HOMEWORK 2 : DEDEKIND DOMAINS; FACTORIZATION

HYOJIN KIM

In this note and the later note, we define the notion of a Dedekind domain and prove that ideals in Dedekind domains factor uniguely into products of prime ideals, and rings of integers in number fields are Dedekind domains.

1. Definitions

We will introduce some basic definitions to know the notions of Dedekind domain and the ideal class group. Being a generation of the ring $\mathbb{Z} \subset \mathbb{Q}$, the ring of integers $\mathcal{O}_L$ in an algebraic number field L, is at the center of all our considerations.

Definition 1.1. *A* ***discrete valuation ring*** *is a principal ideal domain with exactly one non-zero prime ideal.*

Definition 1.2. *A Noetherian, integrally closed integral domain, not equal to a field, in which every nonzero prime ideal is maximal is called a* ***Dedekind domain****.*

The Dedekind domains may be viewed as generalized principal ideal domains. Let A be a principal ideal domain with field of fractions K, and L/K is a finite field extension, then the integral closure B of A in L is not a principal ideal domain in general, but always a Dedekind domain.

Definition 1.3. *For a Dedekind domain A, a* ***fractional ideal*** *of A is a nonzero A-submodule $\mathfrak{a}$ of K such that*

$$d\mathfrak{a} := \{da \mid a \in \mathfrak{a}\}$$

is contained in A for some nonzero $d \in A$(or K), i.e., it is a nonzero A-submodule of K whose elements have a common denominator. Note that a fractional ideal is not an ideal unless it is contained in A, we refer to the ideals in A as ***integral*** *ideals. Every nonzero element b of K defines a fractional ideal $(b) := bA := \{ba | a \in A\}$. A fractional ideal of this type is said to be principal.*

Definition 1.4. *The quotient $Cl(A) = Id(A)/P(A)$ of $Id(A)$ by the subgroup of principal ideals is the* ***ideal class group*** *of A. The* ***class number*** *of A is the order of $Cl(A)$(when finite). In the case that A is the ring of integers $\mathcal{O}_K$ in K in a number field K, we often refer to $Cl(\mathcal{O}_K)$ as the* ***ideal class group*** *of K, and its order as the* ***class number*** *of K.*

The class number of $\mathbb{Q}[\sqrt{-m}]$ for m positive and square-free is 1 iff $m = 1, 2, 3, 7, 11, 19, 43, 67, 163$. $\mathbb{Z}[\sqrt{-5}]$ is not a principal ideal domain, and so can't have class number 1. In fact, it has class number 2. Gauss showed that the class group of a quadratic field $\mathbb{Q}[\sqrt{d}]$ can have arbitrarily many cyclic factors of even order.

We defined an integral basis and the discriminant already. Any basis of the free abelian group A (ring of algebraic integers) is called an integral basis of K. An integral basis is a basis of the vector space K over $\mathbb{Q}$, since it has $n[K : \mathbb{Q}]$ elements. The discriminant in $K|\mathbb{Q}$ of any integral basis is called the discriminant of the field K.

Let d_K be the discriminant of Quadratic field $K = \mathbb{Q}(\sqrt{d})$ where d is a squrae-free integer. Then $d_K = 4d$ if $d \equiv 2$ *or* $3 \pmod 4$, and $d_K = d$ if $d \equiv 1 \pmod 4$.

Recall that for an integral domain A with field of fraction K, we can define a multiplicative subset $S_\mathfrak{p} = A \setminus \mathfrak{p}$ of A, and we write $A_\mathfrak{p} = S_\mathfrak{p}^{-1}A$ where $\mathfrak{p}$ is a prime ideal. For example,

$$\mathbb{Z}_{(p)} = \{m/n \in \mathbb{Q} \mid p \nmid n\}$$

Date: april 5, 2019.

and $\mathbb{Z}_(p)$ is a discrete valuation ring with (p) as its unique nonzero prime ideal. Generally, if $\mathfrak{p}$ is a prime ideal in A, then $A_\mathfrak{p}$ is a local ring because $\mathfrak{p}$ contains every prime ideal disjoint from $S_\mathfrak{p}$. Note that the ring $A_\mathfrak{p}$ is a discrete valuation ring.

