IDEAL THEORY AND PRÜFER DOMAINS

FELIX GOTTI

Dedekind Domains

Throughout this section, R is an integral domain. Recall that $\mathrm{qf}(R)$ denotes the quotient field of R.

Dedekind Domains. It is natural to wonder which Prüfer domains are Noetherian domains. Noetherian Prüfer domains are perhaps the best studied and understood class of Prüfer domains; they are called Dedekind domains. We will use, however, a more standard definition.

Definition 1. An integral domain is a *Dedekind domain* if it is a one-dimensional integrally closed Noetherian domain.

Note that, according to our definition, fields are not Dedekind domains. There are authors, however, who include fields in the class of Dedekind domains. One of the most relevant classes of Dedekind domains is that consisting of rings of integers of algebraic number fields.

Example 2. Let K be an algebraic number field, that is, a finite-dimensional field extension of $\mathbb{Q}$. The integral closure of $\mathbb{Z}$ in K is called the *ring of integers* of K and is denoted by $\mathscr{O}_K$. As a consequence of Theorem 12, we will obtain that $\mathscr{O}_K$ is a Dedekind domain. The ring $\mathscr{O}_K$ is called a *quadratic ring of integers* when K is two-dimensional over $\mathbb{Q}$, in which case, there exists a nonzero square-free integer d such that $K = \mathbb{Q}(\sqrt{d})$. In this case, it is not hard to verify that

$$\mathscr{O}_K = \mathbb{Z}[\sqrt{d}] \ \text{ if } \ d \equiv 2, 3 \pmod 4 \quad \text{and} \quad \mathscr{O}_K = \mathbb{Z}\Big[\frac{1+\sqrt{d}}{2}\Big] \ \text{ if } \ d \equiv 1 \pmod 4.$$

The class of Dedekind domains also includes that of PIDs.

Proposition 3. *Every PID that is not a field is a Dedekind domain.*

Proof. Every PID is clearly Noetherian. Also, as PIDs are UFDs, they are integrally closed. Finally, we know that every prime ideal in a PID is maximal, which implies that every PID has dimension at most 1. Hence every PID that is not a field is a Dedekind domain. □

The converse of Proposition 3 does not hold.

Example 4. Let us verify that $R := \mathbb{Z}[\sqrt{-5}]$ is not a PID. One can easily check that for every $x := a + b\sqrt{-5} \in R$, the equality $|R/Rx| = a^2 + 5b^2$ holds. With this in mind, let us argue that the ideal $J := (2, 1 + \sqrt{-5})$ is not principal. First, notice that

$$R/J \cong \mathbb{Z}[x]/(x^2 + 5, 2, 1 + x) \cong \mathbb{F}_2[x]/(x^2 + 5, 1 + x) = \mathbb{F}_2[x]/(1 + x) \cong \mathbb{F}_2,$$

where $\mathbb{F}_2$ denotes the field of two elements. Therefore $|R/J| = 2$. Now our initial observation, along with the fact that the equation $a^2 + 5b^2 = 2$ is not solvable in $\mathbb{Z}^2$, ensures that J cannot be a principal ideal of R. Indeed, it can be proved that R is not even a UFD as $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ (see [1] for a better understanding about factorizations in $\mathbb{Z}[\sqrt{-5}]$).

We proceed to establish some useful characterizations of a Dedekind domain.

Theorem 5. *For an integral domain R that is not a field, the following statements are equivalent.*

(a) *R is a Dedekind domain.*
(b) *R is Noetherian and R_P is a DVR/PID for every prime ideal P of R.*
(c) *Every nonzero ideal of R is invertible.*
(d) *Every nonzero fractional ideal of R is invertible*

Proof. (a) ⇒ (b): Let R be a Dedekind domain, and let P be a prime ideal of R. The properties of being Noetherian, being integrally closed, and having dimension at most 1 are preserved under localization. Hence R_P is a local ring having the mentioned properties, and therefore R_P is a DVR. Hence R_P is a PID.

(b) ⇒ (c): Suppose, by way of contradiction, that there is a nonzero ideal I of R that is not invertible. Since R is Noetherian, $I = Ra_1 + \cdots + Ra_n$ for some $a_1, \ldots, a_n \in R$. Because I is not invertible, $IJ \subsetneq R$, where $J = \{r \in \text{qf}(R) : rI \subseteq R\}$. Let P be a maximal ideal of R such that $IJ \subseteq P$. By (b), the ideal extension I_P of I is principal in R_P. Then we can take $a \in I$ such that $I_P = aR_P$. For each $i \in [\![1, n]\!]$, take $r_i \in R$ and $s_i \notin P$ such that $a_i = a(r_i/s_i)$, that is, $s_i a_i \in Ra$. Setting $s = s_1 \ldots s_n$, we obtain that $sa^{-1}a_i \in R$ for every $i \in [\![1, n]\!]$, which implies that $sa^{-1}I \subseteq R$. Hence $sa^{-1} \in J$ and, as a result, $s = asa^{-1} \in IJ \subseteq P$, which is a contradiction. As a final note, we observe that the argument used to prove this implication was also used to characterize Prüfer domains as integral domains whose localizations at prime ideals are valuation domains.

