is compact and $\lambda(U_k)$ is a lattice in $\lambda(H)$. Therefore H/U_k is compact, and then $\Big(H/U_k\Big) \times \prod_{v<\infty} U_v$ is compact. The theorem immediately follows from the finiteness of the class group. $\square$

To prove the above Theorem we used the finiteness of the ideal class group and Dirichlet's unit theorem. Conversely, from an independent proof of the above Theorem we can immediately these two results–which are the key structural theorems of the elementary theory. For such a proof, see Chapter II of [4].

Let $\{\epsilon_1, \ldots, \epsilon_{r-1}\}$ be fundamental system of units of the number field k and denote by

$$P = \left\{ \sum_{i=1}^{r-1} a_i \lambda(\epsilon_i) \ : \ 0 \le a_i < 1 \right\}.$$

We define

$$E_0 = \{\alpha = (\alpha_v) \in H \ : \ \lambda(\alpha) \in P \text{ and } 0 \le \arg \alpha_{v_0} < 2\pi/\omega\},$$

where ω is the order of the group of the roots of unity in k and v_0 is a fixed finite place of k. Let $\beta_1, \ldots, \beta_h$ be ideles such that $\eta(\beta_1), \ldots, \eta(\beta_h)$ are representatives of the ideal classes of $\mathcal{C}_k$.

Corollary 3.8. *(Strong approximation theorem for ideles) The fundamental domain D for $k^\times \setminus \mathbb{I}_k^1$ is given by*

$$D = \bigcup_{i=1}^{h} \beta_i \left(E_0 \prod_{v \in S_f} U_v \right).$$

That is,

$$\mathbb{I}_k = \bigcup_{\alpha \in k^\times} \alpha D$$

is a disjoint union.

In particular, the $D = (0, \infty) \prod \mathbb{Z}_p^\times$ is the fundamental domain for $\mathbb{Q}^\times \setminus \mathbb{I}_\mathbb{Q}$. That is, we have a disjoint union

$$\mathbb{I}_\mathbb{Q} = \bigcup_{\alpha \in \mathbb{Q}^\times} \alpha D.$$

3.2 Idele class group and ray class group

3.2.1 Idele class groups

3.2.2 Ray class group

3.2.3 Hecke characters

3.3 Characters on local and global fields

Let G be a topological group. A *quasi-character* χ of G is a continuous homomorphism from G into $\mathbb{C}^\times$. In particular, A quasi-character is called *(unitary) character* if its image is in the circle group $S^1 = \{z \in \mathbb{C} : |z| = 1\}$. We shall show that any quasi-character can be written uniquely as a unitary character times a real power of the norm, so there is no big difference between the two definitions.

3.3.1 Duality theory

Let G be a locally compact abelian group. The set $\widehat{G}$ of all characters of G forms a multiplicative group in an obvious way,

$$\chi_1\chi_2(g) = \chi_1(g)\chi_2(g), \;\; g \in G,$$

called the *character group* or *dual group* of G. We can topologize $\widehat{G}$ as follows. It is said to *compact-open topology*. Fix a character χ_0 of G; then a basis for the open neighbourhood $U(\chi_0, \epsilon)$ of χ_0 in $\widehat{G}$ is given by

$$U_K(\chi_0, \epsilon) = \{\chi \in \widehat{G} : |\chi(g) - \chi_0(g)| < \epsilon, \text{ for any } g \in K\},$$

where $\epsilon > 0$ is in $\mathbb{R}$ and K is any compact subset of G. We have the following fundamental facts, for detailed proof see [12] or [18].

(1), The group $\widehat{G}$ is a locally compact abelian group. If G is compact, then $\widehat{G}$ is discrete, and if G is discrete, then $\widehat{G}$ is compact.

(2), (Pontryagin Duality Theorem) The map that associated to $g \in G$ the character $\widehat{\chi}_g : \; \chi \mapsto \chi(g)$ of $\widehat{G}$ is an isomorphism of the topological groups G and $\widehat{\widehat{G}}$.

(3), If H is closed subgroup of G and the annihilator $H^\perp = \{\chi \in \widehat{G} : \chi(H) = 1\}$, then $H^\perp$ is closed in $\widehat{G}$ and there are canonical isomorphisms $\widehat{H} \cong \widehat{G}/H^\perp$ and $\widehat{G/H} \cong H^\perp$.

(4), Any character on a closed subgroup of G can be extended (non-uniquely) to the whole of G.

(5), If G is compact, or if every element of G is of finite order, then every quasi-character of G is a character.

(6), The dual group of the direct product $G_1 \times G_2$ is isomorphism to $\widehat{G_1 \times G_2}$.

The G is called the *self-dual* if there is a topological isomorphism from G onto $\widehat{G}$. We shall show that k_v and $\mathbb{A}_k$ are self-dual locally compact abelian topological groups.

3.3.2 Characters on local fields

Let k be a locally compact topological field. Then it is a group under addition, and at the same time the set of elements of k other than 0 forms a group under multiplication. Henceforth we denoted by k^+ is the additive group of k, and by $k^\times$ its multiplication group. Let χ be an additive character of a local field k^+, i.e., a continuous homomorphism such that

$$\chi(x+y) = \chi(x)\chi(y), \text{ for any } x, y \in k^+.$$

Let ψ be a multiplicative character of a local field $k^\times$, i.e., a continuous homomorphism such that

$$\psi(xy) = \psi(x)\psi(y), \text{ for any } x, y \in k^\times.$$

A topological group G is said to have *no small subgroup* if there exists a neighborhood U of the identity that contains no nontrivial subgroup of G; otherwise G is said to have small subgroup. A basic example of a topological group with no small subgroup is the general linear group over the complex numbers. In particular, the circle S^1 has no small subgroups. The subgroups $\{1+\mathfrak{p}_\mathfrak{p}^m\}$ are small subgroups of nonarchimedean local field $k_\mathfrak{p}^\times$, that is, any neighborhood of the identity in $k_\mathfrak{p}^\times$ contains some $1+\mathfrak{p}_\mathfrak{p}^n$.

The complex valued function $f(g)$ on a topological group G is *locally constant* if it is constant in some neighborhood of each point.

Lemma 3.9. *Let G be a totally disconnected locally compact topological group. Then any quasi-character χ is locally constant.*

Proof. Let $\{H_n\}$ be a basis of neighborhood of the identity consisting of open and compact subgroups of G. Then $\chi(H_1)$ is compact subgroup of $\mathbb{C}^\times$ and $\mathbb{C}^\times \subset S^1$. Denote the neighborhood $\mathcal{N}$ of 1 in S^1 by $\{z \in S^1 : \Re z > 1/2\}$. Then $\chi^{-1}(\mathcal{N})$ is a neighborhood of the identity of G. Hence we have $H_n \subset \chi^{-1}(\mathcal{N})$ for sufficiently large n. It follow that $\chi(H_i)$ is a subgroup of S^1 contained in $\mathcal{N}$ and must therefore be trivial because $\mathcal{N}$ contains no nontrivial subgroups. □

Let $k_\mathfrak{p}$ be a local field and $\chi_\mathfrak{p}$ be a nontrivial additive character. Then $\chi_\mathfrak{p}$ is locally constant, i.e., there exists $\mathfrak{p}_\mathfrak{p}^m$ such that $\chi_\mathfrak{p}(\mathfrak{p}_\mathfrak{p}^m) = \chi_\mathfrak{p}(0) = 1$. Let m be the smallest integer such that $\chi_\mathfrak{p}(\mathfrak{p}_\mathfrak{p}^m) = 1$. We call $\mathfrak{f}_\mathfrak{p} = \mathfrak{p}_\mathfrak{p}^m$ the *conductor* of $\chi_\mathfrak{p}$. Similarly, let $\psi_\mathfrak{p}$ be a nontrivial multiplicative character of $k_\mathfrak{p}^\times$. Let m be the smallest integer such that $\psi_\mathfrak{p}(1+\mathfrak{p}_\mathfrak{p}^m) = 1$. We also call $\mathfrak{f}_\mathfrak{p} = \mathfrak{p}_\mathfrak{p}^m$ the *conductor* of $\psi_\mathfrak{p}$. If $m = 0$, then by define, $\mathfrak{f} = \mathfrak{o}_\mathfrak{p}$.

