IDEAL THEORY AND PRÜFER DOMAINS

FELIX GOTTI

Discrete Valuation Rings

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

Definition 1. If a valuation domain is Noetherian, then it is called a *discrete valuation ring (DVR)*.

Example 2. For each $p \in \mathbb{P}$, we have seen before that $\mathbb{Z}_{(p)}$ is a valuation domain. Since $\mathbb{Z}$ is Noetherian, $\mathbb{Z}_{(p)}$ is also Noetherian and, therefore, a DVR. Note, in addition, that $\mathbb{Z}_{(p)}$ is a local domain whose maximal ideal, $p\mathbb{Z}_{(p)}$, is principal.

In general, we can characterize DVRs as follows.

Theorem 3. *For an integral domain R, the following statements are equivalent.*

(a) *R is a DVR.*

(b) *R is a local PID.*

(c) *R is a local Noetherian domain whose maximal ideal is principal.*

(d) *R is a local Noetherian integrally closed domain with $\dim R \le 1$.*

Proof. (a) $\Rightarrow$ (b): A valuation domain is always local. On the other hand, since every valuation domain is a Bezout domain, the fact that R is Noetherian implies that every ideal of R is principal.

(b) $\Rightarrow$ (a): Every PID is Noetherian. In addition, every PID is a Bezout domain, and every local Bezout domain is a valuation domain.

(b) $\Rightarrow$ (c): This is clear.

(c) $\Rightarrow$ (b): Assume that R is a local Noetherian domain with maximal ideal $M = Rx$ for some $x \in R$. To show that R is a PID, let I be a proper ideal of R. By Krull's Intersection Theorem, $\bigcap_{n \in \mathbb{N}} M^n = (0)$, and so there is an $n \in \mathbb{N}$ such that $I \subseteq M^n$ but $I \nsubseteq M^{n+1}$. Take $a \in I \setminus M^{n+1}$, and write $a = ux^n$ for some $u \in R$. Since $a \notin M^{n+1}$, we obtain that $u \notin M$. As R is local, $u \in R^\times$, and so $x^n = u^{-1}a \in I$. This implies that $I = M^n$ is a principal ideal. Hence R is a PID.

(b) $\Rightarrow$ (d): It follows from the fact that a PID is a local Noetherian integrally closed domain with Krull dimension at most 1.

(d) $\Rightarrow$ (c): Let M be the maximal ideal of R. If R is a field, then $M = (0)$ is clearly principal. So we will assume that $\dim R = 1$. As R is Noetherian, there is an ideal Rx that is maximal among all the principal ideals contained in M. Our aim is to show that $M = Rx$, and for this it suffices to argue that $M \subseteq Rx$. Suppose, by way of contradiction, that this is not the case. Since R is a 1-dimensional local domain, $\operatorname{Rad} Rx = M$, and so the fact that M is finitely generated guarantees the existence of a minimum $m \in \mathbb{N}$ such that $M^m \subseteq Rx$. Take $y \in M^{m-1}$ so that $y \notin Rx$ (note that $m \ge 2$). Then $y/x \in \operatorname{qf}(R)$ satisfies that $y/x \notin R$ but $(y/x)M \subseteq R$. Since $(y/x)M$ is an ideal of R, either $(y/x)M = R$ or $(y/x)M \subseteq M$.

CASE 1: $(y/x)M = R$. In this case, we can take $r \in M$ such that $yr = x$. Since $r \notin R^\times$, it follows that $Rx \subsetneq Ry$, which contradicts the maximality of Rx.

CASE 2: $(y/x)M \subseteq M$. Set $s = y/x$. Since R is Noetherian, we can take nonzero elements $a_1, \dots, a_n \in R$ such that $M = Rv_1 + \dots + Rv_n$. As $sM \subseteq M$, for every $j \in [\![1, n]\!]$ we can write $sv_j = \sum_{i=1}^n c_{ij} v_i$ for some $c_{1j}, \dots, c_{nj} \in R$. Equivalently, $Av = 0$, where A is the matrix $(\delta_{ij} s - c_{ij})_{1 \le i,j \le n}$ and v is the vector $(v_1, \dots, v_n)^T$. By Cramer's Rule, $(\det A)v_1 = 0$. So $\det A = 0$, which implies that $s = y/x$ is a root of the monic polynomial $\det(tI_n - C) \in R[t]$, where $C = (c_{ij})_{1 \le i,j \le n}$. Hence y/x is integral over R. Since R is integrally closed, $y/x \in R$, which is a contradiction. □

As part of the proof of Theorem 3, we obtained the following result.

