HOMEWORK 1 : THE RING OF INTEGERS

HYOJIN KIM

1. Definitions

In this section, we will introduce some basic definitions to know the notions of the ring of integer and the discriminant.

Definition 1.1. *Let A be an integral domain, and let L be a field containing A. An element α of L is said to be integral over A if it is a root if a monic polynomial with coefficients in A, i.e., of ot satisfies an equation*

$$\alpha^n + a_1\alpha^{n-1} + \cdots + a_n = 0,\ a_i \in A.$$

An algebraic number field is a finite field extensions of $\mathbb{Q}$. The elements of the algebraic number field are called algebraic numbers. An algebraic number is called integral, or an algebraic integer, if it is a zero of a monic polynimial over $\mathbb{Z}$.

Definition 1.2. *The ring of elements of L integral over A is called the integral closure of A in L. The integral closure of $\mathbb{Z}$ in an algebraic number field L is called the ring of integers $\mathcal{O}_L$ in L.*

Consider for the field $\mathbb{Q}[\sqrt{D}]$, where D is a square-free integer. Then the minimum polynomial of $a + b\sqrt{D}, b \neq 0, a, b \in \mathbb{Q}$, is $x^2 - 2ax + (a^2 - b^2D)$, so $a + b\sqrt{D}$ is an algebraic integer if and only if $2a \in \mathbb{Z}, (a^2 - b^2D) \in \mathbb{Z}$.
(a) If $D \equiv 2$ or $D \equiv 3 \pmod 4$, $\mathcal{O}_{\mathbb{Q}[\sqrt{D}]} = \mathbb{Z}[\sqrt{D}]$ consists of all elements of the form $a + b\sqrt{D}$ with a, $b \in \mathbb{Z}$.
(b) If $D \equiv 1 \pmod 4$, $\mathcal{O}_{\mathbb{Q}[\sqrt{D}]} = \mathbb{Z}[\frac{a+b\sqrt{D}}{2}]$.

Definition 1.3. *A ring A is integrally closed if it is its own integral closure in its field of fractions K, i.e., if*

$$\alpha \in K,\ \alpha \text{ integral over} A \Rightarrow \alpha \in A.$$

The rings $\mathbb{Z}$ and $\mathbb{Z}[i]$ are integrally closed, but unique factorization fails in $\mathbb{Z}[\sqrt{-3}]$.

Definition 1.4. *If L is a finite extension of K (L and K fields), then*

$$(\alpha,\ \beta) \mapsto Tr_{L/K}(\alpha\beta) : L \times L \to K.$$

is a symmetric bilinear form on L regarded as a vector space over K, and the discriminant of this form is called the discriminant of L/K.
More generally, let $B \supset A$ be rings, and assume B is free of rank m as an A-module. Let $\beta_1, \ldots, \beta_m$ be elements of B. We define their discriminant to be

$$D(\beta_1, \ldots, \beta_m) = det(Tr_{B/A}(\beta_i\beta_j)).$$

In particular, the ideal in A that it generates is independent of the choice of the basis. This ideal, or $D(\beta_1, \ldots, \beta_m)$ itself regarded as an elemet of $A/A^{\times 2}$, is called the discriminant $disc(B/A)$ of B over A.

Definition 1.5. *When K is a number field, a basis $\alpha_1, \ldots, \alpha_m$ for $\mathcal{O}_K$ as a $\mathbb{Z}$-module is called an integral basis for K.*

Date: march 22, 2019.

2. Properties

Theorem 2.1. *The elements of L integral over A form a ring.*

We will sketch of one of them which is Dedekind's. First, the following propsition is necessary.

Proposition 2.2. *Let L be a field containg A. An element α of L is integral over A if and only if there exists a nonzero finitely generated A-submodule of L such that $\alpha M \subset M$ (in fact, we can take $M = A[\alpha]$, the A-subalgebra generated by α).*

One direction of the proof is trivial, and the opposite is using Cramer's rule. By using **??**, **??** is proved naturally.

Proposition 2.3. *A unique factorization domain, for example, a principal ideal domain, is integrally closed.*

Proposition 2.4. *Let K be the field of fractions of A, and let L be an extension of K of finite degree. Assume A is integrally closed. An element α of L is integral over A if and only if its minimum polynomial over K has coefficients in A.*

An element $\alpha \in \mathbb{Q}[\sqrt{d}]$ is integral over $\mathbb{Z}$ if and only if its trace and norm both lie in $\mathbb{Z}$.

Proposition 2.5. *If B is integral over A and finitely generated as an A-algebra, then it is finitely generated as an A-module.*

Proposition 2.6. *Consider integral domains $A \subset B \subset C$; if B is integral over A, and C is integral over B, then C in integral over A.*

Corollary 2.7. *The integral closure of A in an algebraic extension L of its field of fractions is integrally closed.*

In particular, the ring of integers in a number field is integrally closed.

Let k be a finite field, and let K be a finite extension of $k(X)$. Let $\mathcal{O}_K$ be the integral closure of $k[X]$ in K. The arithmetic of $\mathcal{O}_K$ is very similar to that of the ring of integers in a number field.

Proposition 2.8. *Let $A \subset B$ be integral domains and assume that B is a free A-module of rank m and that $disc(B/A) \neq 0$. Elements $\gamma_1, \dots, \gamma_m$ form a basis for B as an A-module if and only if*

$$(D(\gamma_1, \dots, \gamma_m)) = (disc(B/A)) \text{ (as ideals in } A).$$

Take $A = \mathbb{Z}$ in **??**. Elements $\gamma_1, \dots, \gamma_m$ generate a submodule N of finite index in B if and only if $D(\gamma_1, \dots, \gamma_m) \neq 0$, in which case

$$D(\gamma_1, \dots, \gamma_m) = (B : N)^2 \cdot disc(B/\mathbb{Z}).$$

Proposition 2.9. *Let A be an integrally closed integral domain with field of fractions K, and let B the integral closure of A in a separable extension L of K of degree m. There exists free A-submodules M and M' of L such that*

$$M \subset B \subset M' \tag{2.1}$$

Therefore B is a finitely generated A-module if A is Noetherian, and it is free of rank m if A is a principal ideal domain.

Corollary 2.10. *The ring of integers in a number field L is the largest subring that is finitely generated as a $\mathbb{Z}$-module.*

$\mathcal{O}_K$ is finitely generated as a $\mathbb{Z}$-module. Furthermore, it will be a free module over $\mathbb{Z}$.

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.