♠ Additive characters

Lemma 3.10. *Let k_v be a nonarchimedean local field. Then every quasi-character χ_v of k_v^+ is a character.*

Proof. Let $\mathfrak{o}_v$ be the ring of integers of k_v. Then the restrict of χ_v to $\mathfrak{o}_v$ must be a character because $\mathfrak{o}_v$ is compact. But every element of $k_v^\times$ can be written the form α/m with $\alpha \in \mathfrak{o}_v$ and $m \in \mathbb{N}$, and since $|\chi(\alpha/m)|^m = |\chi(\alpha)| = 1$ we get $|\chi(\alpha/m)| = 1$. □

Theorem 3.11. *Let k_v be any local field. Let χ be a fixed nontrivial additive character of k_v^+. For each $\alpha \in k_v^+$ the map $\chi_\alpha(x) = \chi(x\alpha)$ is an additive character of k_v^+, and the map $\alpha \mapsto \chi_\alpha$ of k_v^+ into $\widehat{k_v^+}$ is a topological group isomorphism. That is, the local field k_v is self-dual.*

Proof. The map $x \mapsto \chi_\alpha(x)$ is a continuous homomorphism of k_v^+ into S^1, since the map $x \mapsto x\alpha$ for fixed α is a continuous homomorphism of k_v^+ into itself.

As is easily seen, $\varphi : \alpha \mapsto \chi_\alpha$ is a injective group homomorphism of k_v^+ into $\widehat{k_v^+}$.

The topology in $\widehat{k_v^+}$ is defined by the neighborhood system of the unit (i.e., trivial) character χ_0, which consists of the sets

$$U(\epsilon, B) = \{\chi' \in \widehat{k_v^+} : |\chi'(x) - 1| < \epsilon \quad \text{for any } x \in B\},$$

where $\epsilon > 0$ is in $\mathbb{R}$, and B is a compact subset of $\widehat{k_v^+}$. It suffices to take for B the sets of the form

$$B_m = \{x \in \widehat{k_v^+} : |x| \le m\}$$

with $m \in \mathbb{R}, m > 0$.

To establish the continuity of φ we must show that for every $U(\epsilon, B_m)$ there exists a neighborhood U of 0 in $\widehat{k_v^+}$ with $\varphi(U) \subseteq U(\epsilon, B_m)$. Let $\delta > 0$ with $|\chi(\beta) - 1| < \epsilon$ for $|\beta| < \delta$. Then

$$U = \{\alpha \in k_v^+ : |\alpha| < \frac{\delta}{m}\}$$

provides what we need to show.

The map φ^{-1} of $\varphi(k_v^+)$ onto k_v^+ is likewise continuous. For this we must show that for every $\delta > 0$ there exist $\epsilon > 0$ and $m > 0$ with $|\varphi^{-1}(\chi_\alpha)| < \delta$ for $\chi_\alpha \in \varphi(k_v^+) \cap U(\epsilon, B_m)$.

Let x_0 be an element of k_v^+ with $\chi(x_0) \neq 1$. We set

$$\epsilon = |\chi(x_0) - 1|, \qquad m = \frac{|x_0|}{\delta}.$$

For $\alpha \in k_v^+$ with $\varphi(\alpha) \in U(\epsilon, B_m)$ we have $x_0 \notin \alpha B_m$ and thus $|x_0| > |\alpha| m$; that is, $|\alpha| < \delta$.

We have proved that the topological groups k_v^+ and $\varphi(k_v^+)$ are isomorphic. When k_v^+ is complete, then so is $\varphi(k_v^+)$, and it is therefore closed in $\widehat{k_v^+}$). By Pontryagin duality theory, there exists a one to one relation between the closed subgroup of k_v^+ and $\widehat{k_v^+}$. Here there corresponds to $\varphi(k_v^+)$ in k_v^+ the subgroup of $x \in k_v^+$ with $\chi_\alpha(x) = 1$ for all $\alpha \in k_v$. Since χ is nontrivial, this holds only for $x = 0$. It follows that $\varphi(k_v^+)$ is equal to $\widehat{k_v^+}$). □

For any local field k_v, we may construct the *standard character* $\chi_v \in \widehat{k_v^+}$. For simplicity, we set $e(z) = e^{2\pi i z}$ for $z \in \mathbb{C}$.

• **Case** $k_v = \mathbb{R}$**:** For any $\alpha \in \mathbb{R}$, set $\lambda_p(\alpha) = -\alpha \mod \mathbb{Z}$ and $\chi_v(\alpha) = e(-\alpha) = e(-\lambda_p(\alpha))$.

• **Case** $k_v = \mathbb{C}$**:** For any $z \in \mathbb{C}$, set $\lambda_p(z) = -2\Im z \mod \mathbb{Z}$ and $\chi_v(z) = e(-2\Im z) = e(-\lambda_p(z))$.

• **Case** $k_v = \mathbb{Q}_p$, $p < \infty$**:** For any $\alpha \in \mathbb{Q}_p$, choose $m \in \mathbb{Z}$ so that $p^m \alpha \in \mathbb{Z}_p$. Since $\mathbb{Z}$ is dense in $\mathbb{Z}_p$, there exists $a \in \mathbb{Z}$ such that

$$\left| \alpha - \frac{a}{p^m} \right|_p \leq 1.$$

Set $\lambda_p(\alpha) = a/p^m (\mathrm{mod}\, \mathbb{Z})$ which is independent of the choice of m and a. Clearly, λ_p is a nontrivial continuous homomorphism of $\mathbb{Q}_p^+$ into $\mathbb{R}/\mathbb{Z}$ in both cases. Denote $\chi_p \in \widehat{\mathbb{Q}_p^+}$ by

$$\chi_p(\alpha) = e(\lambda_p(\alpha)).$$

It is clear that χ_p is trivial on $\mathbb{Z}_p$.

• **Case** $k_v/\mathbb{Q}_p$**,** $p < \infty$**:** Denote $\chi_v \in \widehat{k_v^+}$ by $\chi_v = e \circ \lambda_p \circ \mathrm{Tr}_{k_v/\mathbb{Q}_p}$, i.e.,

$$\chi_v(\alpha) = e(\lambda_p(\mathrm{Tr}_{k_v/\mathbb{Q}_p}(\alpha))).$$

By Theorem (3.11), we immediately obtain that, for any fixed $\alpha \in k_v$, the map

$$\begin{array}{ccc} k_v & \longrightarrow & \widehat{k_v^+} \\ \alpha & \longmapsto & \chi_\alpha \end{array}$$

is an algebraic and topological isomorphism where $\chi_\alpha(x) = e(\lambda_p(\mathrm{Tr}_{k_v/\mathbb{Q}_p}(x\alpha)))$ is a nontrivial additive character of k_v^+.

♠ Multiplicative characters

For any $\alpha \in k_v^\times$, we have that α can be represented uniquely in the form

$$\begin{aligned} v|\infty: &\quad \alpha = ur, \ \ u \in U_v, r > 0; \\ v < \infty: &\quad \alpha = u\pi_v^r, \ \ u \in U_v, r \in \mathbb{Z}, \end{aligned} \tag{3.2}$$

where π_v is an uniformizing parameter at the place v; that is, we have

$$k_v^\times \cong U_v \times \mathbb{R}_+^\times \quad \text{or} \quad k_v^\times \cong U_v \times \mathbb{Z} \tag{3.3}$$

according as v is archimedean or not. By the fact $\widehat{G_1} \times \widehat{G_2} \cong \widehat{G_1 \times G_2}$, we firstly shall consider the character on the unit group U_v.

Let ψ_v be a multiplicative character of a local field $k_v^\times$. The quasi-character ψ_v is called the *unramified* at the place v if it is trivial on U_v; otherwise we called it *ramified*.

Lemma 3.12. *The unramified quasi-characters ψ_v are the form $\psi_v : \alpha \mapsto |\alpha|_v^s$, where s is any complex number; s is determined by ψ_v if v is archimedean and s is determined only mod $2\pi i/\log N\mathfrak{p}$ if v is $\mathfrak{p}$-adic.*

Proof. It is clear that the quasi-character $\psi_v(\alpha) = |\alpha|_v^s$ are unramified. Conversely, let χ be an unramified quasi-character. Then $\psi_v(\alpha)$ depends only on the value group $\Gamma_v = \{|\alpha|_v : \alpha \in k_v^\times\}$. The value group $\Gamma_v = \mathbb{R}_+^\times$ if v is infinite and Γ_v is the infinite cyclic group generated by $N\mathfrak{p}_v$.