Corollary 4. *If R is a DVR with maximal ideal M, then the set of nonzero proper ideals of R is $\{M^n : n \in \mathbb{N}\}$.*

Example 5. Fix $p \in \mathbb{P}$ and consider the DVR $\mathbb{Z}_{(p)}$. Suppose that I is a nonzero proper ideal of $\mathbb{Z}_{(p)}$. Since $\mathbb{Z}_{(p)}$ is principal, there exists $q \in \mathbb{Z}_{(p)}$ such that $I = q\mathbb{Z}_{(p)}$. Let n be the unique nonnegative integer such that $q = p^n \frac{a}{b}$ for some nonzero $a, b \in \mathbb{Z}$ such that $p \nmid a$ (as I is proper, $n \ge 1$). Then $I = p^n \mathbb{Z}_{(p)} = (p\mathbb{Z}_{(p)})^n$.

We can also characterize DVRs in terms of valuation maps; indeed, it is precisely the valuation group in this characterization what motivates the term "discrete valuation ring". A valuation map $v \colon F \to \mathbb{Z} \cup \{\infty\}$ that is surjective is called a *discrete valuation map.*

Theorem 6. *For an integral domain R, the following statements are equivalent.*

(a) *R is a DVR.*

(b) *There is a discrete valuation map $v \colon \operatorname{qf}(R) \to \mathbb{Z} \cup \{\infty\}$ satisfying that $R = v^{-1}(\mathbb{N}_0 \cup \{\infty\})$.*

Proof. (a) $\Rightarrow$ (b): Let R be a DVR, and let M be the maximal ideal of R. It follows from Theorem 3 that $M = Rt$ for some $t \in R$. Suppose now that $q \in \operatorname{qf}(R)^\times$ is contained in R. Because $\bigcap_{n \in \mathbb{N}} M^n = (0)$ by Krull's Intersection Theorem, there is a maximum $v(q) \in \mathbb{N}_0$ such that $t^{v(q)}$ divides q in R. Since R is a valuation domain, we can define $v\colon \operatorname{qf}(R)^\times \to \mathbb{Z}$ by $q \mapsto v(q)$ if $q \in R$ and $v \mapsto -v(q^{-1})$ otherwise. One can easily verify that v is a group homomorphism satisfying $v(q_1+q_2) \ge \min\{v(q_1), v(q_2)\}$ for all $q_1, q_2 \in \operatorname{qf}(R)^\times$ with $q_1 + q_2 \neq 0$. Therefore the extension $v\colon \operatorname{qf}(R) \to \mathbb{Z} \cup \{\infty\}$, where $v(0) = \infty$, is a valuation map. It is clear that $R = \{q \in \operatorname{qf}(R) : v(q) \ge 0\}$.

(b) $\Rightarrow$ (a): Assume now that $v\colon \operatorname{qf}(R) \to \mathbb{Z} \cup \{\infty\}$ is a discrete valuation map with $R = v^{-1}(\mathbb{N}_0 \cup \{\infty\})$. We know from previous lectures that R is a valuation domain with maximal ideal $M := v^{-1}(\mathbb{N} \cup \{\infty\})$ and group of units $R^\times = v^{-1}(0)$. As v is surjective, there is a $t \in R$ with $v(t) = 1$. Now if $r \in M$ and $n = v(r)$, we see that $v(r/t^n) = 0$, and so $r = ut^n$ for some $u \in R^\times$. Hence $M = Rt$ is a principal ideal. Thus, R is a DVR by Theorem 3. □

With notation as in part (b) of Theorem 6, an element $t \in R$ such that $v(t) = 1$ is called a *uniformizer element* of the DVR R.

