Algebra Number Theory

TRISCT

Contents

Fields are algebraic number fields unless otherwise specified. And they are usually denoted by K.

1 Preliminary Topics

1.1 Algebraic Number Field

Algebraic number field A finite extension field of $\mathbb{Q}$ is called an **algebraic number field**. Its elements are called **algebraic numbers**.

1.2 Cayley-Hamilton's Theorem

The statement is as follows.

Theorem 1.1. *Let M be a finitely generated module over a commutative ring with identity R and let ϕ be an endomorphism on R. Then*

(i) If $x_1, \cdots, x_n$ are generators of M, and we write

$$\phi(x_i) = \sum_{j=1}^{n} a_{ij} x_j, \quad a_{ij} \in R$$

then $f(t) = \det(tI - A)$ is an annihilating polynomial of ϕ, where $A = (a_{ij})$.

(ii) If moreover there exists an ideal $\mathfrak{a} \subset R$ such that $\phi(M) \subset \mathfrak{a}M$, then we may choose

$$f(t) \in \mathfrak{a}[t]$$

Proof. (i) It suffices to prove that $f(\phi)(x_i) = 0$ for all i. We start by writing

$$\phi(x_i) = \sum_{j=1}^{n} a_{ij} x_j, \quad a_{ij} \in R$$

in the matrix form:

$$\begin{pmatrix} \phi(x_1) & & \\ & \ddots & \\ & & \phi(x_n) \end{pmatrix} = \begin{pmatrix} \phi & & \\ & \ddots & \\ & & \phi \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$$

$$\implies \begin{pmatrix} \phi - a_{11} & \cdots & -a_{1n} \\ \vdots & \ddots & \vdots \\ -a_{n1} & \cdots & \phi - a_{nn} \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = (\phi I - A) \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$$

Multiply this on the left by the adjugate matrix $(\phi I - A)^*$ and we obtain

$$\det(\phi I - A) I \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} \implies \det(\phi I - A) x_i = 0 \text{ for each } i$$

$$\implies \det(\phi I - A) = 0$$

(ii) By assumption we may choose $a_{ij} \in \mathfrak{a}$, which finishes the proof.

Example 1.1. One application of this theorem is to give a criterion on whether a number is an algebraic integer. If one can find a (nonzero) finitely generated $\mathbb{Z}$-module M in an algebraic number field K, such that the multiplication mapping $a : x \mapsto ax$ by some $a \in K$ from M is into M, then a is an algebraic integer. Furthermore, we may use this to prove that all algebraic integers form a ring. Let a, b be algebraic integers and consider the ring and $\mathbb{Z}$-module $\mathbb{Z}[a, b]$. If is finitely generated by $a^i b^j$ (degrees are finite, because a, b are algebraic). Then each element in $\mathbb{Z}[a, b]$ is an algebraic integer, and so are $a - b$ and ab. □

1.3 Riesz Representation Theorem

This section discusses the use of the following theorem.

Theorem 1.2. *Let V be a finite-dimensional nonsingular*[1] *vector space equipped with a bilinear form $\langle \cdot, \cdot \rangle$ (either symmetric, skew-symmetric or alternate). Then*

[1]In a vector space V over F equipped with a bilinear form $\langle \cdot, \cdot \rangle$ (either symmetric, skew-symmetric or alternate), a vector v is call **degenerate** if $\langle v, \cdot \rangle = 0 \in V^*$. The set of all degenerate vectors is called the **radical** of V, denoted by $\mathrm{rad}V = V^{\perp}$. If $\mathrm{rad}V = 0$, then V is called **nonsingular** or **nondegenerate**, otherwise **singular** or **degenerate**.

the mapping

$$\begin{array}{rccl} \tau & : & V & \to & V^* \\ & & x & \mapsto & \langle x, \cdot \rangle \end{array}$$

*is an isomorphism $V \cong V^*$. It follows that each $f \in V^*$ can be represented uniquely by its **Riesz vector**.*

The following example shows that the ring R of algebraic numbers of an algebraic number field K is finitely generated.

Example 1.2. Let K be an algebraic number field and consider the bilinear form

$$\begin{array}{rccl} \langle \cdot, \cdot \rangle & : & K \times K & \to & \mathbb{Q} \\ & & (x, y) & \mapsto & \mathrm{Tr}_{K/\mathbb{Q}}(xy) \end{array}$$

and the homomorphism it induces

$$\begin{array}{rccl} \varphi & : & K & \to & K^* \\ & & x & \mapsto & \mathrm{Tr}_{K/\mathbb{Q}}(x(\cdot)) \end{array}$$

The bilinear form is symmetric and nondegenerate because if $x \neq 0$, then $\langle x, 1/x \rangle = \mathrm{Tr}_{K/\mathbb{Q}}(1) = [K : \mathbb{Q}] \neq 0$. It follows that φ is an isomorphism between K and K^* (because $K/\mathbb{Q}$ is finite dimensional). Since K is finite dimensional, any basis $e_1, \cdots, e_n$ in K has a dual basis $e_1^*, \cdots, e_n^*$ in K^*, which, by the isomorphism φ induced by the nondegenerate bilinear form $\mathrm{Tr}_{K/\mathbb{Q}}(xy)$, in turn corresponds to a basis $f_1, \cdots, f_n$ in K (such that $\varphi_{f_i} = e_i^*$).

In short, given a basis $e_1, \cdots, e_n$ of K we can find another basis $f_1, \cdots, f_n$ of K such that $\langle e_i, f_j \rangle = \delta_{ij}$.

Let $e_1, \cdots, e_n$ be a basis of any order $\mathcal{O}$ (hence also a basis of $K/\mathbb{Q}$). From what we just proved there is a corresponding basis $f_1, \cdots, f_n$ of K such that $\langle e_i, f_j \rangle = \delta_{ij}$. We shall prove that R is generated by $f_1, \cdots, f_n$ over $\mathbb{Z}$

The most direct approach is to compute the component of an arbitrary $x \in R$ with respect to f_j by

$$x = \sum_{j=1}^{n} x_j f_j \implies x_i = \mathrm{Tr}_{K/\mathbb{Q}}(xe_i) \in \mathbb{Z}$$

Note 1.1. Note that any element in an order is an algebraic integer, and that the product of two algebraic integers is also an algebraic integer.

Note 1.2. This whole proof relies on only three conditions. (i) K is an algebraic number field; (i) $\mathrm{Tr}_{K/\mathbb{Q}}$ is nondegenerate; (iii) Any order is full of algebraic integers and algebraic integers form a ring.