By (3.3), we have $\psi_v(\alpha) = |\alpha|_v^{it}$, $t \in \mathbb{R}$, since every character of $\mathbb{R}_+^\times$ is of the form $\alpha \mapsto \alpha^{it}$, $t \in \mathbb{R}$, see exercises. If v is a finite place, then

$$|\alpha|_v^s = e^{s \log |\alpha|_v} = e^{-\mathrm{ord}_v(\alpha) s \log N(\mathfrak{p}_v)}.$$

Hence s is determined up to addition of a multiple of $2\pi i/\log N\mathfrak{p}_v$. □

Lemma 3.13. *Let $\alpha \in k_v^\times$ be written as the form (3.2). Every quasi-character ψ_v of $k_v^\times$ has the form*

$$\psi_v(\alpha) = c_v(u)|\alpha|_v^s, \tag{3.4}$$

where c_v is a character of U_v and $s \in \mathbb{C}$.

Proof. It is clear that every mapping of the form (3.4) is a quasi-character. Conversely, let ψ_v be an arbitrary quasi-character, and let c_v be the restriction of ψ_v on U_v. Then c_v is a character since U_v is compact. Furthermore, $\psi_v(\alpha)c_v(\alpha)^{-1}$ is an unramified quasi-character of $k_v^\times$. The result immediately follows the above lemma. □

Suppose that c_v is a character of U_v for any place v.

(1) v **is a real place.** We have $U_v = \{\pm 1\}$. There are just two classes of characters on U_v:

$$c_v(x) = 1 \quad \text{or} \quad c_v(x) = \text{sign}(x).$$

It follows that we have, for $x \in \mathbb{R}$,

$$\psi_v(x) = |x|^{s_v} \quad \text{or} \quad \psi_v = \text{sign}(x)|x|^{s_v}, \tag{3.5}$$

for some pure imaginary s_v.

(2) v **is a complex place.** We have $U_v = S^1$. It is well know that $\widehat{S^1} \cong \widehat{\mathbb{R}/\mathbb{Z}} \cong \mathbb{Z}$, that is, any character of S^1 is the form $c_v : e^{i\theta} \mapsto e^{im\theta}$ for any $m \in \mathbb{Z}$. It follows that we have, for $z \in \mathbb{C}$,

$$\psi_v(z) = \left(\frac{z}{|z|}\right)^{n_v} |z|^{s_v}, \tag{3.6}$$

for some pure imaginary s_v and for some integer n_v.

(3), v **is a finite place with respect to a prime ideal $\mathfrak{p}$.** Let $\mathfrak{p}_\mathfrak{p}^m$ be the conductor of c_v, i.e., $c_v(1 + \mathfrak{p}_v^m) = 1$ and $c_v(1 + \mathfrak{p}_v^{m-1}) \neq 1$. $U_v/(1 + \mathfrak{p}_v^m)$ is the finite group with the order $N\mathfrak{p}^{r-1}(N\mathfrak{p} - 1)$ because U_v is compact and $1 + \mathfrak{p}_\mathfrak{p}^m$ is open. Thus c_v is essentially a character of this finite group.

3.3.3 Characters on global fields

Now let us consider the dual groups of the adeles and ideles. Since both the adels and ideles are constructed as restricted direct products, let us consider the general problem of calculating the dual of a restricted direct product

$$G = \prod{}' G_v, \text{ with respect to the compact open subgroup } H_v.$$

Let $\chi \in \widehat{G}$. The the restricted of χ to G_v is a character χ_v of G_v, i.e., for any $\alpha_v \in G_v$, denote χ_v by

$$\chi_v(\alpha_v) = \chi(\alpha|_v), \quad \text{where } \alpha|_v = (1, \dots, 1, \alpha_v, 1, \dots).$$

Proposition 3.14. *(1), Let $\chi \in \widehat{G}$ and χ_v be as above. Then $\chi_v(H_v) = 1$ for almost all v and for $\alpha = (\alpha_v) \in G$,*

$$\chi(\alpha) = \prod_v \chi_v(\alpha_v).$$

(2), Conversely, let $\chi_v \in \widehat{G_v}$ and $\chi_v(H_v) = 1$ for almost all v. Then for any $\alpha = (\alpha_v) \in G$,

$$\chi(\alpha) = \prod_v \chi_v(\alpha_v)$$

defines a character of G.

Proof. (1), Let U be a neighborhood of 1 in S^1 that contains no subgroups of S^1 other than $\{1\}$ and let N be a neighborhood of the identity in G such that $\chi(N) \subset U$ and such that

$$N = \prod_{v\in S} N_v \prod_{v\notin S} H_v,$$

where S is a finite set of v and N_v is a neighborhood of the identity of G_v. Hence the restrict χ_v of χ on G_v satisfies $\chi_v(H_v) = 1$ for $v \notin S$.

For any given $\alpha = (\alpha_v) \in G$, let T be a finite set of v containing all v for which (1) $\alpha_v \notin H_v$, (2), $v \in S$, or (3) H_v undefined. Then

$$\alpha = (\alpha_v) = (\alpha_v; \underbrace{1, \ldots, 1}_{v\notin T})(\underbrace{1, \ldots, 1}_{v\in T}; \alpha_v) \in \prod_{v\in T} G_v \prod_{v\notin T} H_v$$

and $\chi_v(H_v) = 1$ for any $v \notin T$. It follows that

$$\begin{aligned} \chi(\alpha) &= \chi((\alpha_v; \underbrace{1, \ldots, 1}_{v\notin T}))\chi((\underbrace{1, \ldots, 1}_{v\in T}; \alpha_v)) \\ &= \prod_{v\in T} \chi_v(\alpha_v) = \prod_v \chi_v(\alpha_v). \end{aligned}$$

(2),

□

For each v, we define $H_v^\perp = \{\chi_v \in \widehat{G_v} : \chi_v(H_v) = 1\}$. Since H_v is open in G_v, we have G_v/H_v is discrete, hence that $H_v^\perp \cong \widehat{G_v/H_v}$ is compact. Also since H_v is compact in G_v, we have $\widehat{G_v}/H_v^\perp \cong \widehat{H_v}$ is discrete, hence that $H_v^\perp$ is open. Thus for almost all v, the subgroups $H_v^\perp$ of $\widehat{G_v}$ are compact and open in $\widehat{G_v}$. Thus we can define the restricted direct product of $\widehat{G_v}$ with respect to $H_v^\perp$

$$\prod{}' \widehat{G_v} = \left\{(\chi_v) \in \prod \widehat{G_v} : \chi_v \in H_v^\perp \text{ for almost all } v\right\}.$$

Theorem 3.15. *The map $\chi \mapsto (\chi_v)$ is canonically isomorphic of the topological group $\widehat{G}$ into $\prod' \widehat{G_v}$.*

Proof. From Prop 3.13, We can know that the mapping $\chi \to (\chi_v)$ is an algebraic isomorphism. Let us show that it is also a topological isomorphism. Now $\chi \in \widehat{G}$ is close to the identity character $\Leftrightarrow \chi(B)$ is contained in a small neighborhood of 1, for $B \subseteq G$ some large compact set. Without loss of generality, assume that B is of the form $\prod_{v\in S} N_v \prod_{v\notin S} P_v$, where $N_v \subseteq G_v$ compact, S is a finite set of v. Assume that S is so large that if $\chi_v(H_v) \neq 1$, then $v \in S$. Then χ is close to the identity character $\Leftrightarrow \chi(B)$ is close to 1 $\Leftrightarrow \chi_v(N_v)$ is close to 1, for $v \in S$; $\chi_v(H_v) = 1$, for $v \notin S \Leftrightarrow \chi_v$ close to the identity character in $\widehat{G_v}$, for $v \in S$; $\chi_v \in H_v^{\perp}$, for $v \notin S \Leftrightarrow \chi = (\chi_v)$ is close to the identity in $\prod'\widehat{G_v}$. □

