MATH 225A: LECTURE 4
OCTOBER 5, 2021
SCRIBE: ARTHUR DIEP-NGUYEN

In this lecture, we continue our discussion of Dedekind domains, building up theory so that we may later achieve the goal of showing that any nonzero ideal in a Dedekind domain may be written uniquely as a product of prime ideals.

Recall from the previous lecture the following definition.

Definition 2.2. An integral domain R is said to be a **Dedekind domain** if the following conditions are satisfied:

(i) R is a Noetherian ring,
(ii) R is integrally closed, and
(iii) all nonzero prime ideals of R are maximal ideals.

As we shall see in Corollary 2.6, rings of algebraic integers in algebraic number fields are Dedekind domains. Understanding Dedekind domains will inform our study of rings of algebraic integers, which will in turn help us easily solve problems that were historically formulated in terms of integers.

One of our instrumental goals is to prove the following theorem, which guarantees unique factorization for ideals in Dedekind domains.

Theorem 2.3. *Any nonzero ideal in a Dedekind domain may be written uniquely as a product of prime ideals.*

One can clearly see the parallel between unique factorization of ideals into prime ideals and unique factorization of integers into prime numbers. Unique factorization of ideals in Dedekind domains allows us to generalize useful

concepts from elementary number theory like divisibility. We shall defer the proof of Theorem 2.3 for a later lecture, after we have built up a sufficient understanding of Dedekind domains.

Before we proceed, consider the following definition.

Definition 2.4. Let R be an integral domain with a field of fractions K. We call any finitely generated R-submodule M of K a **fractional ideal** of R. Furthermore, if $M \subseteq R$, then we say that R is an **integral ideal** of R.

While fractional ideals aren't used in this lecture, they will be used in the upcoming lecture. In Dedekind domains, the fractional ideals form an (abelian) group. Later, we will see in Theorem 2.9 that for any maximal ideal in a Dedekind domain R, there exists a fractional ideal such that the product of the two ideals is R.

Now consider the following theorem.

Theorem 2.5. *Let R be a Dedekind domain with field of fractions K. Let L/K be a finite separable extension. Then the integral closure S of R in L is a Dedekind domain.*

We shall not prove this theorem in full generality. Instead, for the purposes of this course, it suffices to prove the case where $R = \mathbb{Z}$. By setting $R = \mathbb{Z}$ and letting $L/\mathbb{Q}$ be any finite extension, we obtain an immediate corollary of Theorem 2.5:

Corollary 2.6. The ring of (algebraic) integers in an (algebraic) number field is a Dedekind domain.

By Corollary 2.6, we may apply any of our results about Dedekind domains to rings of integers, which will help us tackle number-theoretic problems.

Next, we will prove Theorem 2.5 for the case $R = \mathbb{Z}$. In the following proof, we shall prove in full generality (i.e. with R any Dedekind domain) that S satisfies conditions (i) and (ii) of the definition of Dedekind domain, then prove that S satisfies condition (iii) for the case $R = \mathbb{Z}$.

Proof. (of Theorem 2.5 for the case $R = \mathbb{Z}$) Suppose R is a Dedekind domain with field of fractions K. Let L/K be a finite separable extension. Let S denote the integral closure of R in L. To show that S is a Dedekind domain, we shall show the following:

(i) S is a Noetherian ring.
(ii) S is integrally closed.
(iii) All nonzero prime ideals of S are maximal ideals. (We shall show this for the case $R = \mathbb{Z}$.)

(i) S is a Noetherian ring: Let $\{x_1, \ldots, x_n\}$ be a K-basis of L. Since L/K is separable, each x_j is algebraic over K, so x_j is the root of some nonzero polynomial in $K[T]$. After clearing denominators, each x_j is then a root of some nonzero polynomial

$$\sum_{i=0}^{n} a_i T^i \in R[T].$$

Multiplying by a_n^{n-1}, we obtain

$$\sum_{i=0}^{n} a_n^{n-1} a_i T^i = (a_n T)^n + a_{n-1}(a_n T)^{n-1} + \cdots + a_0 a_n^{n-1},$$

so $a_n x_j$ is a root of a nonzero monic polynomial in $R[T]$. In particular, we find that $a_n x_j$ is integral over R. Hence, without loss of generality, we may assume $x_j \in S$ for each j.

Since L/K is separable, the K-basis $\{x_1, \ldots, x_n\}$ admits a dual basis $\{y_1, \ldots, y_n\}$ of L, whereby we have the trace

$$\mathrm{Tr}_{L/K}(x_i y_j) = \delta_{ij}$$

for each i and j. Now take $\alpha \in S$, which may be written

$$\alpha = \sum_{i=1}^{n} b_i y_i$$

with $b_i \in K$ for each i. We want to show that $b_i \in R$ for each i. Once we achieve this, we will see that S is a submodule of a finitely generated module over a Noetherian ring, and hence a finitely generated R-module itself.

Multiplying both sides by x_j, we have

$$\alpha x_j = \sum_{i=1}^{n} b_i y_i x_j.$$

Applying $\mathrm{Tr}_{L/K}$ to both sides of the above equation, we obtain

$$\mathrm{Tr}_{L/K}(\alpha x_j) = b_j.$$

Hence, we find that $b_j \in R$ because $\alpha x_j \in S$. Repeating for all j, we conclude that

$$S \subseteq \sum_{i=1}^{n} R y_i = \bigoplus_{i=1}^{n} R y_i.$$

Since R is a Dedekind domain, we know that R is by definition a Noetherian ring. Since S is a submodule of a finitely generated module over a Noetherian ring, we conclude that S is a finitely generated R-module.

