Algebraic Number Theory

HHH

December 16, 2025

Contents

Chapter I

Ring Extensions

§1 Integral Extensions

Definition 1.1. *Let S be a commutative ring with identity and R a subring of S containing 1_S. Then S is said to be an **extension ring** of R.*

1. *An element $s \in S$ is said to be **integral** over R if s is a root of a monic polynomial in $R[x]$.*

2. *If every element of S is integral over R, S is said to be an **integral extension** of R.*

3. *The **integral closure** of R in S is the set of elements of S that are integral over R.*

4. *The ring R is said to be **integrally closed** in S if R is equal to its integral closure in S.*

   *The integral closure of an integral domain R in its field of fractions is called the **normalization** of R. An integral domain is called integrally closed or normal if it is integrally closed in its field of fractions.*

Remark. *If follows from corollary 1.3 that the integral closure of R in S is a subring of S containing R.*

Theorem 1.2. *Let S be an extension ring of R and $s \in S$. Then the following conditions are equivalent.*

1. *s is integral over R*

2. *Subring $R[s]$ is a finitely generated R-module*

3. *There is a subring T that $R[s] \subset T \subset S$, which is finitely generated as an R-module;*

4. *There is a faithful $R[s]$-submodule M which is finitely generated as an R-module.*

Corollary 1.3. *Let S be an extension ring of R. Then*

1. *If S is finitely generated as an R-module, then S is an integral extension of R.*

2. *If $s_1, \ldots, s_t \in S$ are integral over R, then $R[s_1, \ldots, s_t]$ is a finitely generated R-module and an integral extension ring of R.*

3. *If T is an integral extension ring of S and S is an integral extension ring of R, then T is an integral extension ring of R .*

Proposition 1.4. 1. *Every unique factorization domain is integrally closed.*

2. *In particular, the polynomial ring $F[x_1, \ldots, x_n]$ (F a field) is integrally closed in its quotient field $F(x_1, \ldots, x_n)$.*

Theorem 1.5. *Let S be a multiplicative subset of an integral domain R such that $0 \notin S$. If R is integrally closed, then $S^{-1}R$ is an integrally closed integral domain.*

Proof. $S^{-1}R$ is an integral domain and R may be identified with a subring of $S^{-1}R$ by **??**. Extending this identification, the quotient field $Q(R)$ of R may be considered as a subfield of the quotient field $Q(S^{-1}R)$ of $S^{-1}R$. Verify that $Q(R) = Q(S^{-1}R)$.

Let $u \in Q(S^{-1}R)$ be integral over $S^{-1}R$; then for some $r_i \in R$ and $s_i \in S$,

$$u^n + (r_{n-1}/s_{n-1})\, u^{n-1} + \cdots + (r_1/s_1)\, u + (r_0/s_0) = 0.$$

Multiply through this equation by s^n, where $s = s_0 s_1 \cdots s_{n-1} \in S$, and conclude that su is integral over R. Since $su \in Q(S^{-1}R) = Q(R)$ and R is integrally closed, $su \in R$. Therefore, $u = su/s \in S^{-1}R$, whence $S^{-1}R$ is integrally closed. □

Theorem 1.6. *Let S be an integral extension ring of R. Then the following statements hold.*

1. *Assume that S is an integral domain. Then R is a field if and only if S is a field.*

2. *Let $\mathfrak{p}$ be a prime ideal in R. Then there is a prime ideal $\mathfrak{q}$ in S with $\mathfrak{p} = \mathfrak{q} \cap R$.*

   Moreover, $\mathfrak{p}$ is maximal if and only if $\mathfrak{q}$ is maximal.

3. *(The Going-up Theorem) Let $\mathfrak{p}_1 \subseteq \mathfrak{p}_2 \subseteq \cdots \subseteq \mathfrak{p}_n$ be a chain of prime ideals in R and suppose there are prime ideals $\mathfrak{q}_1 \subseteq \mathfrak{q}_2 \subseteq \cdots \subseteq \mathfrak{q}_m$ of S with $\mathfrak{p}_i = \mathfrak{q}_i \cap R, 1 \leq i \leq m$ and $m < n$. Then the ascending chain of ideals can be completed: there are prime ideals $\mathfrak{q}_{m+1} \subseteq \cdots \subseteq \mathfrak{q}_n$ in S such that $\mathfrak{p}_i = \mathfrak{q}_i \cap R$ for all i.*

Theorem 1.7 (The Going-down Theorem)**.** *Assume that S is an integral domain and R is integrally closed in S. Let $\mathfrak{p}_1 \supseteq \mathfrak{p}_2 \supseteq \cdots \supseteq \mathfrak{p}_n$ be a chain of prime ideals in R and suppose there are prime ideals $\mathfrak{q}_1 \supseteq \mathfrak{q}_2 \supseteq \cdots \supseteq \mathfrak{q}_m$ of S with $\mathfrak{p}_i = \mathfrak{q}_i \cap R, 1 \leq i \leq m$ and $m < n$. Then the descending chain of ideals can be completed: there are prime ideals $\mathfrak{q}_{m+1} \supseteq \cdots \supseteq \mathfrak{q}_n$ in S such that $\mathfrak{p}_i = \mathfrak{q}_i \cap R$ for all i.*

Theorem 1.8. *Let S be an integral extension ring of R and let $\mathfrak{q}$ be a prime ideal in S which lies over a prime ideal $\mathfrak{p}$ in R. Then $\mathfrak{q}$ is maximal in S if and only if $\mathfrak{p}$ is maximal in R.*