As a particular case of Theorem (3.15), let $G = \mathbb{A}_k$, the adele ring of a number field k. Then $G_v = k_v$, $H_v = \mathfrak{o}_v$ and

$$\begin{aligned}
\mathfrak{o}_v^{\perp} &= \{\chi_v \in \widehat{k_v} \,:\, \chi_v(\mathfrak{o}_v) = 1\} \\
&= \{\alpha \in k_v \,:\, \chi_\alpha(\mathfrak{o}_v) = 1\} \\
&= \{\alpha \in k_v \,:\, e(\lambda_p(\mathrm{Tr}_{k_v/\mathbb{Q}_p}(\alpha\mathfrak{o}_v))) = 1\} \\
&= \{\alpha \in k_v \,:\, \lambda_p(\mathrm{Tr}_{k_v/\mathbb{Q}_p}(\alpha\mathfrak{o}_v)) \subset \mathbb{Z}\} \\
&= \{\alpha \in k_v \,:\, \mathrm{Tr}_{k_v/\mathbb{Q}_p}(\alpha\mathfrak{o}_v) \subset \mathbb{Z}_p\} \\
&= \mathfrak{D}_v^{-1}.
\end{aligned}$$

Since there is only a finite number of primes that ramify in the extension $k/\mathbb{Q}$, we have $\mathfrak{o}_v^{\perp} = \mathfrak{D}_v^{-1} = \mathfrak{o}_v$ for almost all v. Thus

$$\widehat{\mathbb{A}_k} = \prod\nolimits_v' \widehat{k_v} = \prod\nolimits_v' k_v = \mathbb{A}_k,$$

because k_v is self-dual. The isomorphism between $\mathbb{A}_k$ and $\widehat{\mathbb{A}_k}$ can be explicitly realized as follows. Define the continuous additive mapping

$$\begin{aligned}
\Lambda :\, \mathbb{A}_k &\longrightarrow \mathbb{R}/\mathbb{Z} \\
(\alpha_v) &\longmapsto \sum_v \lambda_p(\mathrm{Tr}_{k_v/\mathbb{Q}_p}(\alpha_v)).
\end{aligned}$$

This sum is well defined since $\alpha_v \in \mathfrak{o}_v = \mathfrak{D}_{k_v/\mathbb{Q}_p}^{-1}$ for almost all v, so $\lambda_p(\mathrm{Tr}_{k_v/\mathbb{Q}_p}(\alpha_v)) = 0$ for almost all v. The character χ_α corresponding to $\alpha = (\alpha_v)$ in $\mathbb{A}_k$ is given by, for any $\beta = (\beta_v) \in \mathbb{A}_k$,

$$\begin{aligned}
\chi_\alpha(\beta) &= \prod_v \chi_v(\alpha_v\beta_v) = \prod_v e\left(\lambda_p(\mathrm{Tr}_{k_v/\mathbb{Q}_p}(\alpha_v\beta_v))\right) \\
&= e\left(\sum \lambda_p\left(\mathrm{Tr}_{k_v/\mathbb{Q}_p}(\alpha_v\beta_v)\right)\right) = e\left(\Lambda(\alpha\beta)\right).
\end{aligned}$$

Corollary 3.16. *The character χ_α is trivial on k if and only if α is in k. In particular, we have $\widehat{\mathbb{A}_k/k} \cong k$, that is, given any non-trivial character χ on $\mathbb{A}_k/k$, all characters on $\mathbb{A}_k/k$ are of the form $x \mapsto \chi(\alpha x)$ for some $\alpha \in k$.*

Proof. Suppose first that α, β are both in k. We have

$$-\lambda_\infty \sum_{v|\infty} \mathrm{Tr}_{k_v/\mathbb{Q}}(\alpha\beta) = \sum_p \lambda_p \sum_{v|p} \mathrm{Tr}_{k_v/\mathbb{Q}_p}(\alpha\beta)$$

Let $G = \{\alpha \in \mathbb{A}_k : \chi_\alpha(k) = 1\}$. Then $G \supset k$ is a k-vector space; thus G/k is a subspace of $\mathbb{A}_k/k$. But the latter is compact, so G/k is trivial. $\square$

3.4 Harmonic Analysis on Adele groups

3.4.1 Haar measures and Haar integrals

Let G be a locally compact topological group, and denote by $\mathcal{B}$ the sigma algebra generated by the closed compact subsets of G. A *left Haar measure* on G is a measure μ on $\mathcal{B}$ which is:

(1), $\mu(E) = \inf\{\mu(U) : U \supset E, U \text{ open}\}$ *for all sets* E.
(2), $\mu(E) = \sup\{\mu(K) : K \subset E, K \text{ compact}\}$ *for all open sets* E.
(3), $\mu(gE) = \mu(E)$ *for all sets* E *and* $g \in G$.
(4), $\mu(K) < \infty$ *for all compact sets* K.
(5), $\mu(E) > 0$ *for all non-empty open sets* E.

Let μ be a left Haar measure of G and $L_1(G)$ be the linear space of measurable complex valued functions on G with respect to $\mathrm{d}\mu$. In this section we shall be mainly interested in locally compact abelian groups. Left and right Haar measure are the same thing. The main result about Haar measure is the following.

Theorem *Let* G *be a locally compact topological group. There exists on* G *a left Haar measure* μ *uniquely determined up to a constant. There is a corresponding integral* $\int_G f(g)\mathrm{d}\mu(g)$ *with the property*

$$\int_G f(g_0 g)\mathrm{d}\mu(g) = \int_G f(g)\mathrm{d}\mu(g).$$

Now let k_v be a locally compact topological field. Associated with k_v there are two topological groups: k_v^+ with the addition law and $k_v^\times$ with the multiplication law. The corresponding Haar measure μ^+ and $\mu^\times$ are different.

Let α be any non-zero element of k_v and S be any measurable set of k_v. Then the map $x \mapsto \alpha x$ is an automorphism of the additive group k_v and $\mu^+(\alpha S)$ is also an additive Haar measure. Then we have

$$\mu^+(\alpha S) = \mathrm{mod}_v(\alpha)\mu^+(S)$$

by the uniqueness of Haar measure, where the constant $\mathrm{mod}_v(\alpha)$ does not depend on the choice of S and μ^+. Clearly, we have

$$\mathrm{mod}_v(\alpha\beta) = \mathrm{mod}_v(\alpha)\mathrm{mod}_v(\beta).$$

Lemma 3.17. *Let the notations and assumptions be as above. Then* $\mathrm{mod}_v(\alpha) = |\alpha|_v$ *or symbolically* $\mathrm{d}^+\alpha x = |\alpha|_v \mathrm{d}^+ x$.

Proof. It is clear that the result is true for $v|\infty$. For nonarchimedean local fields, we take $S = \mathfrak{o}_v$ and $\mathrm{ord}_v\alpha = m$ with $m \geq 0$. The additive subgroup $\alpha\mathfrak{o}_v = \mathfrak{p}_v^m$ of $\mathfrak{o}_v$ has index $(N\mathfrak{p}_v)^m$ and $\mu(\mathfrak{o}_v)$ is finite because $\mathfrak{o}_v$ is open and compact. Hence we get $\mu(\mathfrak{o}_v) = (N\mathfrak{p}_v)^m\mu(\alpha\mathfrak{o}_v)$; it follows that $\mathrm{mod}_v(\alpha) = N\mathfrak{p}_v{}^{-m} = |\alpha|_v$. □

♠ **Additive Haar Measures:** By the fundamental theorem of Haar measures on locally compact abelian groups, we know that Haar measures are unique up to scalars. It will be convenient for us to set:

- v **is real.** d^+x is standard Lesbegue measure for $\mathbb{R}$.
- v **is complex.** d^+z is twice standard Lesbegue measure for $\mathbb{C}$.
- v **is finite.** We choose the Haar measure on k_v^+ such that $\mu(\mathfrak{o}_v) = |d_v|^{-1/2} = (N\mathfrak{D}_v)^{-1/2}$ where d_v is the discriminant of the extension $k_v/\mathbb{Q}_p$ and $\mathfrak{D}_v$ is the local different of the extension $k_v/\mathbb{Q}_p$.

It is called the *normalized additive measure* on k_v^+.