□

1.4 The Discriminant

Let K be an algebraic number field. From Example.**??**., we know any $x \in K$ has the coordinate $x = \sum_{j=1}^{n} \mathrm{Tr}(xe_j)f_j$ (the extension $K/\mathbb{Q}$ of Tr is omitted) under the dual basis f_j of e_i. Then we have a transition matrix from e_i to f_j:

$$\begin{aligned}
\begin{pmatrix} e_1 \\ \vdots \\ e_n \end{pmatrix} &= \begin{pmatrix} \sum_{j=1}^{n} \mathrm{Tr}(e_1e_j)f_j \\ \vdots \\ \sum_{j=1}^{n} \mathrm{Tr}(e_ne_j)f_j \end{pmatrix} = \begin{pmatrix} \mathrm{Tr}(e_1e_1) & \cdots & \mathrm{Tr}(e_1e_n) \\ \vdots & \ddots & \vdots \\ \mathrm{Tr}(e_ne_1) & \cdots & \mathrm{Tr}(e_ne_n) \end{pmatrix} \begin{pmatrix} f_1 \\ \vdots \\ f_n \end{pmatrix} \\
&= (\mathrm{Tr}(e_ie_j)) \begin{pmatrix} f_1 \\ \vdots \\ f_n \end{pmatrix}
\end{aligned}$$

The transition matrix between two bases has a nonzero determinant, which is defined to be the **discriminant** of the basis e_i.

The **discriminant** of a full module M in K is defined as the discriminant of one of its bases.

$$\Delta(M) = \mathrm{disc}(M) = \det\left(\mathrm{Tr}(e_ie_j)\right)$$

for any basis e_i of the module. One can verify that this is invariant under a change of basis. Let e_i' be another basis for M, then the transition matrix[2] $A = (a_{ij})$ from e_i to e_i' has determinant ± 1, hence

$$\begin{aligned}
\det\left(\mathrm{Tr}(e_i'e_j')\right) &= \det\left(\mathrm{Tr}\left(\sum_{t=1}^{n} a_{it}e_t\right)\left(\sum_{s=1}^{n} a_{js}e_s\right)\right) \\
&= \det\left(\sum_{t=1}^{n} a_{it}\sum_{s=1}^{n} a_{js}\mathrm{Tr}(e_te_s)\right) \\
&= \det\left(A \cdot \mathrm{Tr}(e_ie_j) \cdot A^T\right) \\
&= \det(A)^2 \det\left(\mathrm{Tr}(e_ie_j)\right) \\
&= \det\left(\mathrm{Tr}(e_ie_j)\right)
\end{aligned}$$

The **discriminant** of an algebraic number field is the discriminant of its ring of algebraic integers.

1.5 Lattices in $\mathbb{R}^n$

We begin with the definitions and properties.

[2]Such that $(e_1', \cdots, e_n')^T = A\,(e_1, \cdots, e_n)^T$

Discrete set A set D in a topological space X is called **discrete** if the induced topology on D is the discrete topology[3], or equivalently, D has only isolated points. We have the following criterion. Let X be a metric space and $D \subset X$. Then

$$\begin{aligned} & D \text{ is closed and discrete} \\ \iff & \text{for any bounded set } B \subset X,\ D \cap B \text{ is finite} \\ \iff & D \text{ has no limit point in } X \end{aligned}$$

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

$$L = \mathbb{Z}e_1 + \cdots + \mathbb{Z}e_m$$

with linearly independent generators $e_1, \cdots, e_m$ and integer coefficients. A lattice in $\mathbb{R}^n$ is called **full** if it has a basis of $\mathbb{R}^n$, i.e., n linearly independent vectors.

We now move to the most important proposition of this section.

Theorem 1.3. *Any lattice in $\mathbb{R}^n$ is discrete.*

Proof. Let $L = \mathbb{Z}e_1 + \cdots + \mathbb{Z}e_m$ be a lattice in $\mathbb{R}^n$. Since $\mathbb{Z}e_1, \cdots, \mathbb{Z}e_m$ are linearly independent, we can expand them to a basis $\mathbb{Z}e_1, \cdots, \mathbb{Z}e_n$ of $\mathbb{R}^n$. Then we have an isomorphism (as vector spaces)

$$\begin{array}{cccc} \varphi : & \mathbb{R}^n & \to & \mathbb{R}^n \\ & (\lambda_1, \cdots, \lambda_n) & \mapsto & \lambda_1 e_1 + \cdots + \lambda_n e_n \end{array}$$

Note that this is a continuous nonsingular linear map, hence x is isolated in $L \iff \varphi^{-1}(x)$ is isolated in $\varphi^{-1}(L)$. And it follows from $\varphi^{-1}(L) = \mathbb{Z}^m \times \{0\}^{n-m}$ that $L \cong \varphi^{-1}(L)$ is discrete.

The converse is very important, but its proof is postponed.

Theorem 1.4. *Any discrete (additive) subgroup of $\mathbb{R}^n$ is a lattice.*

The method used in the proof of Theorem.**??**. can be better summarized into the following lemma.

Lemma 1.1. *A homeomorphism does not change discreteness and closedness.*

Proof. Let $h : A \to B$ be a homeomorphism where A, B are topological spaces. We want to prove

[3] I think Fu has added in the definition that a discrete set is by default closed, but the Internet says otherwise.

(i) $D \subset A$ is discrete $\implies h(D)$ is discrete.

(ii) $F \subset A$ is closed $\implies h(F)$ is closed.

For (i), let $y \in h(D)$, $x = h^{-1}(y) \in D$. Since D is discrete, there exists an open neighborhood U_x of x such that $U_x \cap D = \{x\}$. By the continuity of h^{-1}, there exists a neighborhood V_y of y such that $h^{-1}(V_y) \subset U_x$. Intersect with D on both side and take h to obtain:

$$h^{-1}(V_y) \cap D \subset U_x \cap D = \{x\} \implies V_y \cap h(D) \subset \{h(x)\} \implies V_y \cap h(D) = \{y\}$$

For (ii), $(h(F))^c = h(F^c) = (h^{-1})^{-1}(F^c)$, and we have F closed $\implies F^c$ open $\implies (h^{-1})^{-1}(F^c)$, being the preimage of F^c under h^{-1}, open $\implies h(F)$ closed.

Note 1.3. Warning: actually the second part seems problematic.

1.6 Completion and Dense Subsets

Completion arises in metric spaces, where Cauchy sequences can be defined. Let (X, d) be a metric space. The **completion** $(\hat{X}, \hat{d})$ of (X, d) is the space of equivalence classes of Cauchy sequences in X, with a metric $\hat{d}$ induced by d.

The completion has the following properties.

Theorem 1.5. *Let $(\hat{X}, \hat{d})$ be the completion of (X, d).*

(i) X is a subspace of $\hat{X}$ by the natural embedding

$$X \hookrightarrow \hat{X}, \ x \mapsto \{x\}$$

(ii) X is dense in $\hat{X}$.

