HOMEWORK 1 : DEDEKIND DOMAINS; FACTORIZATION

HYOJIN KIM

1. Definitions

In this section, 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 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 my be viewed as generalized principal ideal domains. Let A be a principal ideal domain with field of fractions K, and $L \mid K$ 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 1.2. *For a Dedekind domain A, a fractional ideal of A is a nonzero A-submodule $\mathfrak{a}$ of K such that*

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

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 1.3. *The quotient $Cl(A) = Id(A)/P(A)$ of $Id(A)$ by the subfroup 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 $d \equiv 1 \pmod 4$.

2. Properties

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.

Date: march 22, 2019.