♠ **Multiplicative Haar Measures:** Let μ^+ be any additive Haar measure of k_v^+. Then the measure

$$\mu^\times(S) = \int_S \frac{\mathrm{d}^+x}{|x|_v}$$

is a multiplicative measure of $k_v^\times$. Indeed, We have, for any measurable set S of $k_v^\times$ and any $\alpha \in k_v^\times$,

$$\mu^\times(\alpha S) = \int_{\alpha S} \frac{\mathrm{d}^+x}{|x|_v} = \int_S \frac{\mathrm{d}^+\alpha x}{|\alpha x|_v} = \int_S \frac{\mathrm{d}^+x}{|x|_v} = \mu^\times(S)$$

by Lemma (3.17). We normalized the multiplicative measure on $k_v^\times$ such that

$$\mathrm{d}^\times x = \begin{cases} \frac{\mathrm{d}^+x}{|x|_v}, & \text{if } v|\infty; \\ \frac{N\mathfrak{p}_v}{N\mathfrak{p}_v - 1}\frac{\mathrm{d}^+x}{|x|_v}, & \text{if } v < \infty. \end{cases}$$

Lemma 3.18. *For $v < \infty$, we have $\mu^\times(U_v) = \int_{U_v} \mathrm{d}^\times x = |d_v|^{-1/2}$.*

Proof.

$$\begin{aligned} \mu^+(\mathfrak{o}_v) &= \int_{\mathfrak{o}_v} \mathrm{d}^+x = \sum_{m\geq 0} \int_{\pi_v^m U_v} \mathrm{d}^+x \\ &= \sum_{m\geq 0} \int_{U_v} \mathrm{d}^+\pi_v^m u = \sum_{m\geq 0} (N\mathfrak{p}_v)^{-m} \int_{U_v} \mathrm{d}^+u \\ &= \mu^\times(U_v). \end{aligned}$$

□

♠ **Measures on Restricted Direct Products:** We wish to create a measure on the restricted direct product $G = \prod' G_v$ with respect to the compact open subgroups H_v. Let μ_v be measures on the G_v (represented by $\mathrm{d}x_v$ in an integral), with $\mu(H_v) = 1$ for almost all v. Let S be a finite set of v which includes all v for which H_v is undefined and all v for which $\mu(H_v) \neq 1$. Let

$$G_S = \prod_{v \in S} G_v \times \prod_{v \notin S} H_v = \prod_{v \in S} G_v \times G^S.$$

Then G^S is compact and G_S is an open subgroup of G. Choose a Haar measure $\mathrm{d}x^S$ on G^S so that $\mu^S(G^S) = 1$. Given G_S the product measure

$$\mathrm{d}x_S = \prod_{v \in S} \mathrm{d}x_v \times \mathrm{d}x^S.$$

Since G_S is an open subgroup of G, a Haar measure $\mathrm{d}x$ on G is now determined by the requirement that $\mathrm{d}x = \mathrm{d}x_S$ on G_S.

Let $T \supset S$ be a larger set of indices. Then $G_S \subset G_T$, and we have only to check that the $\mathrm{d}x_T$ constructed with T coincides on G_S with the $\mathrm{d}x_S$ constructed with S. Now one sees form the decomposition

$$G^S = \prod_{v \notin S} H_v = \prod_{v \in T \setminus S} H_v \times G^T$$

that $\mathrm{d}x^S = \prod_{v \in T \setminus S} \mathrm{d}x_v \times \mathrm{d}x^T$. Therefore

$$\mathrm{d}x_S = \prod_{v \in S} \mathrm{d}x_v \times \mathrm{d}x^S = \prod_{v \in S} \mathrm{d}x_v \prod_{v \in T \setminus S} \mathrm{d}x_v \times \mathrm{d}x^T = \prod_{v \in T} \mathrm{d}x_v \times \mathrm{d}x^T = \mathrm{d}x_T.$$

Then this measure is independent of the set S, so that it defines a unique Haar measure on G which we may denote symbolically by $\mathrm{d}x = \prod \mathrm{d}x_v$.

Proposition 3.19. *For each v, let $f_v \in L_1(G_v)$. Suppose that (1), $f_v(H_v) = 1$ for almost all v; (2), $\prod \int_{G_v} |f_v(x_v)| \mathrm{d}x_v < \infty$. Set $f(x) = \prod f_v(x_v)$ for any $x = (x_v) \in G$. Then*

$$\int_G f(x) \mathrm{d}x = \prod \int_{G_v} f_v(x_v) \mathrm{d}x_v.$$

Proof. Since $\mathrm{d}x$ is a Haar measure, $\int_G f(x) \mathrm{d}x$ can be computed as

$$\sup\{ \int_B f(x) \mathrm{d}x \}$$

where B ranges over all compact subsets of G. But every compact subset of B is contained in some G_S for some finite subset S of v, Assume that S is so large that $f_v(H_v) = 1$ for $v \notin S$. Then

$$\begin{aligned} |\int_B f(x)\mathrm{d}x| &\leq \int_B |f(x)|\mathrm{d}x \leq \int_{G_S} |f(x)|\mathrm{d}x \\ &= \prod_{v\in S}\int_{G_v} |f_v(x_v)|\mathrm{d}x_v \\ &\leq \prod \int_{G_v} |f_v(x_v)|\mathrm{d}x_v < \infty \end{aligned}$$

So $f \in L_1(G)$. And

$$\begin{aligned} \int_G f(x)\mathrm{d}x &= \sup\{\int_B f(x)\mathrm{d}x\} = \lim_S \int_{G_S} f(x)\mathrm{d}x \\ &= \lim_S \prod_{v\in S}\int_{G_v} f_v(x_v)\mathrm{d}x_v \\ &= \prod \int_{G_v} |f_v(x_v)|\mathrm{d}x_v \end{aligned}$$

□

3.4.2 Fourier transforms

Let μ be a Haar measure of G and $L_1(G)$ be the linear space of measurable complex valued functions on G with respect to $\mathrm{d}\mu$. The *Fourier transform* of f is the function on $\widehat{G}$ given by

$$\widehat{f}(\chi) = \int_G f(g)\overline{\chi(g)}\mathrm{d}\mu g.$$

There is an important result about the Fourier transform as follows.

Inversion Theorem *There exists a unique Haar measure $\widehat{\mu}$ on the dual group $\widehat{G}$ such that for every continuous and integrable function f on G, whose Fourier transform $\widehat{f}$ is also integrable, the following formula holds:*

$$f(g) = \int_{\widehat{G}} \widehat{f}(\chi)\chi(g)\mathrm{d}\widehat{\mu}\chi = \widehat{\widehat{f}}(-g).$$

In the above theorem, the Haar measure $\widehat{\mu}$ is said to be *dual* to μ. In particular, if G is self-dual, then one can choose the Haar measure so that the inversion formula holds with the same measure on G and $\widehat{G}$; it is called the *self-dual Haar measure.*

Theorem 3.20. *The normalized Haar measure* d^+x *of* k_v^+ *is self-dual.*

Proof. To prove the theorem, is to prove that on identifying k with its dual as $\alpha \mapsto \chi_\alpha = e(x\lambda_p(Tr_{k/\mathbb{Q}_p}(\alpha)))$, the Fourier inversion formula holds for $d^+\chi_\alpha = d^+\alpha$.It suffices to verify that the Fourier inversion formula holds for a single f. Let us consider the three cases separately.

Case 1: $k_v = \mathbb{R}$, set $f(x) = e^{-\pi x^2}$. Then

$$\begin{aligned}\hat{f}(x) &= \int_{\mathbb{R}} e^{-\pi y^2+2\pi xy} d^+y = e^{-\pi x^2}\int_{-\infty}^{\infty} e^{-\pi(ix+y)^2} d^+y \\ &= e^{-\pi x^2}\int_{-\infty}^{\infty} e^{-\pi y^2} d^+y = e^{-\pi x^2}\end{aligned}$$

Hence we have that $\hat{f}(x) = f(x)$ and $\hat{\hat{f}}(x) = f(x) = f(-x)$, the Fourier inversion theorem holds.