By Proposition 1.5, since S is a finitely generated R-module and R is Noetherian, we know that S is a Noetherian R-module. Finally, by Proposition 1.6, we conclude that S is a Noetherian ring, as desired.

(ii) S is integrally closed: Let $x \in L$ be integral over S, i.e. x is the root of some nonzero monic polynomial in $S[T]$, say

$$T^n + s_{n-1}T^{n-1} + \cdots + s_1 T + s_0 \in S[T].$$

To show that S is integrally closed, we must show that x is integral over R. Since each $s_i \in S$ is integral over R, we know that $R[s_1, \ldots, s_n]$ is finitely generated as an R-module. Since x is a root of the above monic polynomial in $R[s_1, \ldots, s_n]$, we find that $R[x, s_1, \ldots, s_n]$ is finitely generated over $R[s_1, \ldots, s_n]$, so $R[x, s_1, \ldots, s_n]$ is finitely generated over R. Therefore, by Proposition 1.11, we conclude that x is integral over R, so S is integrally closed, as desired.

(iii) All nonzero prime ideals of S are maximal ideals: Set $R = \mathbb{Z}$, so $K = \mathbb{Q}$. As a finite extension of $\mathbb{Q}$, we see that L is an (algebraic) number field and S is the ring of (algebraic) integers of L. Since S is a free $\mathbb{Z}$-module of rank n, we may write

$$S = \bigoplus_{i=1}^{n} \mathbb{Z}\omega_i$$

with some basis $\omega_1, \ldots, \omega_n \in S$ of the $\mathbb{Q}$-vector space L.

Now let $\mathfrak{P}$ be a nonzero prime ideal of S. We have either $\mathfrak{P} \cap \mathbb{Z} = p\mathbb{Z}$ for some prime $p \in \mathbb{Z}$ or $\mathfrak{P} \cap \mathbb{Z} = \{0\}$. Let $x \in \mathfrak{P} \setminus \{0\}$. We observe that we have the norm

$$0 \neq N_{L/\mathbb{Q}}(x) \in \mathfrak{P} \cap \mathbb{Z}$$

so we must have $\mathfrak{P} \cap \mathbb{Z} = p\mathbb{Z}$ for some prime $p \in \mathbb{Z}$. Consequently, we have the ideals

$$pS \subseteq \mathfrak{P} \subseteq S,$$

so by the Third Isomorphism Theorem we obtain a surjection

$$S/pS \twoheadrightarrow S/\mathfrak{P},$$

whereby we obtain the isomorphism

$$S/pS \cong \bigoplus_{i=1}^{n} \mathbb{F}_p \omega_i,$$

which is finite of cardinality $|S/pS| = p^n$.

Since $\mathfrak{P}$ is prime, we know $S/\mathfrak{P}$ is an integral domain. Since the finite ring S/pS surjects onto $S/\mathfrak{P}$, we know $S/\mathfrak{P}$ is a finite integral domain, so $S/\mathfrak{P}$ is a field. Hence, $\mathfrak{P}$ is a maximal ideal of S, as desired.

Therefore, S is a Dedekind domain. □

We still require some additional preparation before we are ready to prove Theorem 2.3. The following lemma will be useful in this endeavor.

Lemma 2.8. *Let R be a Dedekind domain. Then any nonzero ideal of R contains a product of nonzero prime ideals.*

Proof. Suppose for contradiction that there exists a nonzero ideal of R that does not contain a product of nonzero prime ideals. Let S denote the set of all nonzero ideals of R not containing a product of nonzero prime ideals. By our hypothesis, S is nonempty, so by Proposition 1.3, we find that S contains a maximal element by inclusion, say $\mathfrak{B} \in S$. We know that $\mathfrak{B}$ is not a prime ideal because $\mathfrak{B} \in S$, so there exist $x, y \in R \setminus \mathfrak{B}$ such that $xy \in \mathfrak{B}$. Since $\mathfrak{B}$ is maximal in S by inclusion, the ideals $(x, \mathfrak{B})$ and $(y, \mathfrak{B})$ do contain a product of nonzero prime ideals, say

$$\mathfrak{P}_1\mathfrak{P}_2\cdots\mathfrak{P}_n \subseteq (x, \mathfrak{B}) \quad \text{and} \quad \mathfrak{Q}_1\mathfrak{Q}_2\cdots\mathfrak{Q}_m \subseteq (y, \mathfrak{B}).$$

Since $xy \in \mathfrak{B}$, the product $(x, \mathfrak{B}) \cdot (y, \mathfrak{B})$ is a subset of $\mathfrak{B}$. We have the product of prime ideals

$$\mathfrak{P}_1\mathfrak{P}_2 \cdots \mathfrak{P}_n\mathfrak{Q}_1\mathfrak{Q}_2 \cdots \mathfrak{Q}_m \subseteq (x, \mathfrak{B}) \cdot (y, \mathfrak{B}) \subseteq \mathfrak{B},$$

which contradicts our assumption $\mathfrak{B} \in S$. □

As a preview for the content of the next lecture, we shall introduce one more theorem (without proof, for now) before concluding this lecture. This theorem is one of the reasons why we introduced fractional ideals earlier in the lecture.

Theorem 2.9. *Let R be a Dedekind domain with field of fractions K, and let M be a maximal ideal in R. Then there exists a fractional ideal $\mathfrak{M}^{-1}$ in K such that $\mathfrak{M}\mathfrak{M}^{-1} = R$.*

As we will see next time, setting $\mathfrak{M}^{-1}$ as

$$\mathfrak{M}^{-1} = \{x \in K : x\mathfrak{M} \subseteq R\}$$

will give us the desired fractional ideal.