2. Unique factorization of ideals

We now prove that a proper nonzero ideal $\mathfrak{a}$ of a Dedekind domain A can be factored uniguely into a product of prime ideals. To prove the existence of the prime ideal factorization, we will use followings without proof.

Lemma 2.1. *Let A be a Noetherian ring; then every ideal of $\mathfrak{a}$ in A contains a product of nonzero prime ideals.*

Theorem 2.2. *Let $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ be ideals in a ring A, relatively prime in pairs. Then for any elements $x_1, \ldots, x_n$ of A, the congruences*

$$x \equiv x_i \pmod{\mathfrak{a}_i}$$

have a simultaneous solution $x \in A$; moreover, if x is one solution, then the other solutions are the elements of the form $x + a$ with $a \in \cap\mathfrak{a}_i$, and $\cap\mathfrak{a}_i = \prod \mathfrak{a}_i$. In other words, the natural maps give an exact sequence

$$0 \to \mathfrak{a} \to A \to \prod_{i=1}^{n} A/\mathfrak{a}_i \to 0$$

with $\mathfrak{a} = \cap\mathfrak{a}_i = \prod \mathfrak{a}_i$.

Lemma 2.3. *Let A be a ring and let $\mathfrak{a}$ and $\mathfrak{b}$ be relatively prime ideals in A; for any m, $n \in \mathbb{N}$, $\mathfrak{a}^m$ and $\mathfrak{b}^n$ are relatively prime.*

Lemma 2.4. *Let $\mathfrak{p}$ be a maximal ideal of a ring A, and let $\mathfrak{q}$ be the ideal it generates in $A_\mathfrak{p}$, $\mathfrak{q} = \mathfrak{p}A_\mathfrak{p}$. The map*

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

is an isomorphism.

According to above, the ideal $\mathfrak{a}$ of A contains a product of nonzero prime ideals,

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

where the $\mathfrak{p}_i$ are distinct, and there exist isomorphisms

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

where $\mathfrak{q}_i = \mathfrak{p}_i A_{\mathfrak{p}_i}$ is the maximal ideal of $A_{\mathfrak{p}_i}$. Recall that the rings $A_{\mathfrak{p}_i}$ are all discrete valuation rings. $\mathfrak{a}/\mathfrak{b}$ 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 $s_i \leq r_i$. Since this ideal is also the isomorphic image of $\mathfrak{p}_1{}^{s_1} \cdots \mathfrak{p}_m{}^{s_m}$, $\mathfrak{a} = \mathfrak{p}_1{}^{s_1} \cdots \mathfrak{p}_m{}^{s_m}$ in $A/\mathfrak{b}$. Hence $\mathfrak{a} = \mathfrak{p}_1{}^{s_1} \cdots \mathfrak{p}_m{}^{s_m}$ in A since both contain $\mathfrak{b}$ and there is a one-to-one correspondence between the ideals of $A/\mathfrak{b}$ and the ideals of A containing $\mathfrak{b}$.

Let $\mathfrak{a} = \mathfrak{p}_1{}^{s_1} \cdots \mathfrak{p}_m{}^{s_m} = \mathfrak{p}_1{}^{t_1} \cdots \mathfrak{p}_m{}^{t_m}$ be two factorizations after adding factors with zero exponent. We have $\mathfrak{a}A_{\mathfrak{p}_i} = \mathfrak{q}_i^{s_i} = \mathfrak{q}_i^{t_i}$ where $\mathfrak{q}_i$ the maximal ideal in $A_{\mathfrak{p}_i}$. Therefore $s_i = t_i$ for all i.

Now we get the following theorem.

Theorem 2.5. *Let A be a Dedekind domain. Every proper nonzero ideal $\mathfrak{a}$ of A can be written in the form*

$$\mathfrak{a} = \mathfrak{p}_1{}^{r_1} \cdots \mathfrak{p}_n{}^{r_n}$$

with the $\mathfrak{p}_i$ distinct prime ideals and the $r_i > 0$; the $\mathfrak{p}_i$ and the r_i are uniquely determined.

References

[1] James. S. Milne, *Algebraic Number Theory (v3.07)*, 2017. Available at www.jmilne.org/math/.

[2] P. Samuel, *Algebraic Theory of Numbers*, traslated from the French by Allan J.Silberger, HERMANN, Paris, 1970.