Case 2: $k_v = \mathbb{C}$, set $f(z) = e^{-\pi|z|_\infty}$ and $z = x + iy$. Then we have $d^+z = 2d^+xd^+y$ and $|z|_\infty = x^2 + y^2$. Therefore,

$$\begin{aligned}\hat{f}(\chi_x + i\chi_y) &= 2\int_{-\infty}^{\infty}\int_{-\infty}^{\infty} e^{-\pi(x^2+y^2)+4\pi i\mathrm{Re}((\mathrm{x+iy})(\chi_\mathrm{x}+\mathrm{i}\chi_\mathrm{y}))} d^+xd^+y \\ &= 2\int_{-\infty}^{\infty}\int_{-\infty}^{\infty} e^{-\pi x^2+4\pi x\chi_x} e^{-\pi y^2-4\pi y\chi_y} d^+xd^+y \\ &= 2\left(\int_{-\infty}^{\infty} e^{-\pi(x-2i\chi_x)^2} d^+x)(\int_{-\infty}^{\infty} e^{-\pi(y+2i\chi_y)^2} d^+y\right) \\ &= 2e^{-4\pi(\chi_x^2+\chi_y^2)} \\ &= 2f(2\chi_x + 2i\chi_y)\end{aligned}$$

Therefore, $\hat{\hat{f}}(z) = f(z) = f(-z)$, the Fourier inversion theorem holds.

Case 3: $v < \infty$, let f be the characteristic function of $\mathfrak{o}_k$. Then we have

$$\hat{f}(y) = \int_k f(x)\chi_y(x)d^+x = \int_{\mathfrak{o}_k} \chi_y(x)d^+x.$$

If $y \in \mathfrak{D}^{-1}, \mathfrak{D} = \mathfrak{D}_{k/\mathbb{Q}_p}$, then $\chi_y(x) = 1$ for any $x \in \mathfrak{o}_k$, hence $\hat{f}(y) = N\mathfrak{D}^{-\frac{1}{2}}$. If $y \notin \mathfrak{D}^{-1}$, then there exists $x_0 \in \mathfrak{o}_k$ such that $\chi_y(x_0) \neq 1$, so that $\chi_y(x)$ is

nontrivial. Therefore,

$$\begin{aligned}\hat{f}(y) &= \int_{\mathfrak{o}_k} \chi_y(x)d^+x = \int_{\mathfrak{o}_k} \chi_y(x+x_0)d^+x \\ &= \chi_y(x_0)\int_{\mathfrak{o}_k} \chi_y(x)d^+x \\ &\Rightarrow (1-\chi_y(x_0)\int_{\mathfrak{o}_k} \chi_y(x)d^+x) = 0 \\ &\Rightarrow \hat{f}(y) = 0\end{aligned}$$

Hence we have $\hat{f}(y) = N\mathfrak{D}^{-\frac{1}{2}}$.(characteristic function of $\mathfrak{D}^{-1}$)
Therefore,

$$\hat{\hat{f}}(x) = N\mathfrak{D}^{-\frac{1}{2}}\int_{\mathfrak{D}^{-1}} \chi_x(y)d^+y.$$

By the same method as we calculate $\hat{f}$, we have that for $x \in \mathfrak{o}_k$,

$$\begin{aligned}\hat{\hat{f}}(x) &= N\mathfrak{D}^{-\frac{1}{2}}\int_{\mathfrak{D}^{-1}} d^+y = N\mathfrak{D}^{-\frac{1}{2}}\int_{\pi^{\mathrm{ord}_k(\mathfrak{D}^{-1})}\mathfrak{o}_k} d^+y \\ &= N\mathfrak{D}^{-\frac{1}{2}}Np^{-\mathrm{ord}_k(\mathfrak{D}^{-1})}N\mathfrak{D}^{-\frac{1}{2}} = 1\end{aligned}$$

Similarly, if $x \notin \mathfrak{o}_k$, $\hat{\hat{f}}(x) = 0$. Therefore, $\hat{\hat{f}}(x) = f(-x)$, the Fourier inversion theorem holds. □

Corollary 3.21. *Let d^+x_v be the normalized Haar measures (self-dual) of k_v^+ for any places v of k. Then $\mathrm{d}x = \prod \mathrm{d}^+x_v$ is a self-dual measure on $\mathbb{A}_k$.*

Proof. Let $\chi_x = (\chi_{x_v}) \in \mathbb{A}_k$ and $f(x) = (f_v(x_v))$ where $f_v(x_v)$ is continuous for all v and is the characteristic function of H_v for almost all v. For almost all v, $\chi_{x_v} \in H_v^\perp$. Thus for almost all v, $f_v(x_v)\langle x_v, \chi_{x_v}\rangle$ is the characteristic function of H_v. Moreover,

$$\prod_v \int_{G_v} |f_v(x_v)\langle x_v, \chi_{x_v}\rangle|_\infty d^+x_v \le \prod_v \int_{G_v} |f_v(x_v)|_\infty d^+x_v < \infty.$$

Since almost all the factors of the product is 1 and $f_v \in L^1(G_v)$. Therefore, we have that

$$\begin{aligned}\hat{f}(\chi_x) &= \int_G f(x)\langle x, \chi_x\rangle dx \\ &= \int_{G_v} (\prod_v f_v(x_v)\langle x_v, \chi_{x_v}\rangle)dx \\ &= \prod_v \int_{G_v} f_v(x_v)\langle x_v, \chi_{x_v}\rangle d^+x_v \\ &= \prod_v \hat{f}_v(\chi_{x_v})\end{aligned}$$

Hence we have that

$$\hat{\hat{f}}(x) = \prod_v \hat{\hat{f}}_v(x_v) = \prod_v f_v(-x_v) = f(-x),$$

the Fourier inversion theorem holds. □

3.4.3 The Schwartz-Bruhat space

In this subsection, we shall introduce a class of functions: the Schwartz-Bruhat functions on the additive groups $G = k_v^n$, where k_v is any local field or $G = \mathbb{A}^n$ where $\mathbb{A}$ is the adele ring of a global field.

Let f be a complex valued function on k_v^n. Then f is said to *smooth* if f has derivatives of all order as $v|\infty$, i.e., $f \in C^\infty(k_v^n)$ and f is locally constant as $v < \infty$. The function f on $\mathbb{R}^n$ is said to *rapidly decreasing* at ∞ if

$$\|f\|_{\alpha,\beta} = \sup_{x\in\mathbb{R}^n} |x_1^{\alpha_1} \dots x_n^{\alpha_n}| \frac{\partial^{\beta_1+\dots+\beta_n} f}{\partial x_1^{\beta_1} \dots \partial x_n^{\beta_n}}(x)$$

is bounded for all $\alpha_i, \beta_i \in \{0\} \cup \mathbb{N}$. The function f is said to *compactly supported* if the closure of the set $\mathrm{supp} f = \{x : f(x) \neq 0\}$ is compact.

Definition 3.22. *(1), The complex valued function $f(x)$ on $G = k_v^n$ is called the Schwartz-Bruhat function if f is smooth and rapidly decreasing as $v|\infty$; if f is smooth and compactly supported if $v < \infty$. Denote the Schwartz-Bruhat functions space by $\mathcal{S}(G)$.*

(2), A Schwartz-Bruhat funtion on $\mathbb{A}_k$ is a linear combination of functions of the form

$$f = \prod_v f_v = f_\infty \prod_{v<\infty} f_v, \quad f_\infty \in \mathcal{S}(\mathbb{R}^n) \text{ and } f_v \in \mathcal{S}(k_v)$$

where f_v is the characteristic function of $\mathfrak{o}_v$ for almost all $v < \infty$.

Proposition 3.23. *For any $f \in \mathcal{S}(G)$, there is an open compact subgroup K of G, such that f is right K-invariant.*

Proof. Let S be the support of the functions f. It is compact. According to locally constant, for all $x \in S$, there exists an open compact subgroup K_x such that $f(x)$ is constant on xK_x. We have

$$S \subset \bigcup_{x\in S} xK_x.$$

By the compactness of S, there are $x'_1, x'_2, \cdots, x'_m$, such that

$$S \subset \bigcup_{i=1}^{m} x'_i K_{x_i}.$$

Take $K = \cap_{i=1}^{i=m} K_{x'_i}$. Since $K_{x'_i}/K$ is finite, we have

$$S \subset \bigcup_{i=1}^{n} x_i K.$$

Therefor there exist complex numbers $c_1, c_2, \cdots, c_n$ such that

$$f(x) = \sum_{i=1}^{n} c_i \, \mathrm{char}(x_i K)$$

where $\mathrm{char}(g_i K)$ is the characteristic function of the right coset $g_i K$. It is clear now that $f(x)$ is right K-invariant. □

According to Prop(**), we can define

$$\int_G f(g) \mathrm{d}g = \sum_{i=1}^{n} c_i \mu(K),$$

which is a finite sum.