(iii) A closed subspace of a complete space is complete.

A dense subset provide a criterion for completeness.

Theorem 1.6. ***(Exer.)****Let (X, d) be a metric space. Let D be a dense subset of X. If $\overline{D} = \hat{D} \subset X$, then X is complete.*

Dense subsets have another nice property.

Theorem 1.7. *Let (X, d) be a metric space. Let $S \subset L \subset X$ and S dense in L and L dense in X. Then S is dense in X.*

Proof. For any $x \in X$, we find $\{l_n\} \subset L$ such that

$$d(l_n, x) \leqslant \frac{1}{2n}$$

and for each l_n we find $s_n \in S$ such that

$$d(l_n, s_n) \leqslant \frac{1}{2n}$$

Then

$$d(x, s_n) \leqslant \frac{1}{n} \to 0$$

2 Modules in an Algebraic Number Field

2.1 Definitions and Properties

Module Let K be an algebraic number field and $\mu_1, \cdots, \mu_n \in K$. The $\mathbb{Z}$-module M generated by the finitely many elements $\mu_1, \cdots, \mu_n$

$$M = \{r_1\mu_1 + \cdots + r_n\mu_n,\ r_i \in \mathbb{Z}\}$$

is simply called a **module** in K. In other words, a **module** in an algebraic number field is a finitely generated $\mathbb{Z}$-module in K. If the generators are linearly independent, then they form a **basis**. The cardinality of each basis is unique, and is called the **rank** of the module. Two modules M_1, M_2 are called **similar** if $M_1 = \alpha M_2$ for some $\alpha \neq 0$ in K. A module in K is called **full** if it contains a basis of $K/\mathbb{Q}$, i.e., $[K : \mathbb{Q}]$ linearly independent elements in K, otherwise **nonfull**.

Note 2.1. Even though a module in K cannot have more than $n = [K : \mathbb{Q}]$ linearly independent elements, it may not be finitely generated. For example, $\mathbb{Q}$ is not a finitely generated module over $\mathbb{Z}$, but any two elements in $\mathbb{Q}$ are linearly dependent. However, if it is finitely generated, we can always reduce the generators to less than n generators.

Now we move to properties of modules in an algebraic number field.

(i) Any module in an algebraic number field is free, i.e., has a basis.

Proof. Recall that a finitely generated torsion-free module over a PID must be free.

(ii) An additive subgroup of a module is also a module.

Note 2.2. I have no idea why this is a theorem.

Note 2.3. Now I know. One needs to verify that it is finitely generated.

(iii) A basis for a full module is also a basis for the field extension. Conversely, though a basis for an extension may not be a basis for a full module, there exists $c \in \mathbb{Z}$ such that c times the basis is in the module and hence is a basis of this module.

Ring of coefficients Let K be an algebraic number field and M a module in K. A number $\alpha \in K$ is called a **coefficient** if $\alpha M \subset M$. The set of all coefficients form a ring $\mathcal{O}_M$ called the **ring of coefficients** of M. $\mathcal{O}_M$ has the following properties.

(i) $\mathcal{O}_M$ is a commutative ring with identity.

Note 2.4. Even though the definition of $\mathcal{O}_M$ seems to coincide with $(M : M)$, they are not the same. The former is chosen from K while the latter is from $\mathbb{Z}$ (actually $(M : M) = \mathbb{Z}$). However, obviously we have $\mathbb{Z} = (M : M) \subset \mathcal{O}_M$.

Note 2.5. We may not conclude from $\mathcal{O}_M$ being an additive group in K that $\mathcal{O}_M$ is a module in K, because $\mathcal{O}_M$ may not be finitely generated. See (iii) below.

(ii) If $\alpha \in K$ is such that $\alpha\mu_i \in M$ for a basis $\mu_1, \cdots, \mu_n$ of M, then $\alpha \in \mathcal{O}_M$.

(iii) $\mathcal{O}_M$ is a module.

Proof. Let $\gamma \in M$ be nonzero, then $\gamma\mathcal{O}_M \subset M$ is a additive subgroup of M and hence a module. It follows that $\mathcal{O}_M$ is also a module.

(iv) If M is full in K, then $\mathcal{O}_M$ is full in K.

Proof. Let $\mu_1, \cdots, \mu_n$ be a basis for M. Show that for each $\alpha \in K$ there exists some $c \in \mathbb{Z}$ such that $c\alpha \in \mathcal{O}_M$. And then prove that for a basis $\alpha_1, \cdots, \alpha_n$ for $K/\mathbb{Q}$ there is a $c \in \mathbb{Z}$ such that $c\alpha_1, \cdots, c\alpha_n \subset \mathcal{O}_M$ and hence $\mathcal{O}_M$ is full.

Note 2.6. **(Theorem)**

$$M \text{ is full in } K \iff \forall \alpha \in K,\ \exists c \in \mathbb{Z},\ c\alpha \in M$$

Proof. ($\Rightarrow$) Expand α with respect to a basis of M. ($\Leftarrow$) Choose a basis $\alpha_1, \cdots, \alpha_n$ of $K/\mathbb{Q}$.

(v) $\mathcal{O}_{\gamma M} = \mathcal{O}_M$ for $\gamma \neq 0$

(vi) $\mathcal{O}_{\mathcal{O}_M} = \mathcal{O}_M$

(vii) $\mathcal{O}_M$ for any full module M is an order (see below).

Order An **order** $\mathcal{O}$ of an algebraic number field K is a full module that is also a ring with identity. An element ε in an order $\mathcal{O}$ is call a **unit** of the ring if $\varepsilon, \varepsilon^{-1} \in \mathcal{O}$. Two numbers μ_1, μ_2 in a full module M are **associates** if $\mu_1/\mu_2 \in \mathcal{O}_M^*$. The following are true.

(i) (**Equivalent definitions for the units**) Let $\mathcal{O}_M$ be the ring of coefficients of a full module M, we have

$$\varepsilon, \varepsilon^{-1} \in \mathcal{O}_M \iff \varepsilon M = M \iff N(\varepsilon) = \pm 1$$

(ii) Let $\mathcal{O}$ be an order and $a \in \mathcal{O}$. Then the minimal and characteristic polynomials of a have integer coefficients.

Proof. Choose a basis for $\mathcal{O}$ and for any

(iii) An order $\mathcal{O}$ contains only finitely many nonassociate elements of given norm. The same is true for a full module.

Algebraic integers An **algebraic integer** a in an algebraic number field K is a number whose minimal polynomial has integer coefficients. All algebraic integers form a ring R called the **ring of algebraic integers**. The following are true.