(c) ⇒ (a): We have seen before that every invertible ideal is finitely generated. Thus, R is Noetherian. Now suppose that M is a maximal ideal of R. We can easily verify that the extension of any invertible ideal of R is invertible in R_M. Then each nonzero ideal of R_M is invertible. Since every invertible ideal of a local ring is principal (see previous lectures), R_M is a PID. Hence R_M is both integrally closed and 1-dimensional. As M was an arbitrarily-chosen maximal ideal of R, it follows that R

is also integrally closed and 1-dimensional. Thus, we conclude that R is a Dedekind domain.

(c) $\Leftrightarrow$ (d): It suffices to show that (c) implies (d). To do so, let J be a nonzero fractional ideal of R. Take $r \in R$ such that $I := rJ$ is a nonzero ideal of R. Since I is invertible by hypothesis, $rI^{-1} := r(R : I)$ is the inverse of the fractional ideal J: indeed, $(rI^{-1})J = I^{-1}(rJ) = I^{-1}I = R$. □

The Noetherian Prüfer domains (which are not fields) are precisely the Dedekind domains, as the following corollary indicates.

Corollary 6. *An integral domain that is not a field is a Dedekind domain if and only if it is a Noetherian Prüfer domain.*

Proof. Let R be an integral domain that is not a field. If R is a Dedekind domain, then R is Noetherian, and Theorem 5 ensures that R_P is a PID for every prime ideal P. Since every PID is a valuation domain, R is a Prüfer domain, and the direct implication follows. For the reverse implication, it suffices to observe that in a Noetherian Prüfer domain every nonzero ideal is finitely generated and so invertible, whence we are done by virtue of Theorem 5. □

It turns out that Dedekind domains can be characterized as integral domains where every nonzero ideal factors (uniquely) as a product of prime ideals. Before establishing this characterization, let us argue the following lemma.

Lemma 7. *For $m, n \in \mathbb{N}$, let $P_1, \dots, P_m$ and $Q_1, \dots, Q_n$ be invertible prime ideals of an integral domain R. If $P_1 \dots P_m = Q_1 \dots Q_n$, then $m = n$ and $Q_1, \dots, Q_m$ can be relabeled so that $P_i = Q_i$ for every $i \in [\![1, n]\!]$.*

Proof. We proceed by induction on m. Suppose first that $m = 1$. As P_1 is prime, the inclusion $Q_i \subseteq P_1$ holds for some $i \in [\![1, n]\!]$. After relabeling, one can assume that $i = 1$. Since $P_1 = Q_1 \cdots Q_n \subseteq Q_1$, the equality $P_1 = Q_1$ holds. Multiplying both sides of $P_1 = Q_1 \cdots Q_n$ by P_1^{-1}, we obtain that $n = 1$. Now suppose that the statement of the lemma holds for $m \in \mathbb{N}$, and let the equality $P_1 \cdots P_{m+1} = Q_1 \cdots Q_{n+1}$ hold for invertible prime ideals $P_1, \dots, P_{m+1}$ and $Q_1, \dots, Q_{n+1}$ of R. After a possible relabeling, we can assume that P_{m+1} is minimal in the set $\{P_1, \dots, P_{m+1}\}$. As P_{m+1} is prime, $Q_i \subseteq P_{m+1}$ for some $i \in [\![1, n+1]\!]$, and we can assume after a possible relabeling that $i = n+1$. Since Q_{n+1} is prime, $P_j \subseteq Q_{n+1}$ for some $j \in [\![1, m+1]\!]$. Because $P_j \subseteq Q_{n+1} \subseteq P_{m+1}$, the minimality of P_{m+1} ensures that $P_j = P_{m+1}$, and so that $Q_{n+1} = P_{m+1}$. Multiplying $P_1 \cdots P_{m+1} = Q_1 \cdots Q_{n+1}$ by P_{m+1}^{-1} and using the induction hypothesis, we obtain that $m+1 = n+1$ and also that, after a possible relabeling of $Q_1, \dots, Q_{m+1}$, the equality $P_i = Q_i$ holds for every $i \in [\![1, m+1]\!]$. □

We are in a position to give two more characterizations of a Dedekind domain.