Proof. Suppose $\mathfrak{q}$ is maximal in S, there is a maximal ideal $\mathfrak{m}$ of R that contains $\mathfrak{p}$ and $\mathfrak{m}$ is prime by **??**. By **??** there is a prime ideal $\mathfrak{q}'$ in S such that $\mathfrak{q} \subset \mathfrak{q}'$ and $\mathfrak{q}'$ lies over $\mathfrak{m}$. Since $\mathfrak{q}'$ is prime, $\mathfrak{q}' \neq S$. The maximality of $\mathfrak{q}$ implies that $\mathfrak{q} = \mathfrak{q}'$, whence $\mathfrak{p} = \mathfrak{q} \cap R = \mathfrak{q}' \cap R = \mathfrak{m}$. Therefore, $\mathfrak{p}$ is maximal in R.

Conversely suppose $\mathfrak{p}$ is maximal in R. Since $\mathfrak{q}$ is prime in $S, \mathfrak{q} \neq S$ and there is a maximal ideal N of S containing $\mathfrak{q}$ and N is prime, whence $1_R = 1_S \notin N$. Since $\mathfrak{p} = R \cap \mathfrak{q} \subset R \cap N \subset R$, we must have $\mathfrak{p} = R \cap N$ by maximality. Thus $\mathfrak{q}$ and N both lie over $\mathfrak{p}$ and $\mathfrak{q} \subset N$. Therefore, $\mathfrak{q} = N$ by 1.8 . □

§2 Discrete Valuation and Discrete Valuation Ring

Definition 2.1. *Let K be a field. A **discrete valuation** on K is a nonzero group homomorphism $v : K^\times \to \mathbb{Z}$ such that $v(a+b) \geq \min(v(a), v(b))$.*

*As v is not the zero homomorphism, its image is a nonzero subgroup of $\mathbb{Z}$, and is therefore of the form $m\mathbb{Z}$ for some $m \in \mathbb{Z}$. If $m = 1$, then $v : K^\times \to \mathbb{Z}$ is surjective, and v is said to be **normalized**; otherwise, $x \mapsto m^{-1} \cdot v(x)$ will be a normalized discrete valuation.*

We extend v to a map $K \to \mathbb{Z} \cup \{\infty\}$ by setting $v(0) = +\infty$, where ∞ is a symbol $\geq n$ for all $n \in \mathbb{Z}$.

Remark. *We have*

1. *$v(\zeta) = 0$ for some $\zeta \in K^\times$*
2. *$v(-a) = v(a)$ for all $a \in K$;*
3. *$v(a+b) = \max\{v(a), v(b)\}$ if $v(a) \neq v(b)$.*

We often use "ord" rather than " v " to denote a discrete valuation.

Definition 2.2. *The following conditions on a principal ideal domain are equivalent:*

1. *A has exactly one nonzero prime ideal;*
2. *up to associates, A has exactly one prime element;*
3. *A is local and is not a field.*

*A ring satisfying these conditions is called a **discrete valuation ring**.*

Theorem 2.3. *Let A be a domain ring. The following conditions are equivalent:*

1. *A is a discrete valuation ring*
2. *There is a discrete valuation v on $K = \mathrm{Frac}(A)$ such that*

$$A = \mathcal{O}_v := \{a \in K \mid v(a) \geq 0\}$$

   with unique maximal ideal $\mathfrak{m} = \{a \in K \mid v(a) > 0\}$.

3. *there exists a element $\pi \in A$ such that every nonzero ideal of A is of the form (π^n) for some $n \geq 0$.*

4. *A is a noetherian, integrally closed and has exactly one nonzero prime ideal.*

We can associate discrete valuations to prime ideals in Dedekind domains.

Definition 2.4. *Let A be a Dedekind domain and let $\mathfrak{p}$ be a prime ideal in A. For any $c \in K^\times$, let $v(c)$ be the exponent of $\mathfrak{p}$ in the factorization of (c). Then v is a normalized discrete valuation on K, called the* ***discrete valuation associated to*** $\mathfrak{p}$*, denoted by* $\mathrm{ord}_{\mathfrak{p}}$.

Proposition 2.5. *Let $x_1, \ldots, x_m$ be elements of a Dedekind domain A, and let $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$ be distinct prime ideals of A. For every integer n, there is an $x \in A$ such that*

$$\mathrm{ord}_{\mathfrak{p}_i}(x - x_i) > n, \quad i = 1, 2, \ldots, m.$$

§3 Dedekind Domain

Definition 3.1. *A* ***Dedekind domain*** *is an integral domain A satisfying*

(i) *A is noetherian;*

(ii) *A is integrally closed;*

(iii) *A has Krull dimension one, i.e., every nonzero prime ideal is maximal.*

Proposition 3.2. *Let A be an integral domain, and let S be a multiplicative subset of A.*

1. *If A is noetherian, then so also is $S^{-1}A$.*

2. *If A is integrally closed, then so also is $S^{-1}A$.*

3. *If A has Krull dimension one, then so also does $A_{\mathfrak{p}}$ for any prime ideal $\mathfrak{p}$.*

Remark. *It follows that the localization $A_{\mathfrak{p}}$ of a Dedekind domain A is local thus DVR.*

§3.1 Fractional Ideals

Definition 3.3. *Let A be an integral domain with quotient field $K = \mathrm{Frac}(A)$.*

1. *A* ***fractional ideal*** *of A is*

   (i) *a nonzero A-submodule I of K*

   (ii) *there exists a nonzero $d \in A$ such that $dI \subset A$ i,e, $(A : I) \cap A \neq \varnothing$*

2. *A fractional ideal I of A is said to be* ***integral*** *if $I \subset A$.*

3. *A fractional ideal I of A is said to be* ***principal*** *if $I = Ax$ for some nonzero $x \in K$.*

4. *the* ***ideal quotient*** *of two fractional ideals I and J is defined as*

$$(I : J) := \{x \in K \mid xJ \subset I\}.$$

5. *the* ***inverse*** *of a fractional ideal I is defined as*

$$I^{-1} := (A : I).$$

   thus $II^{-1} \subset A$.

