

HOMEWORK 3 : DEDEKIND DOMAINS; FACTORIZATION

HYOJIN KIM

In this note prove that rings of integers in number fields are Dedekind domains, and hence that their ideals factor uniquely into products of prime ideals. We will bring some basic definitions and statements from the first and the second notes.

1. INTEGRAL CLOSURE OF DEDEKIND DOMAINS

Lemma 1.1. *Every integral domain B containing a field k and algebraic over k is itself a field.*

Proof: Let β be a nonzero element of B . We have to prove that it has an inverse in B . Because β is algebraic over k , the ring $k[\beta]$ is finite-dimensional as a k -vector space, and the map $x \mapsto \beta x : k[\beta] \rightarrow k[\beta]$ is injective because B is an integral domain. From linear algebra we deduce that the map is surjective, and so there is an element $\beta' \in k[\beta]$ such that $\beta\beta' = 1$. \square

Theorem 1.2. *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 . Then B is a Dedekind domain.*

Proof: By definition, a Dedekind domain is an integrally closed Noetherian integral domain. We first show that the integral closure B is Noetherian.

Note that for an integrally closed integral domain A with field of fractions K , and the integral closure B of A in a separable extension L of K of degree m , there exists free A -submodules M and M' of L such that

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

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.

Hence B is contained in a finitely generated A -module. It follows that every ideal in B is finitely generated when regarded as an A -module (being a submodule of a Noetherian A -module) and as an ideal (= B -module).

Since B is the integral closure of A in an algebraic extension L of its field of fractions, B is integrally closed. It remains to prove that every nonzero prime ideal \mathfrak{q} of B is maximal. Let $\beta \in \mathfrak{q}$, $\beta \neq 0$. Then β is integral over A , and so there is an equation

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

which we may suppose to have the minimum possible degree. Then $a_n \neq 0$. As $a_n \in \beta B \cap A$, we have that $\mathfrak{q} \cap A \neq (0)$. But $\mathfrak{q} \cap A$ is a prime ideal, and so it is a maximal ideal \mathfrak{p} of A , and A/\mathfrak{p} is a field. Since B/\mathfrak{q} is an integral domain, and the map

$$a + \mathfrak{p} \mapsto a + \mathfrak{q}$$

identifies A/\mathfrak{p} with a subfield B/\mathfrak{q} . As B is integral over A , B/\mathfrak{q} is algebraic over A/\mathfrak{p} . Above lemma implies that B/\mathfrak{q} is a field, and hence that \mathfrak{q} is maximal. \square

REFERENCES

- [1] James. S. Milne, *Algebraic Number Theory* (v3.07), 2017. Available at www.jmilne.org/math/.
- [2] P. Samuel, *Algebraic Theory of Numbers*, translated from the French by Allan J. Silberberger, HERMANN, Paris, 1970.