Theorem 8. *For an integral domain R that is not a field, the following statements are equivalent.*

(a) *R is a Dedekind domain.*

(b) *Every nonzero proper ideal of R factors into prime ideals.*

(c) *Every nonzero proper ideal of R factors uniquely (up to permutation) into prime ideals.*

Proof. (a) ⇒ (b): Suppose, by way of contradiction that there is a proper nonzero ideal that does not factor into prime ideals. Let I be maximal among all such ideals, which exists because R is Noetherian. Clearly, I is a proper ideal that is not prime. Therefore I is properly contained in a maximal ideal P of R. Since P is invertible, $P^{-1}I \subseteq P^{-1}P = R$. Therefore $P^{-1}I$ is an ideal of R, which contains I because $I = P(P^{-1}I)$. In addition, I is properly contained in $P^{-1}I$ as $I = P^{-1}I$ would imply that $IP = I$ and so $P = I^{-1}I = R$. Then $P^{-1}I$ factors as a product of prime ideals, and so the same holds for I, a contradiction.

(b) ⇒ (a): We first argue that every invertible prime ideal of R is maximal. To do this, let P be an invertible prime ideal and suppose, towards a contradiction, that $P + Rx \neq R$ for some $x \in R \setminus P$. Take prime ideals $P_1, \dots, P_m$ and $Q_1, \dots, Q_n$ such that $P + Rx = P_1 \cdots P_m$ and $P + Rx^2 = Q_1 \cdots Q_n$. Note the the images $\pi(P_1), \dots, \pi(P_m)$ and $\pi(Q_1), \dots, \pi(Q_n)$ under the canonical homomorphism $\pi \colon R \to R/P$ are prime ideals in the integral domain R/P. These prime ideals are also invertible as each of them is a factor of one of the invertible ideals $(\pi(x))$ and $(\pi(x^2))$. Because

$$\pi(Q_1) \cdots \pi(Q_n) = (\pi(x^2)) = (\pi(x))^2 = \pi(P_1)^2 \cdots \pi(P_m)^2,$$

it follows from Lemma 7 that $n = 2m$ and that, after a possible relabeling, $\pi(Q_{2j-1}) = \pi(Q_{2j}) = \pi(P_j)$ for every $j \in [\![1, m]\!]$. As a result, $Q_{2j-1} = Q_{2j} = P_j$ for every $j \in [\![1, m]\!]$. Then $P + Rx^2 = (P + Rx)^2$, which implies that $P \subseteq P + Rx^2 = (P + Rx)^2 \subseteq P^2 + Rx$. Indeed, this implies that $P \subseteq P^2 + Px$ because $x \notin P$. Multiplying both sides of the last inclusion by P^{-1}, we obtain that $P + Rx = R$, a contradiction. Thus, every invertible prime ideal of R is maximal.

By virtue of Theorem 5, finishing the proof of the current implication amounts to verifying that every nonzero prime ideal of R is invertible. Let P be a nonzero prime ideal of R, and take a nonzero element $a \in P$. Write $Ra = P_1 \cdots P_k$ for prime ideals $P_1, \dots, P_k$. The ideals $P_1, \dots, P_k$ are invertible because Ra is invertible. Since $P_1 \cdots P_k \subseteq P$, it follows that $P_i \subseteq P$ for some $i \in [\![1, k]\!]$. As P_i is an invertible prime ideal, it is maximal. Hence $P = P_i$, and so P is invertible.

(b) ⇔ (c): It is clear that (c) implies (b). On the other hand, if (b) holds, then (a) also holds, and so every nonzero ideal of R is invertible by Theorem 5. Thus, it follows from Lemma 7 that every factorization of a nonzero proper ideal into prime ideals must be unique, whence (b) implies (c). □

We have seen in Proposition 3 that every PID that is not a field is a Dedekind domain. On the other hand, not every UFD is a Dedekind domain as, for instance, the UFD $\mathbb{Q}[x,y]$ has Krull dimension two. However, if a UFD is a Dedekind domain, then it must be a PID.

Proposition 9. *Let R be a Dedekind domain. Then R is a UFD if and only if it is a PID.*

Proof. It suffices to prove the direct implication as the reverse implication always holds. Suppose that the Dedekind domain R is a UFD. Let P be a nonzero prime ideal of R, and take a nonzero $a \in P$. As R is a UFD, we can write $a = a_1 \cdots a_n$ for some irreducibles $a_1, \dots, a_n$ of R. Since each of the elements $a_1, \dots, a_n$ is prime so are the principal ideals $Ra_1, \dots, Ra_n$. Because the product of these ideals equals Ra, which is contained in the prime ideal P, the inclusion $Ra_i \subseteq P$ holds for some index $i \in [\![1, n]\!]$. As both Ra_i and P are prime ideals of R and $\dim R = 1$, we obtain that $P = Ra_i$. Hence every prime ideal of R is principal. Finally, it follows from Theorem 8 that every proper ideal of R factors into prime ideals, whence every ideal of R must be principal. Thus, R is a PID. □

The previous proposition can be strengthened as the following remark indicates.