6. *A fractional ideal I is called* ***invertible*** *if there is a fractional ideal J such that $IJ = A$.*

Remark. *Let I be a fractional ideal of A, $\mathfrak{p}$ a prime ideal of A and $S = A - \mathfrak{p}$. Then the localization $I_{\mathfrak{p}} := IA_{\mathfrak{p}} = S^{-1}I = \{x/s : x \in I, s \in S\}$ is a fractional ideal of $A_{\mathfrak{p}}$.*

We may assume that all rings and ideals are contained in $K = \mathrm{Frac}(A)$.

Lemma 3.4. *Let A be a integral domain and fractional ideal I, J, then*

- $I + J$
- IJ
- $I \cap J$
- $(I : J)$

are both ideal fractional ideal. And

1. $IJ \subset I \cap J$
2. $H + (I + J) = I + (H + J) := H + I + J$
3. $IJ = JI$
4. $H(IJ) = (HI)J := HIJ$
5. $H(I + J) = HI + HJ$

Proposition 3.5. *Let A be an integral domain, $K = \mathrm{Frac}(A)$ and I a fractional ideal. Then the following statements hold:*

1. *$II^{-1} \subseteq A$.*
2. *I is invertible $\Leftrightarrow II^{-1} = A$.*
3. *Let J be an invertible ideal. Then $(I : J) = IJ^{-1}$.*
4. *If $0 \neq i \in I$ such that $i^{-1} \in I^{-1}$, then $I = (i)$.*

Corollary 3.6. *Let A be an integral domain. The set $\mathcal{I}(A)$ of invertible fractional ideals forms an abelian group with respect to multiplication, with A being the identity element, and the inverse of $I \in \mathcal{I}(A)$ being I^{-1}.*

Definition 3.7. *Let A be an integral domain. One calls $\mathcal{I}(A)$ the group of invertible fractional ideal and $\mathcal{P}(R)$ the subgroup of principal invertible fractional ideal. The quotient group* $\operatorname{Pic}(R) := \mathcal{I}(R)/\mathcal{P}(R)$ *is called the* ***Picard group*** *of A.*

If K is a number field and $\mathbb{Z}_K$ its ring of integers, one also writes $\mathrm{CL}(K) := \operatorname{Pic}(\mathbb{Z}_K)$*, and calls it the* ***ideal class group*** *of K.*

Remark. *Then we have the exact sequence of abelian groups*

$$1 \to A^\times \to K^\times \xrightarrow{\text{prin}} \mathcal{I}(A) \xrightarrow{\text{proj}} \operatorname{Pic}(A) \to 1,$$

where $f(x)$ is the principal fractional R-ideal xR.

Invertibility is a local property:

Proposition 3.8. *For a fractional ideal I in integral domain A, the following are equivalent:*

1. *I is invertible;*
2. *I is finitely generated and, for each prime ideal $\mathfrak{p}$, $I_\mathfrak{p}$ is invertible:*
3. *I is finitely generated and, for each maximal ideal $\mathfrak{m}$, $I_\mathfrak{m}$ is invertible.*

§3.2 Unique factorization of fractional ideals

Theorem 3.9. *Let A be a Dedekind domain. Every fractional ideal I of A can be written uniquely in the form*

$$I = \prod_{\mathfrak{p} \text{ prime}} \mathfrak{p}^{v_\mathfrak{p}(I)}$$

where discrete valuation $v_\mathfrak{p}(I)$.

The set $\mathcal{I}(A)$ of fractional ideals is a group; in fact, it is the free abelian group on the set of nonzero prime ideals.

Proof. In order to show that $\mathcal{I}(A)$ is a group, it remains to show that inverses exist. Let $\mathfrak{a}$ be a nonzero integral ideal, there is an ideal $\mathfrak{a}^*$ and an $a \in A$ such that $\mathfrak{a}\mathfrak{a}^* = (a)$. Clearly $\mathfrak{a} \cdot (a^{-1}\mathfrak{a}^*) = A$, and so $a^{-1}\mathfrak{a}^*$ is an inverse of $\mathfrak{a}$. If $\mathfrak{a}$ is a fractional ideal, then $d\mathfrak{a}$ is an integral ideal for some d, and $d \cdot (d\mathfrak{a})^{-1}$ will be an inverse for $\mathfrak{a}$.