The main result about the Fourier transform of a Schwartz-Bruhat function is as follows.

Theorem 3.24. *The Fourier transform of a Schwartz-Bruhat function on a locally compact abelian group is a Schwartz-Bruhat function on the Pontryagin dual group. In particular, if $f \in \mathcal{S}(G)$ for the self-dual groups $G = k_v^+$ or $\mathbb{A}_k$, then $\widehat{f} \in \mathcal{S}(G)$.*

Proof. See [7]. □

3.4.4 Poisson summation formula

The Poisson summation formula is an equation that relates the Fourier series coefficients of the periodic summation of a function to values of the function's continuous Fourier transform. Consequently, the periodic summation of a function is completely defined by discrete samples of the original function's Fourier transform. And conversely, the periodic summation of a function's Fourier transform is completely defined by discrete samples of the original function [22].

Theorem 3.25. *Let H be a discrete subgroup of a locally compact abelian group G such that G/H is compact. Then*

$$\mu\,(G/H)\sum_{h\in H} f(h) = \sum_{\hat{h}\in H^\perp} \widehat{f}(\hat{h}),$$

provided that f is integrable on G, the series $\sum_{h\in H} f(g+h)$ is absolutely convergent uniformly in g and $\sum_{\hat{h}\in H^\perp} \widehat{f}(\hat{h})$ is absolutely convergent.

Proof. $H^\perp$ is discrete and $\hat{G}/H^\perp$ is compact, by the Pontryagin Duality Theorem. Define the function $\phi(x)$ on G/H by $\phi(x) = \sum_{h\in H} f(x+h)$; then

$$\int_{G/H} \phi(x)\,d\mu = \int_G f(g)\,d\mu, \hat{\phi}(\hat{h}) = \int_{G/H} \phi(x)\overline{\hat{h}(x)}\,d\mu. \quad (*)$$

By the Fourier Inverse formula,

$$\phi(x)\mu(G/H) = \sum_{H^\perp} \hat{h}(x)\hat{\phi}(\hat{h})$$

up to a constant factor. To see that the constant is correct, set $\phi(x) = 1$; the $\hat{\phi}(1) = \mu(G/H)$ and $\hat{\phi}(\hat{h}) = 0$ otherwise, the latter result coming from writing xx_0 for x in the second equation $(*)$ where $\hat{h}(x_0) \neq 1$. Also,

$$\hat{\phi}(\hat{h}) = \int_{G/H} \phi(x)\overline{\hat{h}(x)}\,d\mu = \int_G f(g)\overline{\hat{h}(g)}\,d\mu,$$

the change in the order of summation and integration being justified by the hypotheses on f. Hence

$$\phi(x)\mu(G/H) = \sum_{\hat{h}\in H^\perp} \hat{h}(x)\hat{f}(\hat{h})$$

and writing $x = 0, \phi(0) = \sum_{h\in H} f(h)$ gives the theorem. □

Corollary 3.26. *Let $f = \prod_v f_v \in$ Then*

$$\mu(\mathbb{A}_k/k)|\alpha| \sum_{x\in k} f(\alpha x) = \sum_{x\in k} \widehat{f}(\alpha^{-1}x).$$

Proof. Write $g(\xi) = f(\alpha\xi)$, then

$$\begin{aligned} \hat{g}(\eta) &= \int_{\mathbb{A}} g(\xi)\overline{\chi_\eta(\xi)}\,d\mu = \int_{\mathbb{A}} f(\alpha\xi)\overline{\chi(\xi\eta)}\,d\mu \\ &= |\alpha|^{-1}\int_{\mathbb{A}} f(\xi)\overline{\chi(\alpha^{-1}\xi\eta)}\,d\mu = |\alpha|^{-1}\hat{f}(\alpha^{-1}\eta), \end{aligned}$$

where to go from the first line to the second we have written $\alpha^{-1}\xi$ for ξ. Now apply the Theorem 3.25 to $g(\xi)$ with $G = \mathbb{A}_k$ and $H = k$, and use the fact that $H^\perp = k$ by the Corollary 3.16. □

Corollary 3.27. *The measure of* $\mathbb{A}_k/k$ *is* 1 *with respect to the self-dual Haar measure* $\mathrm{d}x$ *on* $\mathbb{A}_k$.

Proof. If we identify $\overline{\mathbb{A}_k}$ with $\mathbb{A}_k$, the symmetry property of the Fourier transform becomes

$$\hat{f}(\eta) = \int_{\mathbb{A}} f(\xi)\overline{\chi(\xi\eta)}\, d\mu \Leftrightarrow f(\xi) = \int_{\mathbb{A}} \hat{f}(\eta)\chi(\xi\eta)\, d\mu$$

where μ is normalized by the condition $\mu(\mathbb{A}_k/k) = 1$. For we know from the Fourier inversion formula that $f(\xi) = A\int_{\mathbb{A}} \hat{f}(\eta)\chi(\xi\eta)\, d\mu$ for some constant A depending on μ. Applying Theorem 3.25. to both f and $\hat{f}$ and remembering that $\overline{\chi(\xi\eta)} = \chi(-\xi\eta)$ we obtain $A(\mu(\mathbb{A}_k/k))^2 = 1$. Therefore $A = 1$ is equivalent to $\mu(\mathbb{A}_k/k) = 1$ □

Exercises

You are encouraged to collaborate on solving the problems given as homework. However, the solutions should be written on your own and in your own words. Please send me your homework to my email before the next week's class.

1, Let p_n be the nth positive prime in $\mathbb{Z}$, and let $\alpha^n = (\alpha_v^{(n)}) \in \mathbb{A}_{\mathbb{Q}}$ with $\alpha_v^{(n)} = p_n$ if $v = p_n$ and $\alpha_v^{(n)} = 1$ if $v \neq p_n$. The result is a sequence $\{\alpha^n\}$ of ideleds in $\mathbb{I}_{\mathbb{Q}}$. Show that this sequence converges to the idele $(1)_v$ in the topology of the adeles but not converges in the topology of the ideles.

2, Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$ be distinct places of a number field k and $x_1, \ldots, x_m \in k$. Let $\epsilon > 0$ be given. Then there exists $x \in k$ such that $|x - x_i|_{\mathfrak{p}_i} < \epsilon$ for $1 \leq i \leq m$ and $\mathrm{ord}_{\mathfrak{p}}(x) \geq 0$ for any $\mathfrak{p} \notin \{\mathfrak{p}_1, \ldots, \mathfrak{p}_m\}$.

3, Show that $|\alpha|_v = 1$ at each place $v \leq \infty$ of k if and only if α is a root of unity in k.

4, Show that $\widehat{\mathbb{R}/\mathbb{Z}} \cong \mathbb{Z}$, i.e., every character of $\mathbb{R}/\mathbb{Z}$ is of form $x \mapsto e(mx)$ for some integer m.

5, Let χ be a character on a compact group G and $\mathrm{d}x$ be a Haar measure on G. Then

$$\int_G \chi(x)\mathrm{d}x = \begin{cases} \mu(G), & \text{if } \chi \text{ is trivial;} \\ 0, & \text{otherwise.} \end{cases}$$

6, $\widehat{\mathfrak{o}_v} \cong k_v^+/\mathfrak{D}_v^{-1}$.

7, Every additive quasicharacter χ_α of $\mathbb{R}^+$ is of form $\chi_\alpha : x \mapsto \chi_\alpha(x) = e(x\alpha)$ for some complex number α, i.e., the mapping

$$\mathbb{R}^+ \longrightarrow \widehat{\mathbb{R}^+} \quad \text{by} \quad \alpha \longmapsto \chi_\alpha$$

is an isomorphism of topological groups.

8, Every multiplicative character of the group $\mathbb{R}_+^\times$ (the multiplicative group of positive real numbers) is of form $x \mapsto x^s$ for some $s \in \mathbb{C}$.