(i) An algebraic integer has integer norm and trace.

Proof. What is the relation between the norm, the trace and the coefficients of the minimal polynomial?

(ii) $a \in R \implies \mathbb{Z}[a]$ is both a module and a ring in K.

(iii) $\mathcal{O}$ is any order, $a \in R \implies \mathcal{O}[a]$ is an order.

(iv) R is an order, and R is the maximal order of K in the sense that any other order is contained in it.

Proof. Note that any element in an order is an algebraic integer. The maximality is therefore evident, and it remains to show that R is an order, i.e., a ring with 1 and a full module. For the ring part, see Example.**??**; for the module part see Example.**??**; for the full part see Note.**??**.

Discriminant A bit troublesome. See Sect.**??**.

3 The Space $L^{s,t}$ and the Dirichlet Theorem

Let $\mathcal{O}$ be an order in K. We have shown that the problem of solving an equation in a full module can be converted to solving it in its ring of coefficient, which is an order. The equation solving is then again decomposed into two parts: (i) find enough (finite) particular solutions; (ii) find all units in $\mathcal{O}$, i.e., $\mathcal{O}^*$. And this section is focused on the second part. To understand the structure of $\mathcal{O}^*$, we design a mapping $L : K^* \to \mathbb{R}^{s+t}$ and study $\mathrm{Ker}(L|_{\mathcal{O}^*})$ and $\mathrm{Im}(L|_{\mathcal{O}^*}) = L(\mathcal{O}^*)$ respectively, the second part of which is known as the Dirichlet's theorem.

3.1 $L^{s,t}$ and $\mathbb{R}^{s+t}$

Let K be an algebraic number field, and $\sigma_1, \cdots, \sigma_s, \sigma_{s+1}, \overline{\sigma}_{s+1}, \cdots, \sigma_{s+t}, \overline{\sigma}_{s+t}$ all possible embeddings from K to $\mathbb{C}$, among which the first s embeddings are real, and the rest are complex. In the following text, we use s, t with the tacit understanding that they denote respectively the number of real embeddings and half of the number of complex embeddings, and that $n = s + 2t$ is the dimension of the extension $K/\mathbb{Q}$.

The space $L^{s,t}$ The following set is called the **space** $L^{s,t}$.

$$\begin{aligned} L^{s,t} &= \mathbb{R}^s \times \mathbb{C}^t \\ &= \{(x_1, \cdots, x_s, x_{s+1}, \cdots, x_{s+t}) : x_1, \cdots, x_s \in \mathbb{R},\ x_{s+1}, \cdots, x_{s+t} \in \mathbb{C}\} \end{aligned}$$

It is a real vector space of dimension $s + 2t$, with the **standard basis**

$$\begin{aligned} e_1 &= (1, \cdots, 0, 0, \cdots, 0) \\ e_s &= (0, \cdots, s, 0, \cdots, 0) \\ &\vdots \\ e_{s+1} &= (0, \cdots, 0, 1, \cdots, 0) \\ e'_{s+1} &= (0, \cdots, 0, i, \cdots, 0) \\ &\vdots \\ e_{s+t} &= (0, \cdots, 0, 0, \cdots, 1) \\ e'_{s+t} &= (0, \cdots, 0, 0, \cdots, i) \end{aligned}$$

One can use the following mapping $X : K \to L^{s,t}$ to embed an algebraic number field into the space $L^{s,t}$.

$$\begin{aligned} X : K &\to L^{s,t} \\ \alpha &\mapsto (\sigma_1\alpha, \cdots, \sigma_s\alpha, \sigma_{s+1}\alpha, \cdots, \sigma_{s+t}\alpha) \end{aligned}$$

This mapping has the following properties.

(i) (**Preserving bases**) If $\alpha_1, \cdots, \alpha_n$ is a basis for $K/\mathbb{Q}$, then $X\alpha_1, \cdots, X\alpha_n$ is a basis for $L^{s,t}$ over $\mathbb{R}$.

(i′) (**Preserving linear independence**) If $\beta_1, \cdots, \beta_k$ are linearly independent over $K/\mathbb{Q}$, then $X\beta_1, \cdots, X\beta_k$ are independent over $\mathbb{R}$.

(ii) (**Turning a full module into a full lattice**) If M is a full module in K with basis $\alpha_1, \cdots, \alpha_n$, then $X(M)$ is a full lattice in $L^{s,t}$ as a real vector space.

Proof. (i) The is done by directly computing the determinant of the matrix formed by the coordinates of $X\alpha_1, \cdots, X\alpha_n$ under the standard basis, which is

$$\begin{vmatrix} \sigma_1\alpha_1 & \cdots & \sigma_s\alpha_1 & \operatorname{Re}\sigma_{s+1}\alpha_1 & \operatorname{Im}\sigma_{s+1}\alpha_1 & \cdots & \operatorname{Re}\sigma_{s+t}\alpha_1 & \operatorname{Im}\sigma_{s+t}\alpha_1 \\ \vdots & & \vdots & \vdots & \vdots & & \vdots & \vdots \\ \vdots & & \vdots & \vdots & \vdots & & \vdots & \vdots \\ \sigma_1\alpha_1 & \cdots & \sigma_s\alpha_1 & \operatorname{Re}\sigma_{s+1}\alpha_1 & \operatorname{Im}\sigma_{s+1}\alpha_1 & \cdots & \operatorname{Re}\sigma_{s+t}\alpha_1 & \operatorname{Im}\sigma_{s+t}\alpha_1 \end{vmatrix}$$

$$= \frac{1}{(-2i)^t} \begin{vmatrix} \sigma_1\alpha_1 & \cdots & \sigma_s\alpha_1 & \sigma_{s+1}\alpha_1 & \overline{\sigma}_{s+1}\alpha_1 & \cdots & \sigma_{s+t}\alpha_1 & \overline{\sigma}_{s+t}\alpha_1 \\ \vdots & & \vdots & \vdots & \vdots & & \vdots & \vdots \\ \vdots & & \vdots & \vdots & \vdots & & \vdots & \vdots \\ \sigma_1\alpha_1 & \cdots & \sigma_s\alpha_1 & \sigma_{s+1}\alpha_1 & \overline{\sigma}_{s+1}\alpha_1 & \cdots & \sigma_{s+t}\alpha_1 & \overline{\sigma}_{s+t}\alpha_1 \end{vmatrix}$$

Note 3.1. Use only elementary operations to obtain

$$(\operatorname{Re}\alpha, \operatorname{Im}\alpha) \mapsto (\alpha, \overline{\alpha})$$

is easy exercise.