It remains to show that the group $\operatorname{Id}(A)$ is freely generated by the prime ideals, i.e., that each fractional ideal can be expressed in a unique way as a product of powers of prime ideals. Let $\mathfrak{a}$ be a fractional ideal. Then $d\mathfrak{a}$ is an integral ideal for some $d \in A$, and we can write

$$d\mathfrak{a} = \mathfrak{p}_1^{r_1} \cdots \mathfrak{p}_m^{r_m}, \quad (d) = \mathfrak{p}_1^{s_1} \cdots \mathfrak{p}_m^{s_m}.$$

Thus $\mathfrak{a} = \mathfrak{p}_1^{r_1-s_1} \cdots \mathfrak{p}_m^{r_m-s_m}$. The uniqueness follows from the uniqueness of the factorization for integral ideals. $\square$

§3.3 Proof of factorization

We prove the theorem in several steps. Assume that A is a commutative ring throughout.

Lemma 3.10. *Let A be a noetherian ring; then every ideal $\mathfrak{a}$ in A contains a product of nonzero prime ideals.*

Proof. Suppose that the statement is false for A, and choose a maximal counterexample $\mathfrak{a}$ by Noetherian property. Then $\mathfrak{a}$ itself cannot be prime, and so there exist elements x and y of A such that $xy \in \mathfrak{a}$ but neither x nor $y \in \mathfrak{a}$.

The ideals $\mathfrak{a}+(x)$ and $\mathfrak{a}+(y)$ strictly contain $\mathfrak{a}$ and contain a product of prime ideals respectively, but their product is contained in $\mathfrak{a}$. It follows that $\mathfrak{a}$ contains a product of prime ideals. $\square$

Lemma 3.11. *Let A be a ring, and let $\mathfrak{a}$ and $\mathfrak{b}$ be relatively prime ideals in A;*

1. *for all $m, n \in \mathbb{N}$, $\mathfrak{a}^m$ and $\mathfrak{b}^n$ are relatively prime.*
2. *$I \cap J = IJ$*
3. *$A/(IJ) \cong A/(I) \times A/(J)$*
4. *if $IJ = H^n$ for some ideal H and some $n \in \mathbb{N}$, then there exist ideals $I_1 := I + H$ and $J_1 := J + H$ such that $I = I_1^n$, $J = J_1^n$ and $I_1 J_1 = H$*

Proof. If $\mathfrak{a}^m$ and $\mathfrak{b}^n$ are not relatively prime, then they are both contained in some prime (even maximal) ideal $\mathfrak{p}$. Thus $\mathfrak{a}$ and $\mathfrak{b}$ are both contained in $\mathfrak{p}$, which contradicts the hypothesis. $\square$

Lemma 3.12. *Let $\mathfrak{p}$ be a maximal ideal of an integral domain A, and let $\mathfrak{q} = \mathfrak{p}^e = \mathfrak{p}A_{\mathfrak{p}}$ be the ideal in $A_{\mathfrak{p}}$. The map*

$$a + \mathfrak{p}^m \mapsto a + \mathfrak{q}^m : A/\mathfrak{p}^m \to A_{\mathfrak{p}}/\mathfrak{q}^m$$

is an isomorphism for all $m \in \mathbb{N}$.

Proof. Let S be the $A - \mathfrak{p}$. The map is clearly a homomorphism of rings, so we have to prove that it is bijective.

We first show that the map is injective. For this we have to show that $\mathfrak{q}^m \cap A = \mathfrak{p}^m$. But $\mathfrak{q}^m = S^{-1}\mathfrak{p}^m$, and so we have to show that $\mathfrak{p}^m = (S^{-1}\mathfrak{p}^m) \cap A$. An element of $(S^{-1}\mathfrak{p}^m) \cap A$ can be written $a = b/s$ with $b \in \mathfrak{p}^m$, $s \in S$, and $a \in A$. Then $sa \in \mathfrak{p}^m$, and so $sa = 0$ in $A/\mathfrak{p}^m$. The only maximal ideal containing $\mathfrak{p}^m$ is $\mathfrak{p}$ (because $\mathfrak{m} \supset \mathfrak{p}^m \Rightarrow \mathfrak{m} \supset \mathfrak{p}$), and so the only maximal ideal in $A/\mathfrak{p}^m$ is $\mathfrak{p}/\mathfrak{p}^m$; in particular, $A/\mathfrak{p}^m$ is a local ring. As $s + \mathfrak{p}^m$ is not in $\mathfrak{p}/\mathfrak{p}^m$, it is a unit in $A/\mathfrak{p}^m$, and so $sa = 0$ in $A/\mathfrak{p}^m \Rightarrow a = 0$ in $A/\mathfrak{p}^m$, i.e., $a \in \mathfrak{p}^m$.

We now prove that the map is surjective. Let $\frac{a}{s} \in A_{\mathfrak{p}}$. Because $s \notin \mathfrak{p}$ and $\mathfrak{p}$ is maximal, we have that $(s) + \mathfrak{p} = A$, i.e., (s) and $\mathfrak{p}$ are relatively prime. Therefore (s) and $\mathfrak{p}^m$ are relatively prime by lemma 3.11 , and so there exist $b \in A$ and $q \in \mathfrak{p}^m$ such that $bs + q = 1$. Then b maps to s^{-1} in $A_{\mathfrak{p}}/\mathfrak{q}^m$ and so ba maps to $\frac{a}{s}$. Thus the map is surjective. □