(2) Every multiplicative character of the group $\mathbb{R}^\times$ (the multiplicative group of nonzero real numbers) is of form $x \mapsto \mathrm{sign}^\epsilon(x)|x|^s$ for some $s \in \mathbb{C}$ and $\epsilon = 0$, or 1.

9, The circle group S^1 has no small subgroups, i.e., there is a neighborhood U of the identity $1 \in S^1$ such that the only subgroup of S^1 inside U is the trivial group $\{1\}$.

10, Let G be a totally disconnected locally compact topological group. Prove that the kernel of any continuous homomorphism of $G \longrightarrow GL_m(\mathbb{C})$ contains an open subgroup.

11, If G is a compact topological abelian group, or if every element of G is of finite order, then every quasicharacter of G is a character.

12, Let n be a positive integer and let

$$U(n) = \mathbb{R}_+^\times \prod_{p|n} U_p(n) \prod_{p\nmid n} \mathbb{Z}_p^\times$$

where $U_p(n) = \{x \in \mathbb{Z}_p^\times \,:\, x \equiv 1 \mod n\}$. And let

$$V(n) = \mathbb{R}_+^\times \prod_{p|n} U_p(n) \prod_{p\nmid n} \mathbb{Q}_p^\times.$$

Show that

$$\mathbb{I}_\mathbb{Q}/U(n)\mathbb{Q}^\times \cong (\mathbb{Z}/n\mathbb{Z})^\times.$$

13, We will call $\chi : \mathbb{I}_k/k^\times \to S^1$ a character of finite order if there exists a positive integer m such that $\chi(x)^m = 1$ for all $x \in \mathbb{I}_k$. Then χ has finite order if and only if its restriction to $\mathbb{R}_+^\times$ is trivial.

14, (1) Let dx be an additive measure such that the measure $\mathbb{Z}_p$ is 1. Let $d^\times x$ be a multiplicative measure such that the measure $\mathbb{Z}_p^\times$ is 1. Then

$$d^\times x = \frac{p}{p-1}\frac{dx}{|x|_p}.$$

(2), Compute the integral

$$\int_{\mathbb{Z}_p} |x|_p^s \, dx.$$

15, Let $\chi_p(\alpha) = e(\lambda_p(\alpha))$ be an additive character of $\mathbb{Q}_p$ and dx be an additive measure such that the measure $\mathbb{Z}_p$ is 1.

(1), Compute $k \in \mathbb{Z}$

$$\int_{\varpi^k\mathbb{Z}_p} \chi_p(x)\mathrm{d}x.$$

(2), Compute $k \in \mathbb{Z}$

$$\int_{\varpi^k U_p} \chi_p(x)\mathrm{d}x,$$

where ϖ is an uniformizer of $\mathbb{Z}_p$ and $U_p = \mathbb{Z}_p^\times$ is the unit group of $\mathbb{Z}_p$.

16, Show that Theorem 3.23.

Chapter 4

Arithmetic L-functions

4.1 Tate's thesis

In number theory, Tate's thesis is the 1950 thesis of John Tate (1950) under supervision of Emil Artin. In it he used a translation invariant integration on the locally compact group of ideles to lift the zeta function of a number field, twisted by a Hecke character, to a zeta integral and study its properties. Using harmonic analysis, more precisely the summation formula, he proved the functional equation and meromorphic continuation of the zeta integral and the twisted zeta function. He also located the poles of the twisted zeta function. His work can be viewed as an elegant and powerful reformulation of a work of Erich Hecke on the proof of the functional equation of the twisted zeta function (L-function). Hecke used a generalized theta series associated to an algebraic number field and a lattice in its ring of integers.

Kenkichi Iwasawa independently discovered during the war essentially the same method (without an analog of the local theory in Tate's thesis) and announced it in his 1950 ICM paper and his letter to Dieudonne written in 1952. Hence this theory is often called Iwasawa-Tate theory. Iwasawa in his letter to Dieudonne derived on several pages not only the meromorphic continuation and functional equation of the L-function, he also proved finiteness of the class number and Dirichlet's theorem on units as immediate byproducts of the main computation.

A noncommutative generalisation: Iwasawa-Tate theory was extended to a general linear group over an algebraic number field and automorphic representations of its adelic group by Roger Godement and Herv Jacquet in 1972. This work is part of activities in the Langlands correspondence. [22]

In hindsight, Tate's work may be viewed as giving the theory of automorphic representations and L-functions of the simplest connected reducible group $GL_1(F)$, where F is the number field.

4.1.1 Local theory

4.1.2 Global theory

4.2 Dedekind zeta functions, Hecke character and Hecke L-functions

4.2.1 Dedekind zeta functions

4.2.2 Hecke character

4.2.3 Hecke L-functions

4.3 Applications of Hecke L-functions

4.3.1 Splitting of primes

4.3.2 Abelian L-functions

4.3.3 Tchebotarev's density theorem

4.3.4 Class number formulas

4.4 Artin L-functions

12,
12,
12,
12,

Bibliography

[1] R. B. Ash, *Basic Abstract Algebra, for Graduate Students and Advanced Undergraduates*, `http://www.math.uiuc.edu/~r-ash/Algebra.html`, Dover Publications Inc., Mineola, New York, 2007.

[2] J. Bernstein, S. Gelbert, *An Introduction to the Langlands Program*, Birkhäuser, 2003.

[3] D. Bump, *Automorphic forms and representations*, Cambridge Studies in Advanced Mathematics, 55, Cambridge University Press, 1997.

[4] J. W. S. Cassels, A. Fröhlich eds., *Algebraic Number Theory*, New York, Academic Press, 2010.

[5] S. S. Ding, L. Z. Nie, *An Introduction to Algebra*, in Chinese, Higher Education Press, 2000.

[6] K. Q. Feng, *Algebraic Number Theory*, in Chinese, Science Press, 2001.

[7] L. J. Goldstein, *Analyic Number Theory*, Prentice-Hall, Inc. Englewood Cliffs, New Jersey, 1971.

[8] H. Iwaniec, *Topics in the Classical Automorphic Forms*, Graduate Studies in Mathematics 17, AMS, Providence, 1997.

[9] H. Iwaniec and E. Kowalski, *Analytic Number Theory*, Amer. Math. Soc. Colloquium Publ. 53, AMS, Providence, 2004.

[10] A. W. Knapp, *Introduction to the Langlands Program*, in Representation Theory and Automorphic Forms, T. N. Bailey and A. W. Knapp editors, Proc. Symp. Pure Math., Vol. 61, Amer. Math. Soc., Providence, 1997, 245-302.

[11] S. Lang, *Algebraic Number Theory*, GTM 110, Spring-Verlag, 1994.

[12] K. F. Lai and X. N. Feng, *Introduction to Topological Groups,* in Chinese, Science Press, 1999.

[13] C. J. Moreno, *Advanced Analyitc Number Theory: L-Functions*, Mathematics Surveys and Monographs, Vol. 115, AMS, Providence, 2005.

[14] M. R. Murty, V. K. Murty, *Non-vanishing of L-Functions and Applications*, Birkhauser Basel, 1997.

[15] W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers,* Springer, 2004.

[16] J. Neukirch, *Algebraic Number Theory*, Springer-Verlag, 1999.

[17] F. Oggier, *Introduction to Algebraic Number Theory*, available at `http://www1.spms.ntu.edu.sg/~frederique/ANT10.pdf`.

[18] D. Ramakrishnan, R. J. Valenza, *Fourier Analysis on Number Fields,* GTM 186, Springer, 1998.

[19] W. Stein, *A Brief Introduction to Classical and Adelic Algebraic Number Theory,* available from `http://wstein.org/papers/ant/`.

[20] H. P. F. Swinnerton-Dyer, *A Brief Guide to Algebraic Number Theory*, Cambridge University Press, 2003.

[21] A. Weil, *Basic Number Theory*, Spring-Verlag, 1974.

[22] Wikipedia, the free encyclopedia that anyone can edit. `http://en.wikipedia.org/`

[23] X. K. Zhang, *Introduction to Algebraic Number Theory*, 2nd, in Chinese, Higher Education Press, 2006.

Guanghua Ji
School of Mathematics
Shandong University
Jinan, Shandong 250100
P. R. China
ghji@sdu.edu.cn

Index