If we denote the matrix inside by A, then by direct computation, the (i, j)-element of AA^T is

$$\begin{pmatrix} \sigma_1\alpha_i & \cdots & \sigma_s\alpha_i & \sigma_{s+1}\alpha_i & \overline{\sigma}_{s+1}\alpha_i & \cdots & \sigma_{s+t}\alpha_i & \overline{\sigma}_{s+t}\alpha_i \end{pmatrix} \begin{pmatrix} \sigma_1\alpha_j \\ \cdots \\ \sigma_s\alpha_j \\ \sigma_{s+1}\alpha_j \\ \overline{\sigma}_{s+1}\alpha_j \\ \cdots \\ \sigma_{s+t}\alpha_j \\ \overline{\sigma}_{s+t}\alpha_j \end{pmatrix}$$

$$= \sum_{k=1}^{s} \sigma_k(\alpha_i\alpha_j) + \sum_{k=1}^{t} (\sigma_{s+k}(\alpha_i\alpha_j) + \overline{\sigma}_{s+k}(\alpha_i\alpha_j))$$
$$= \mathrm{Tr}(\alpha_i\alpha_j)$$

Then $AA^T = (\mathrm{Tr}(\alpha_i\alpha_j))$, which has a nonzero determinant if $\alpha_1, \cdots, \alpha_n$ is a basis for K over $\mathbb{Q}$ (see Sect.**??**.). It follows that $\det(A) \neq 0 \implies X\alpha_1, \cdots, X\alpha_n$ are linearly independent. In short, first we transform the coordinate matrix into the conjugate form, and then consider the transformed matrix multiplied by its transpose.

(i′) This is a simple corollary. First expand $\beta_1, \cdots, \beta_k$ to a basis, then use (i).

(ii) This follows from (i). Writing $X(M)$ in terms of $X\alpha_1, \cdots, X\alpha_n$ should do the job.

Using the mapping $X : K \to L^{s,t}$, we take a structure in K to a structure in $L^{s,t}$, and by studying the latter we may be able to characterize the structure of the former. We have shown that a module is mapped to a lattice, hence a further examination requires some understanding about lattices in $L^{s,t}$, i.e., $\mathbb{R}^n$, and this is separated as an individual text (see Sect.**??**.).

Embedding $L^{s,t}$ into $\mathbb{R}^{s+t}$ Besides the addition structure of $L^{s,t}$ (being a vector space), it also has a componentwise multiplication structure. Under the mapping $X : K \to L^{s,t}$, the componentwise multiplication corresponds to the multiplication of elements in K, and hence is of great importance. For we to examine this structure more easily, we embed $L^{s,t}$ once again into $\mathbb{R}^{s+t}$ with a logarithm-like mapping, changing the multiplication into addition. Consider the mapping

$$\begin{aligned} \mathrm{Log} : L^{s,t} &\to \mathbb{R}^{s+t} \\ (x_1, \cdots, x_{s+t}) &\mapsto (\log|x_1|, \cdots, \log|x_s|, \log|x_{s+1}|^2, \cdots, \log|x_{s+t}|^2) \end{aligned}$$

Note 3.2. Note that each x_i should be nonzero.

3.2 The Structure of $\mathrm{Ker}(L|_{\mathcal{O}^*})$

On the structure of $\mathcal{O}^*$, we have the following theorem.

Theorem 3.1. *Let $\mathcal{O}$ be an order in an algebraic number field K. Let $L = \mathrm{Log} \circ X$ be the mapping*

$$\begin{aligned} L : K^* &\to \mathbb{R}^{s+t} \\ \alpha &\mapsto (\log|\sigma_1\alpha|, \cdots, \log|\sigma_s\alpha|, \log|\sigma_{s+1}\alpha|^2, \cdots, \log|\sigma_{s+t}\alpha|^2) \end{aligned}$$

Then L is a homomorphism in the sense that K^* is a multiplicative group while $\mathbb{R}^{s+t}$ is an additive group. And we have

$$\begin{aligned}\mathrm{Ker}(L|_{\mathcal{O}^*}) &= \{\text{All elements in } \mathcal{O} \text{ that is a root of unity}\} \\ &= \{\xi \in \mathcal{O} : \xi^k = 1 \text{ for some } k\}\end{aligned}$$

And more over $\mathrm{Ker}(L|_{\mathcal{O}^*})$ *is finite and has even order.*

4 Theory of Divisors and Valuations

4.1 Theory of Divisors and the Class Group

The base structure of a theory of divisors we are about to define is a commutative monoid. Let $\mathcal{D}$ be a **commutative monoid**. Let $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}, \mathfrak{p} \in \mathcal{D}$. We say $\mathfrak{b}$ **divides** $\mathfrak{a}$ (written as $\mathfrak{b}\big|\mathfrak{a}$) if $\mathfrak{a} = \mathfrak{b}\mathfrak{c}$ for some $\mathfrak{c} \in \mathcal{D}$. $\mathfrak{p}$ is called **irreducible** if $\mathfrak{p} = \mathfrak{b}\mathfrak{c} \implies \mathfrak{b} = 1$ or $\mathfrak{c} = 1$. $\mathcal{D}$ is said to have the **unique factorization property** if each $\mathfrak{a}$ is a unique product of irreducible elements in $\mathcal{D}$.

Note 4.1. These definitions arise form the analysis of ideals. All nonzero ideals of a ring form a commutative monoid under multiplication, with (1) being the identity.

Note 4.2. Recall that in a Dedekind domain every nonzero ideal has a unique factorization as a product of prime ideals.

Let R be an integral domain. A **theory of divisors** on R is a pair $(\mathcal{D}, \tau)$, where $\mathcal{D}$ is a unique factorization commutative monoid, and $\tau : R\backslash\{0\} \to \mathcal{D}$ a monoid homomorphism (we usually write $\tau(a) = (a)$) satisfying

(i) $(ab) = (a)(b)$ (homomorphism)

(ii) $a\big|b \iff (a)\big|(b)$

(iii) $\forall \mathfrak{a} \in \mathcal{D}$, the set $I(\mathfrak{a}) = \{a \in R\backslash\{0\} : \mathfrak{a}\big|(a)\} \cup \{0\}$ is an ideal of R.