Proof of factorization. We now prove that a nonzero ideal $\mathfrak{a}$ of Dedekind domain A can be factored into a product of prime ideals. According to 3.10 applied to A, the ideal $\mathfrak{a}$ contains a product of nonzero prime ideals,

$$\mathfrak{b} = \mathfrak{p}_1^{r_1} \cdots \mathfrak{p}_m^{r_m}$$

We may suppose that the $\mathfrak{p}_i$ are distinct. Then

$$A/\mathfrak{b} \simeq A/\mathfrak{p}_1^{r_1} \times \cdots \times A/\mathfrak{p}_m^{r_m} \simeq A_{\mathfrak{p}_1}/\mathfrak{q}_1^{r_1} \times \cdots \times A_{\mathfrak{p}_m}/\mathfrak{q}_m^{r_m},$$

where $\mathfrak{q}_i = \mathfrak{p}_i A_{\mathfrak{p}_i}$ is the maximal ideal of $A_{\mathfrak{p}_i}$. Under this isomorphism,

$$A \to A/\mathfrak{b} \simeq A_{\mathfrak{p}_1}/\mathfrak{q}_1^{r_1} \times \cdots \times A_{\mathfrak{p}_m}/\mathfrak{q}_m^{r_m}$$

$\mathfrak{a}/\mathfrak{b}$ in $A/\mathfrak{b}$ corresponds to $\mathfrak{q}_1^{s_1}/\mathfrak{q}_1^{r_1} \times \cdots \times \mathfrak{q}_m^{s_m}/\mathfrak{q}_m^{r_m}$ for some $s_i \leq r_i$ (recall that the rings $A_{\mathfrak{p}_i}$ are all discrete valuation rings). Since this ideal is also the image of $\mathfrak{p}_1^{s_1} \cdots \mathfrak{p}_m^{s_m}$ under the isomorphism, we see that

$$\mathfrak{a} = \mathfrak{p}_1^{s_1} \cdots \mathfrak{p}_m^{s_m} \text{ in } A/\mathfrak{b}.$$

Both of these ideals contain $\mathfrak{b}$, and so this implies that

$$\mathfrak{a} = \mathfrak{p}_1^{s_1} \cdots \mathfrak{p}_m^{s_m}$$

in A.

To complete the proof, we have to prove that the above factorization is unique. Suppose that we have two factorizations of the ideal $\mathfrak{a}$. After adding factors with zero exponent, we may suppose that the same primes occur in each factorization, so that

$$\mathfrak{p}_1^{s_1} \cdots \mathfrak{p}_m^{s_m} = \mathfrak{a} = \mathfrak{p}_1^{t_1} \cdots \mathfrak{p}_m^{t_m}$$

In the course of the above proof, we showed that

$$\mathfrak{q}_i^{s_i} = \mathfrak{a} A_{\mathfrak{p}_i} = \mathfrak{q}_i^{t_i},$$

where $\mathfrak{q}_i = \mathfrak{p}_i A_{\mathfrak{p}_i}$ the maximal ideal in $A_{\mathfrak{p}_i}$. Therefore $s_i = t_i$ for all i. □

Corollary 3.13. *Let $\mathfrak{a} \supset \mathfrak{b} \neq 0$ be two ideals in a Dedekind domain; then $\mathfrak{a} = \mathfrak{b} + (a)$ for some $a \in A$.*

Proof. Let $\mathfrak{b} = \mathfrak{p}_1^{r_1} \cdots \mathfrak{p}_m^{r_m}$ and $\mathfrak{a} = \mathfrak{p}_1^{s_1} \cdots \mathfrak{p}_m^{s_m}$ with $r_i, s_j \geq 0$. Because $\mathfrak{b} \subset \mathfrak{a}$, $s_i \leq r_i$ for all

i. For $1 \leq i \leq m$, choose an $x_i \in A$ such that $x_i \in \mathfrak{p}_i^{s_i}, x_i \notin \mathfrak{p}_i^{s_i+1}$. By the Chinese Remainder Theorem, there is an $a \in A$ such that

$$a \equiv x_i \mod \mathfrak{p}_i^{r_i}, \text{ for all } i.$$

Now one sees that $\mathfrak{b} + (a) = \mathfrak{a}$ by looking at the ideals they generate in $A_\mathfrak{p}$ for all $\mathfrak{p}$. □

Corollary 3.14. *Let $\mathfrak{a}$ be an ideal in a Dedekind domain, and let a be any nonzero element of $\mathfrak{a}$; then there exists $b \in \mathfrak{a}$ such that $\mathfrak{a} = (a, b)$.*

Corollary 3.15. *Let $\mathfrak{a}$ be a nonzero ideal in a Dedekind domain; then there exists a nonzero ideal $\mathfrak{a}^*$ in A such that $\mathfrak{a}\mathfrak{a}^*$ is principal. Moreover, $\mathfrak{a}^*$ can be chosen to be relatively prime to any particular ideal $\mathfrak{c}$, and it can be chosen so that $\mathfrak{a}\mathfrak{a}^* = (a)$ with a any particular element of $\mathfrak{a}$ (but not both).*

Proof. Let $a \in \mathfrak{a}, a \neq 0$; then $\mathfrak{a} \supset (a)$, and so we have

$$(a) = \mathfrak{p}_1^{r_1} \cdots \mathfrak{p}_m^{r_m} \text{ and } \mathfrak{a} = \mathfrak{p}_1^{s_1} \cdots \mathfrak{p}_m^{s_m}, \quad s_i \leq r_i.$$

If $\mathfrak{a}^* = \mathfrak{p}_1^{r_1-s_1} \cdots \mathfrak{p}_m^{r_m-s_m}$, then $\mathfrak{a}\mathfrak{a}^* = (a)$.