Remark 10. It is true, in fact, that if R is an integral domain with dimension at most 1, then R is a UFD if and only if R is a PID.

Overrings and Extensions of Dedekind Domains. Overrings and certain extension rings of a Dedekind domain are Dedekind domain. Let us start with the overrings of Dedekind domains.

Proposition 11. *Any overring of a Dedekind domain is a Dedekind domain.*

Proof. Let R be a Dedekind domain, and let T be an overring of R. Since R is a one-dimensional Noetherian domain, so is T. Let Q be a prime ideal of T, and consider the prime ideal $P = Q \cap R$ of R. Then $R_P \subseteq T_Q \subseteq \operatorname{qf}(R)$, that is, T_Q is an overring of R_P. Since R is Dedekind, R_P is a valuation domain, whence T_Q is also a valuation domain. Since T is Noetherian, T_Q is a Noetherian valuation domain, that is, a DVR. Hence T is a Dedekind domain by Theorem 5. □

Our final goal in this lecture is to prove that the integral closure of a Dedekind domain in a finite-dimensional field extension of its quotient field is again a Dedekind domain. In certain way, this result can be considered as the starting point of algebraic number theory.

Theorem 12. *Let R be a Dedekind domain, and let K be a finite-dimensional field extension of the quotient field of R. Then the integral closure of R in K is a Dedekind domain.*

Proof. Let F denote the quotient field of R (inside K), and let T denote the integral closure of R in K. It is clear that T is integrally closed. To argue that T is a one-dimensional Noetherian domain, take a basis $\{v_1, \dots, v_n\}$ for K as a vector space over F. As K is finite-dimensional over F, for every $i \in [\![1, n]\!]$ there is an element $r_i \in R$ such that $r_i v_i \in T$. After multiplying each element in the basis by $r_1 \cdots r_n$, we can assume that the basis is contained in T. Now set $S := R[v_1, \dots, v_n]$, and observe that the quotient field of S is K. As S is a finitely generated R-module, it is a Noetherian ring. On the other hand, as S is an integral extension of the one-dimensional domain R, it is also one-dimensional. Now the fact that T is an overring of S, which is a one-dimensional Noetherian domain, allows us to conclude that T is also a one-dimensional Noetherian domain. Hence T is a Dedekind domain. □

We conclude with the following promised corollary.

Corollary 13. *For any algebraic number field K, the ring of integers $\mathscr{O}_K$ is a Dedekind domain.*

Exercises

Exercise 1. *Let R be a Dedekind domain, and let I and J be two nonzero ideals of R. Prove the following statements.*

(1) *$I \subseteq J$ if and only if $I = JK$ for some ideal K of R.*

(2) *$I + J$ is the greatest common divisor of I and J in the (free commutative) monoid of nonzero ideals of R under ideal multiplication.*

Exercise 2 (Chinese Remainder Theorem)**.** *Let R be a Dedekind domain, and let $P_1, \dots, P_n$ be distinct prime ideals of R. Prove that if $k_1, \dots, k_n \in \mathbb{N}$, then*

$$R/(P_1^{k_1} \cdots P_n^{k_n}) \cong R/P_1^{k_1} \times \cdots \times R/P_n^{k_n}.$$

Exercise 3. *Let R be a Dedekind domain, and let I be a nonzero ideal of R. Prove the following statements.*

(1) *Every ideal of R/I is principal.*

(2) *For every nonzero $a \in I$, there is a $b \in I$ such that $I = Ra + Rb$. In particular, every ideal in a Dedekind domain can be generated by two elements.*

Hint: Use the Chinese Remainder Theorem.

Exercise 4. *Let R be an integral domain with dimension at most 1. Prove that R is a UFD if and only if R is a PID.*

References

[1] S. T. Chapman, F. Gotti, and M. Gotti: *How do elements really factor in* $\mathbb{Z}[\sqrt{-5}]$*?*. In: Advances in Commutative Algebra (Eds. A. Badawi and J. Coykendall), pp. 171–195, Springer Trends in Mathematics, Birkhäuser, Singapore, 2019.

Department of Mathematics, MIT, Cambridge, MA 02139
Email address: fgotti@mit.edu