(iv) $\mathfrak{a}, \mathfrak{b} \in \mathcal{D},\ I(\mathfrak{a}) = I(\mathfrak{b}) \implies \mathfrak{a} = \mathfrak{b}$

Example 4.1. Let R be a Dedekind domain and $\mathcal{D}$ its nonzero ideals. Let τ be the mapping $\tau : R\backslash\{0\} \to \mathcal{D}, a \mapsto (a)$. Then $(\mathcal{D}, \tau)$ is a theory of divisors on R. □

Example 4.2. The ring of algebraic integers in an algebraic number field is a Dedekind domain. □

Moreover, we can define a mapping on R and its field of fractions K, if R is a integral domain equipped with a theory of divisors $(\mathcal{D}, \tau)$. Since $\mathcal{D}$ is a UFCM[4], we can let $\mathcal{P}$ be the set of irreducible elements in $\mathcal{D}$. Then the unique factorization property says for any $a \in R\backslash\{0\}$, we can write (a) as a unique product

$$(a) = \prod_{\mathfrak{p} \in \mathcal{P}} \mathfrak{p}^{n_{\mathfrak{p}}}$$

where each $n_{\mathfrak{p}}$ is uniquely determined by a (hence we can write $n_{\mathfrak{p}} = v_{\mathfrak{p}}(a)$ to emphasize the dependence) and only finitely many $n_{\mathfrak{p}} \geqslant 0$ are nonzero. Then we have defined the mapping

$$\begin{array}{rcccl} v_{\mathfrak{p}} & : & R\backslash\{0\} & \to & \mathbb{Z}_{\geqslant 0} \\ & & a & \mapsto & v_{\mathfrak{p}}(a) \end{array}$$

This can be naturally extended to K^*.

This map $v_{\mathfrak{p}}$ (extended to K^*) satisfies all axioms of a (discrete) valuation.

Theorem 4.1. *The map $v_{\mathfrak{p}}$ defined above is a valuation, that is,*

(i) v *is surjective.*

(ii) $v(xy) = v(x) + v(y)$ *(homomorphism)*

(iii) $v(x + y) \geqslant \min(v(x), v(y))$

The following are some example of valuations.

Example 4.3. Let K be the field of all meromorphic functions on $\mathbb{P}^1$. For every $f \in K^*$, define $v_a(f)$ to be the order of the zero/pole (positive if a is a zero; negative if a pole) of f at a. Then v_a is a valuation. □

Example 4.4. Let K be the field of rational functions $\mathbb{F}(x)$ and define $v_\infty(f) = -\deg(f)$. Then v_∞ is a valuation. □

Example 4.5. Let C be a compact Riemann surface. Let K be the field of meromorphic functions on C. Define $\mathrm{Div}(C) = \mathbb{Z}^{(C)}$,[5] whose elements are called the **divisors** on C. Let $\tau : K^* \to \mathrm{Div}(C), f \mapsto (f) = \sum_{a \in C} v_a(f)a$. Since C is compact and f is nonzero meromorphic, the sum is finite. Then $(\mathrm{Div}(C), \tau)$ is a theory of divisors on K. And $\mathrm{Coker}\tau = \mathrm{Div}(C)/\mathrm{Im}(\tau)$ is called the **class group** of C. And elements in $\mathrm{Im}(\tau)$ are called the **principal divisors**. □

We now move to generalize the notion of the class group. Let R be an integral domain. $(\mathcal{D}, \tau : a \mapsto (a))$ a theory of divisors on R. Let $\mathcal{P}$ be the set of all irreducible elements in $\mathcal{D}$. Define the **divisors** on R to be $\mathrm{Div} = \mathbb{Z}^{(\mathcal{P})}$. The unique factorization property of $\mathcal{D}$ implies $\mathcal{D} \subset \mathrm{Div}$.[6] Let τ extend to K^* and define the

[4]Unique factorization commutative monoid.

[5]The free abelian group generated by all points in C.

[6]So the set of divisors may be much larger than the theory of divisors.

principal divisors to be the image of the mapping τ, i.e., all elements in $\mathcal{D}$ of the form (f) with $f \in K^*$. The **class group** of R is defined as $\mathrm{Cl}(R) = \mathrm{Div}/\mathrm{Im}(\tau)$.[7].

Note 4.3. $\mathrm{Im}(\tau) \subset \mathcal{D} \subset \mathrm{Div}$

We have the following theorem concerning the class group.

Theorem 4.2. $\mathrm{Cl}(R)$ *is a finite abelian group.*

Proof. No proof here.

Following the theorem, $\#\mathrm{Cl}(R)$ is called the **class number** of K.

Theorem 4.3. $\mathrm{Cl}(R) = \{0\} \iff R$ *is a PID.*

Example 4.6. When these concepts are applied to an algebraic number field $K \supset \mathbb{Q}$, we have

$$\begin{aligned} R &= \text{algebraic integers in } K \\ \mathcal{D} &= \text{nonzero ideals of } R \\ \tau &: a \mapsto (a) \end{aligned}$$

4.2 Discrete Valuations and Normed Fields

A **discrete valuation** on a field K is a mapping $v : K^* \to \mathbb{Z}$ such that

(i) v is surjective.

(ii) $v(xy) = v(x) + v(y)$ (homomorphism)

(iii) $v(x+y) \geqslant \min(v(x), v(y))$

For convenience we put $v(0) = +\infty$ in addition. The valuation induces a **norm** $\|\cdot\|$ on K by defining

$$\|\cdot\| = \lambda^{v(x)}, \text{ for some } 0 < \lambda < 1$$

We can check that

(i) $\|ab\| = \|a\| \, \|b\|$

(ii) $\|a+b\| \leqslant \max(\|a\|, \|b\|)$

(iii) $\|x\| = 0 \iff x = 0$

[7] Class group=divisors/principal divisors

That is, $\|\cdot\|$ satisfies all the axioms of a norm and in addition a *stronger triangle inequality*.

Example 4.7. The p-adic valuation v_p on $\mathbb{Q}$ induces the p-adic norm $\|\cdot\|_p = \left(\frac{1}{p}\right)^{v_p(\cdot)}$. The number $\frac{1}{p}$ is chosen out of respect to p.

Before we advance, we discuss some properties of the norm on a field. Let $(K, \|\cdot\|)$ be a normed field. Some times these norms satisfy a strong triangle inequality of the form $\|a+b\| \leqslant \max(\|a\|, \|b\|)$, which has an equivalent condition.

Theorem 4.4. $\|a+b\| \leqslant \max(\|a\|, \|b\|) \iff \forall n \in \mathbb{N},\ \|n\| \leqslant 1$

Proof. ("$\Rightarrow$") easy. ("$\Leftarrow$") Use the hypothesis on the binomial coefficients: consider $\|a+b\|^n = \|(a+b)^n\|$.

The notion of the norm can be generalized to rings (The axioms are exactly the same).

The Ostrowski theorem gives all possibilities of the norms on $\mathbb{Q}$.

Theorem 4.5. *Any norm on $\mathbb{Q}$ is one of the three.*

(i) The 0-1 trivial norm $|\cdot|_\infty^0$.

(ii) The absolute value with a power $|\cdot|_\infty^\alpha$, with $0 < \alpha \leqslant 1$.