We now show that $\mathfrak{a}^*$ can be chosen to be prime to $\mathfrak{c}$. We have $\mathfrak{a} \supset \mathfrak{a}\mathfrak{c}$, and so (by 3.15) there exists an $a \in \mathfrak{a}$ such that $\mathfrak{a} = \mathfrak{a}\mathfrak{c} + (a)$. As $\mathfrak{a} \supset (a)$, we have $(a) = \mathfrak{a} \cdot \mathfrak{a}^*$ for some ideal $\mathfrak{a}^*$ (by the above argument); now, $\mathfrak{a}\mathfrak{c} + \mathfrak{a}\mathfrak{a}^* = \mathfrak{a}$, and so $\mathfrak{c} + \mathfrak{a}^* = A$. (Otherwise $\mathfrak{c} + \mathfrak{a}^* \subset \mathfrak{p}$ some prime ideal, and $\mathfrak{a}\mathfrak{c} + \mathfrak{a}\mathfrak{a}^* = \mathfrak{a}(\mathfrak{c} + \mathfrak{a}^*) \subset \mathfrak{a}\mathfrak{p} \neq \mathfrak{a}$.) □

Chapter II

§1 Number Fields and Rings of Integers

Definition 1.1. *A **number field** K is a finite extension of the field of rational numbers $\mathbb{Q}$.*

Remark. *As* $\operatorname{char}\mathbb{Q} = 0$*, $K/\mathbb{Q}$ is separable, then $K = \mathbb{Q}(\alpha)$ for some primitive element α.*

Definition 1.2. *Let K be a number field. The **ring of integers** of K is the integral closure of $\mathbb{Z}$ in K, denoted by $\mathcal{O}_K$ or $\mathbb{Z}_K$; its elements are called the **algebraic integers** in K.*

§2

Definition 2.1. *Let $A = \mathbb{Z}$ and M be a free A-module of rank n, the **index** of $N := \mathbb{Z}f_1 + \mathbb{Z}f_2 + \cdots + \mathbb{Z}f_n$ in M is*

$$(M : N) := |\det(a_{ij})|$$

where $(f_k) = (a_{ij})(e_k)$ for some A-basis $\{e_k\}$.

§3 Trace and Norm

Definition 3.1. *Let B/A be a ring extension such that B is a free A-module of rank n. Then every $\beta \in B$ defines an A-linear map*

$$T_\beta : B \to B, \quad x \mapsto \beta x$$

*and the trace and determinant of this map are well-defined. We call them the **trace** $\operatorname{Tr}_{B/A}\beta$ and **norm** $\mathrm{N}_{B/A}\beta$ of β in the extension B/A.*

Proposition 3.2. *Let L/K be an separable extension of fields of degree n, $\overline{K}$ an algebraic closure of K containing L. Let*

$$\{\sigma_1, \ldots, \sigma_n\} = \operatorname{Hom}_K\left(L, \overline{K}\right)$$

Then the following statements hold for any $a \in L$:

1. $\chi_a = m_a^e$ *where* $e = [L : K(a)] = n/\deg m_a$.

2. $\chi_a(X) = \prod_{\sigma \in \mathrm{Hom}_K(L,\overline{K})}(X - \sigma(a))$,

3. $\mathrm{Tr}_{L/K}(a) = \sum_\sigma \sigma(a)$, *and* $\mathrm{N}_{L/K}(a) = \prod_\sigma \sigma(a)$.

Proof. Let $F = K(a)$, then $\overline{K}/F$ is Galois thus separable

$$m_a(X) := \prod_{\overline{\sigma}_\alpha \in K'/F'} (X - \overline{\sigma}_\alpha(a)) .$$

Then by the preceding proposition and $e = [L : F] = [F' : L']$

$$\prod_{\overline{\sigma}_\alpha \in K'/F'} (X - \overline{\sigma}_\alpha(a))^e = \prod_{\overline{\sigma}_\alpha \in K'/F'} \prod_{\overline{\sigma}_\beta \in F'/L'} (X - \overline{\sigma}_\alpha \circ \overline{\sigma}_\beta(a)) = \prod_{\sigma \in \mathrm{Hom}_K(L,\overline{K})} (X - \sigma(a)).$$

□

Corollary 3.3. *Let $L/F/K$ be finite separable field extensions. Then*

$$\mathrm{Tr}_{L/K} = \mathrm{Tr}_{F/K} \circ \mathrm{Tr}_{L/F} \text{ and } \mathrm{Norm}_{L/K} = \mathrm{Norm}_{F/K} \circ \mathrm{Norm}_{L/F}$$

§4 Discriminant

§4.1

Let A be an integral domain with fraction field $K = \mathrm{Frac}(A)$ and L/K be finite separable field extension. Let $B := A_L$ be the integral closure of A in L.

Proposition 4.1. *Then the following statements hold:*

1. *Every $a \in L$ can be written as $a = \frac{s}{r}$ with $s \in B$ and $0 \neq r \in A$.*

2. *$L = \mathrm{Frac}(B)$ and B is integrally closed.*

If A is integrally closed

3. *For any K-basis $\alpha_1, \ldots, \alpha_n$ of L, there is an element $r \in A \backslash \{0\}$ such that $r\alpha_i \in B$ for all $i = 1, \ldots, n$. Clearly, $\{r\alpha_i\}_{i=1}^n \subset B$ is also a K-basis of L.*

4. *$B \cap K = A$.*

Lemma 4.2. *Let $\alpha_1, \ldots, \alpha_n$ be a basis of L/K which is contained in B, of discriminant $d = d(\alpha_1, \ldots, \alpha_n)$. Then one has*

$$dB \subseteq A\alpha_1 + \cdots + A\alpha_n$$

Proposition 4.3. *,*

1. *There exists free A-submodules M and M' of L such that*

$$M \subset B \subset M'.$$

2. *Therefore B is a finitely generated A-module if A is noetherian,*

3. *If A is a principal ideal domain, then every finitely generated B-submodule $M \neq 0$ of L is a free A-module of rank n. In particular, B admits an integral basis over A.*

Remark. *When A is a principal ideal domain, a basis for B as an A-module is called an* ***integral basis*** *of B over A (is also a K-basis of L).*

Proof. Let $\{\alpha_1, \ldots, \alpha_n\} \subset B$ be a basis for L over K. Because the trace pairing is nondegenerate, there is a dual basis $\{\alpha_1', \ldots, \alpha_n'\}$ of L over K such that $\operatorname{Tr}\left(\alpha_i \cdot \alpha_j'\right) = \delta_{ij}$. We shall show that

$$A\alpha_1 + A\alpha_2 + \cdots + A\alpha_n \subset B \subset A\alpha_1' + A\alpha_2' + \cdots + A\alpha_n'.$$

The first inclusion is clear because the α_i are in B.

To show the second inclusion, let $b \in B$ and b can be written uniquely as a linear combination $b = \sum k_j \alpha_j'$ of the α_j' with coefficients $k_j \in K$. As α_i and b are in B, so also is $b \cdot \alpha_i$, and so $\operatorname{Tr}(b \cdot \alpha_i) \in A$. But

$$\operatorname{Tr}(b \cdot \alpha_i) = \operatorname{Tr}\left(\sum_j k_j \alpha_j' \cdot \alpha_i\right) = \sum_j k_j \operatorname{Tr}\left(\alpha_j' \cdot \alpha_i\right) = \sum_j k_j \cdot \delta_{ij} = k_i.$$

Hence $k_i \in A \cap K = A$, proving the second inclusion. □

§4.2 Discriminant

Definition 4.4. *Let B/A be a ring extension, and assume that B is free of rank n as an A-module.*

1. *Let $\alpha_1, \ldots, \alpha_n$ be A-basis of B. We define their* ***discriminant*** *to be*

$$\operatorname{disc}_{B/A}(\alpha_1, \ldots, \alpha_n) := \det\left(\operatorname{Tr}_{B/A}(\alpha_i \alpha_j)\right)_{1 \leq i,j \leq n}.$$

2. *The* ***trace pairing*** *on B/A is the bilinear pairing*

$$B \times B \to A, \quad (x, y) \mapsto \operatorname{Tr}_{B/A}(xy)$$

with Gram matrix $\left(\operatorname{Tr}_{B/A}(\alpha_i \alpha_j)\right)_{1 \leq i,j \leq n}$ with respect to the basis $\{\alpha_1, \ldots, \alpha_n\}$ of B.

3. *If two basis $(\beta_1, \ldots, \beta_n) = (\alpha_1, \ldots, \alpha_n)(a_{ij})_{1 \leq i,j \leq n}$ where $(a_{ij}) \in M_n(A)$, then*

$$\operatorname{disc}(\beta_1, \ldots, \beta_n) = \det(a_{ij})^2 \operatorname{disc}(\alpha_1, \ldots, \alpha_n).$$

Thus the discriminant of a basis of B is well-defined up to multiplication by the square of a unit in A. The ideal generated by the discriminant, or $\operatorname{disc}(\alpha_1, \ldots, \alpha_n)$ *itself regarded as an element of $A/A^{\times 2}$, is called the* ***discriminant*** *of B over A, denoted* $\operatorname{disc}(B/A)$.

Remark. *Then elements $\gamma_1, \ldots, \gamma_n$ form a basis for B as an A-module if and only if*

$$(\operatorname{disc}(\gamma_1, \ldots, \gamma_n)) = (\operatorname{disc}(B/A)) \quad (\text{ as ideals in } A).$$

Definition 4.5. *By proposition, every finitely generated $\mathcal{O}_K$-submodule $\mathfrak{a}$ of K admits a $\mathbb{Z}$-basis $\alpha_1, \ldots, \alpha_n$. The **discriminant** of ideal $\mathfrak{a}$ is defined as*

$$d(\mathfrak{a}) := \operatorname{disc}_{\mathfrak{a}/\mathbb{Z}}(\alpha_1, \ldots, \alpha_n)$$

is independent of the choice of a $\mathbb{Z}$-basis. ($\mathbb{Z}^{\times 2} = \{1\}$)

In the special case of an integral basis $\omega_1, \ldots, \omega_n$ of $\mathcal{O}_K$ we obtain the discriminant of the algebraic number field K,

$$d_K := d(\mathcal{O}_K) = d(\omega_1, \ldots, \omega_n)$$

Remark. *Note that $d_K = \operatorname{disc}_{\mathcal{O}_K/\mathbb{Z}}(\omega_1, \ldots, \omega_n) = \operatorname{disc}_{K/\mathbb{Q}}(\omega_1, \ldots, \omega_n)$.*