(iii) The p-adic norm $\|\cdot\|_p = \lambda^{v_p(\cdot)}$ for some prime number p and some $0 < \lambda < 1$.

Proof. Since $\mathbb{Q}$ is the field of fractions of $\mathbb{Z}$, it suffices to prove the Ostrowski theorem for $\mathbb{Z}$.

Theorem 4.6. *Any norm on $\mathbb{Z}$ is one of the three.*

(i) The norm induced on $\mathbb{Z}/(p)$.*

(i) The 0-1 trivial norm $|\cdot|_\infty^0$.

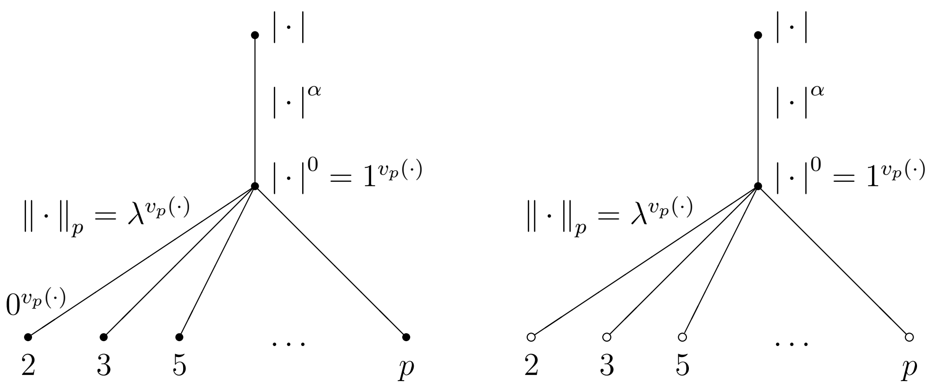
(ii) The absolute value with a power $|\cdot|_\infty^\alpha$, with $0 < \alpha \leqslant 1$.

(iii) The p-adic norm $\|\cdot\|_p = \lambda^{v_p(\cdot)}$ for some prime number p and some $0 < \lambda < 1$.

Proof. First notice that in either case, $\|1\| = 1$. Then we remark that these two cases (a), (b) leads to (ii) and (iii) respectively.[8]
(a) $\exists N \in \mathbb{N},\ \|N\| > 1$
(b) $\forall N \in \mathbb{N},\ \|N\| \leqslant 1$
And taking the limit yields the other one.

[8] We have exhibited the theorem that a strong triangle inequality is equivalent to (b), so it is an educated guess that (b) leads to (iii).

Each of the possible norms corresponds to a point of the following diagrams, which are called the **Berkovich spaces** on $\mathbb{Z}$ (left) and $\mathbb{Q}$ (right).



4.3 Properties of Discrete Valuations

4.3.1 Single Valuation

Let $v : K^* \to \mathbb{Z}$ be a discrete valuation on the field K. Then v satisfies the following properties.

Theorem 4.7. *The following are true for v.*

(i) v *is surjective.*

(ii) v *is homomorphism.*

(iii) $v(x+y) \geqslant \min(v(x),(y))$.

(iv) $v(x) \neq v(y) \implies v(x+y) = \min(v(x), v(y))$

Proof. The first three are axioms. It suffices to prove the last. Wlog suppose that $v(x) > v(y)$ and the goal is then to prove $v(x+y) = v(y)$. Suppose not then we must have $v(x+y) > v(y) = v((x+y)-x) \geqslant \min(v(x+y), v(x)) > v(y)$.

Note 4.4. The key is $v(y) \geqslant \min(v(x+y), v(x))$.

4.3.2 Distinct Valuations

Theorem 4.8. *Distinct valuations are independent. Let K be a field and $v_1, \cdots, v_m : K^* \to \mathbb{Z}$ distinct valuations on K.*

(i) For integers $\lambda_1, \cdots, \lambda_m$*,*

$$\lambda_1 v_1 + \cdots + \lambda_m v_m = 0 \implies \lambda_1 = \cdots = \lambda_m = 0$$

(ii) There exists $x \in K^*$ *such that*

$$v_1(x) = k_1,\ v_2(x) = k_2,\ \cdots,\ v_m(x) = k_m$$

for any predesignated $k_1, \cdots, k_m \in \mathbb{Z}$*.*

An important corollary is in order.

Theorem 4.9. ***(Approximation theorem)*** *Let* K *be a field with distinct valuations* $v_1, \cdots, v_m : K^* \to \mathbb{Z}$ *and denote the norms induced by* v_i *by* $\|\ \|_i = \lambda^{v_i(\ )}$ *for some* $0 < \lambda < 1$*. For any* $a_1, \cdots, a_m$ *we can find* $x \in K$ *to approximate them all. The formulation is as follows.*

(i) For any $N \in \mathbb{Z}$ *there exists* $x \in K$ *such that*

$$v_1(x - a_1) \geqslant N,\ \cdots,\ v_m(x - a_m) \geqslant N$$

(ii) If $a_1, \cdots, a_m \in \mathbb{Z}$ *and* $p_1, \cdots, p_m$ *are distinct prime numbers, then for any* $N \geqslant 0$*, there exists* $x \in \mathbb{Z}$ *such that*

$$\begin{aligned} x &\equiv a_1 \pmod{p_1^N} \\ &\vdots \\ x &\equiv a_m \pmod{p_m^N} \end{aligned}$$

(iii) For any $\varepsilon > 0$ *there exists* $x \in K$ *such that*

$$\|x - a_1\|_1 \leqslant \varepsilon,\ \cdots,\ \|x - a_m\|_m \leqslant \varepsilon$$

(iv) The product space

$$(K, \|\ \|_1) \times \cdots \times (K, \|\ \|_m)$$

has a dense diagonal.

Note 4.5. If we are considering $(\mathbb{Q}, \|\ \|_p = \left(\frac{1}{p}\right)^{v_p(\ )})$, then note that $\|p^k\| = \|p^k \frac{a}{b}\|$, hence we can always assume an integer if we only want to fix the norm.

Theorem 4.10. ***(Riemann-Roch)*** *Let* C *be a compact Riemann surface and* g *the genus of* C*. Let* $K(C)$ *the field of all meromorphic functions on* C*. Let* $D = \sum_{p \in C} n_p p$ *be a divisor, and let*

$$l(D) = \dim\{f \in K(C) : (f) + D \geqslant 0\}$$

Then $l(D) \geqslant 1 - g + \deg D,\ l(D) - l((f) - D) = 1 - g + \deg D$*.*

Note 4.6. The set $\{f \in K(C) : (f) + D \geqslant\}$ is a $\mathbb{C}$-linear space. Note that $(f) = \sum_{p \in C} v_p(f)p$. Hence the expression $(f) + D \geqslant 0$ means $v_p(f) + n_p \geqslant 0$ for all $p \in C$.