Proposition 4.6. *If $\mathfrak{a} \subseteq \mathfrak{a}'$ are two nonzero finitely generated $\mathcal{O}_K$-submodules of K, then the index $(\mathfrak{a}' : \mathfrak{a})$ is finite and satisfies*

$$d(\mathfrak{a}) = (\mathfrak{a}' : \mathfrak{a})^2 \, d(\mathfrak{a}').$$

Proposition 4.7. *Let L/K be a finite separable field extension of degree n, $\{\alpha_i\}$ a K-basis of L and $\operatorname{Hom}_K(L, \overline{K}) = \{\sigma_1, \ldots, \sigma_n\}$. Then let matrix $D = D(\alpha_1, \ldots, \alpha_n) := (\sigma_i(\alpha_j))_{1 \le i,j \le n}$, the following statements hold:*

1. *Then $D^{\mathrm{tr}} D$ is the Gram matrix of the $\operatorname{Tr}_{L/K}(- \cdot -)$ with respect to $\{\alpha_i\}$. That is,*

$$D^{\mathrm{tr}} D = \left(\operatorname{Tr}_{L/K}(\alpha_i \alpha_j)\right)_{1 \le i,j \le n}$$

   Consequently, $\det\left(\operatorname{Tr}_{L/K}(\alpha_i \alpha_j)\right)_{1 \le i,j \le n} = (\det D(\alpha_1, \ldots, \alpha_n))^2$.

2. *Let $L = K(a)$ for some primitive element a, then*

$$\operatorname{disc}\left(1, a, \ldots, a^{n-1}\right) = \det\left(\sigma_i(a)^{k-1}\right)_{1 \le i,k \le n} = \prod_{1 \le i < j \le n} (\sigma_j(a) - \sigma_i(a))^2 \neq 0.$$

3. *Therefore* $\operatorname{disc}(L/K)$ *is non-zero and the trace pairing on L/K is non-degenerate.*

Corollary 4.8. $d_{\mathcal{O}_K} \neq 0$

§5 Ramification

In this section, let A be a Dedekind domain with field of fractions K, and let B be the integral closure of A in a finite separable extension L of K.

Theorem 5.1. *B is also a Dedekind domain.*

Definition 5.2. *A prime ideal $\mathfrak{p}$ of A will factor in B,*

$$\mathfrak{p}B = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}$$

wher $\mathfrak{P}$ are distinct prime ideals in B and $e_i \geq 1$,

1. *We say $\mathfrak{P}$ divides $\mathfrak{p}$,written $\mathfrak{P} \mid \mathfrak{p}$, if $\mathfrak{P}$ occurs in the factorization of $\mathfrak{p}$ in B. The number e_i is called the **ramification index** of $\mathfrak{P}_i$ over $\mathfrak{p}$.*

2. *If any of the numbers is > 1, then we say that $\mathfrak{p}$ is **ramified**.*

*We then write $e(\mathfrak{P}/\mathfrak{p})$ for the ramification index and $f(\mathfrak{P}/\mathfrak{p})$ for the degree of the field extension $[B/\mathfrak{P} : A/\mathfrak{p}]$ (called the **residue class degree**).*

3. *$\mathfrak{p}$ is said to **split** (or split completely) in L if $e_i = f_i = 1$ for all i*

4. *$\mathfrak{p}$ is said to be **inert** in L if $\mathfrak{p}$ is a prime ideal in B (so $g = 1 = e$).*

Theorem 5.3. *Let m be the degree of L over K, and let $\mathfrak{P}_1, \ldots, \mathfrak{P}_g$ be the prime ideals dividing $\mathfrak{p}$; then*

$$\sum_{i=1}^{g} e_i f_i = m$$

where $e_i = e(\mathfrak{P}_i/\mathfrak{p})$ and $f_i = f(\mathfrak{P}_i/\mathfrak{p})$. If L is Galois over K, then all the ramification numbers are equal, and all the residue class degrees are equal, and so

$$efg = m.$$

Again A is a Dedekind domain with field of fractions K, and B is the integral closure of A in a finite separable extension L of K.

Theorem 5.4. *Assume that B is a free A-module. Then a prime $\mathfrak{p}$ ramifies in L if and only if $\mathfrak{p} \mid \mathrm{disc}(B/A)$. In particular, only finitely many prime ideals ramify.*

Theorem 5.5 (Dedekind-Kummer)**.** *Suppose that $B = A[\alpha]$, and let $f(X)$ be the minimal polynomial of α over K. Let $\mathfrak{p}$ be a prime ideal in A and reducible $f(X) = \prod g_i(X)^{e_i}$ in $(A/\mathfrak{p})[X]$. Then*

$$\mathfrak{p}B = \prod (\mathfrak{p}, g_i(\alpha))^{e_i}$$

is the factorization of $\mathfrak{p}B$ into a product of powers of distinct prime ideals.

Moreover, the residue field $B/(\mathfrak{p}, g_i(\alpha)) \simeq (A/\mathfrak{p})[X]/(\bar{g}_i)$, and so the residue class degree f_i is equal to the degree of g_i.

Chapter III

Dirichlet Unit Theorem

Theorem 0.1 (Dirichlet). *Let K be a number field of degree $n = r_1 + 2r_2$. Then there is a group isomorphism*

$$\mathcal{O}_K^\times \simeq \mu_K \times \mathbb{Z}^{r_1+r_2-1},$$

where μ_K is the torsion subgroup of $\mathcal{O}_K^\times$ (the finite cyclic subgroup consisting of roots of unity)