4.3.3 Extension and Restriction

The extension of a valuation is associated to the extension of a field. But unlike an extension of a mapping, the **ramification index** comes into play when we extend valuations.

Let $K \subset L$ be an extension of fields. A discrete valuation $v' : L^* \to \mathbb{Z}$ on L can be restricted to K in the following manner. Note that $v'(K^*)$ is a subgroup of $\mathbb{Z}$ and hence has the form of an ideal[9] $v'|_{K^*} \neq e\mathbb{Z}$. Then if $e \neq 0$, the new mapping

$$v = \frac{v'|_{K^*}}{e} : K^* \to \mathbb{Z}$$

is a valuation on K, called the **restriction** of v' to K^*. Conversely, if $v : K^* \to \mathbb{Z}$ is a valuation on K such that $v'|_{K^*} = ev$ then v' is called an **extension** of v to L. The integer e is call the **ramification index**.

4.3.4 *Valuation and Distance

We know that a valuation v induces a norm $\|\cdot\|_v = \lambda^v(\cdot)$ with some $0 < \lambda < 1$. We have

$$\|x\| \text{ arbitrarily small } \iff v(x) \text{ arbitrarily large}$$

This norm satisfies a stronger triangle inequality

$$\|a + b\| \leqslant \max(\|a\|, \|b\|)$$

Hence we have this **amazing** result

$$\|a_i\| < \varepsilon \implies \|a_1 + \cdots + a_m\| < \varepsilon$$

This greatly simplifies the criterion for a Cauchy series.

Theorem 4.11. *Let $\sum_i x_i$ be a series with terms in K, whose norm is defined by a valuation. Then it is a Cauchy sequence if one of these equivalent conditions holds.*

(i) $\forall \varepsilon > 0,\ \exists N > 0,\ \forall m, n \geqslant N,\ \|x_n + \cdots + x_m\| < \varepsilon$

(ii) $\forall M > 0,\ \exists N > 0,\ \forall m, n \geqslant N,\ v(x_n + \cdots + x_m) > M$

(1) $\|x_n\| \to 0$

(2) $v(x_n) \to \infty$

Note 4.7. Note that this does not ensure the convergence of the series unless we assume K to be complete.

[9] A subgroup of $\mathbb{Z}$ is also an ideal.

4.4 The Valuation Ring

Let K be a field and $v : K^* \to \mathbb{Z}$ a discrete valuation on K. The subset

$$R = \{x \in K : v(x) \geqslant 0\}$$

is a subring of K, called the **valuation ring** or **integer ring** of K.

Note 4.8. Since $v(x) \geqslant 0 \iff \|x\| \leqslant 1$, one can see R as the unit ball in K.

Other important subsets should also be introduced.

$$\mathfrak{m} = \{x \in K : v(x) \geqslant 1\}$$

is the (only) maximal ideal of R.

Note 4.9.

$$\mathfrak{m}^n = \{x \in K : v(x) \geqslant n\}$$

$$R^* = \{x \in K : x, x^{-1} \in R\} = \{x \in K : v(x) = 0\}$$

is the invertible elements of R.

The following are some properties of R.

Theorem 4.12. *Let R be the valuation ring of (K, v). Let $\mathfrak{m}$ be defined as above.*

(i) *R is local with $\mathfrak{m}$ being its only maximal ideal.*

(ii) $\mathfrak{m}^n = \{x \in K : v(x) \geqslant n\}$

(iii) $R^* = \{x \in K : v(x) = 0\}$

(iv) *π for which $v(\pi) = 1$ is so special that any $x \in K$ has a unique factorization $x = \eta\pi^{v(x)}$ with $\eta \in R^*$.*

(v) *R is a PID.*

I would like to call a $\pi \in K$ such that $v(\pi) = 1$ a **regular** element of v. Note that all regular elements are associates in R.

4.5 Power Series Development

Let (K, v) be a valued field, R its valuation ring and $\mathfrak{m}$ the maximal ideal of R. Let $\pi \in K$ have value $v(\pi) = 1$. Let the set $S \subset R$ consist of *exactly one* preimage of each element in $R/\mathfrak{m}$. We construct the power series development as follows.

Theorem 4.13. *For any $x \in R$, we can write $x = \xi + \pi x'$ with $\xi \in S,\ x' \in R$.*

Proof. By the definition of S and the UFD property of R.

Theorem 4.14. *For any $x \in R$, we can write $x = \sum_{k=0}^{\infty} \xi_k \pi^k$ with $\xi_k \in S$.*

Proof. Repeatedly use the last theorem.

Theorem 4.15. *For any $x \in K$, we can write $x = \sum_{k=0}^{\infty} \xi_k \pi^k$ with $\xi_k \in S$.*

Proof. If $x \in R$ then we are done. If $v(x) < 0$, then let $n = -v(x)$ and $x = \frac{\eta}{\pi^n}$ with $\eta \in R^*$. Hence we have $\eta = \sum_{k=0}^{\infty} a_{k-n} \pi^k$ and $x = \frac{a_{-n}}{\pi^n} + \frac{a_{-(n-1)}}{\pi^{n-1}} + \cdots + a_0 + \frac{a_1}{\pi} + \frac{a_2}{\pi^2} + \cdots$.

Next we consider its completion $(\hat{K}, \hat{v})$, and the following sets.

$$\begin{aligned} R &= \{x \in K : v(x) \geqslant 0\} \quad , \quad \hat{R} = \{x \in \hat{K} : \hat{v}(x) \geqslant 0\} \\ \mathfrak{m} &= \{x \in K : v(x) \geqslant 1\} \quad , \quad \hat{\mathfrak{m}} = \{x \in \hat{K} : \hat{v}(x) \geqslant 1\} \end{aligned}$$

Then

Theorem 4.16. *(i) $\hat{R}$ is closed and hence complete.*

(ii) R is dense in $\hat{R}$.

If no valuation is given and we have only a norm, then consider a normed field $(K, |\cdot|)$. Choose some $\pi \in K$ with $|\pi| < 1$, say $|\pi| = 1/10$. Let $R = \{x \in K : |x| \leqslant 1\}$ and $S \subset R$ be such that $\forall x \in R,\ \exists a \in S,\ |x - a| \leqslant |\pi|$. Then we have

Theorem 4.17. *Let $(K, |\cdot|)$ be a normed field and let R, S be as above. Then for any $x \in K$, we can write $x = \sum_{k=0}^{\infty} a_k \pi^k$ with $a_k \in S$.*

Proof. The condition $R = \{x \in K : |x| \leqslant 1\}$ is for iteration and the convergence of the final series.