Example 7. Fix $p \in \mathbb{P}$. The quotient field of the DVR $\mathbb{Z}_{(p)}$ is $\mathbb{Q}$. For each nonzero rational q, there is a unique $n \in \mathbb{Z}$ satisfying that $q = p^n \frac{a}{b}$ for nonzero $a, b \in \mathbb{Z}$ such that $p \nmid ab$. One can easily verify that the map $v\colon \mathbb{Q} \to \mathbb{Z} \cup \{\infty\}$ given by $v(q) = n$ is a discrete valuation map, and it is clear that $\mathbb{Z}_{(p)} = \{q \in \mathbb{Q} : v(q) \ge 0\}$. Note that the uniformizers of $\mathbb{Z}_{(p)}$ are the elements of the form $p\frac{a}{b}$ for nonzero $a, b \in \mathbb{Z}$ with $p \nmid ab$.

Proposition 8. *Let R be a DVR. An element $t \in R$ is a uniformizer if and only if the maximal ideal of R is Rt.*

Proof. We have already argued the direct implication in the proof of Theorem 6 (the part (b) $\Rightarrow$ (a)). For the reverse implication, suppose that $v\colon \operatorname{qf}(R) \to \mathbb{Z} \cup \{\infty\}$ is a discrete valuation map with $R = v^{-1}(\mathbb{N}_0 \cup \{\infty\})$ and that the maximal ideal of R is Rt. Since v is surjective there is a $q \in \operatorname{qf}(R)$ such that $v(q) = 1$, and it is clear that $q \in M$. Writing $q = rt$, we see that $v(t)v(r) = v(q) = 1$, which implies that $v(t) = 1$. Hence t is a uniformizer element of R. □

Corollary 9. *In a DVR, every uniformizer is a prime element, and any two uniformizer elements are associates.*

We have seen before that every DVR is a PID. We conclude this lecture showing that every DVR is indeed a Euclidean domain.

Proposition 10. *Every DVR is a Euclidean domain.*

Proof. Let R be a DVR, and let $v\colon R \to \mathbb{Z} \cup \{\infty\}$ be a discrete valuation map with $R = v^{-1}(\mathbb{N}_0 \cup \{\infty\})$. We verify that R is a Euclidean domain with respect to the norm $v\colon R \setminus \{0\} \to \mathbb{N}_0$. To do so, take $a, b \in R$ such that $b \neq 0$. If $ab^{-1} \in R$, then we can write $a = qb + r$, where $q = ab^{-1} \in R$ and $r = 0$. On the other hand, assume that $ab^{-1} \notin R$. In this case, we can write $a = qb + r$ for $q = 0$ and $r = a$, and observe that $ab^{-1} \notin R$ guarantees that $v(ab^{-1}) < 0$, that is, $v(r) = v(a) < v(b)$. Thus, R is a Euclidean domain. □

Exercises

Exercise 1. *Let F be a field.*

1. *Prove that the ring of formal power series $F[\![x]\!]$ is a DVR.*
2. *The quotient field of $F[\![x]\!]$ is the field of formal Laurent series $F(\!(x)\!)$. Find a discrete valuation map $v \colon F(\!(x)\!) \to \mathbb{Z} \cup \{\infty\}$ such that $v^{-1}(\mathbb{N}_0 \cup \{\infty\}) = F[\![x]\!]$.*

Exercise 2. *Fix $p \in \mathbb{P}$. A p-adic integer is a formal series $\sum_{n \ge 0} c_n p^n$, where c_n belongs to the discrete interval $[\![0, p-1]\!] := \{0, 1, \dots, p-1\}$ for every $n \in \mathbb{N}_0$. We define the addition (resp., multiplication) of two p-adic integers as it is done with formal power series but using carries to keep the coefficients of the sum (resp., product) in the discrete interval $[\![0, p-1]\!]$. The set of p-adic integers is denoted by $\mathbb{Z}_p$.*

1. *Prove that $\mathbb{Z}_p$ is an integral domain. The field of fractions of $\mathbb{Z}_p$, denoted by $\mathbb{Q}_p$, is called the field of p-adic numbers.*
2. *Prove that $\mathbb{Z}_p^\times = \big\{ \sum_{n \ge 0} c_n p^n \in \mathbb{Z}_p : c_0 \neq 0 \big\}$, and then deduce that $\mathbb{Z}_p$ is a local ring.*
3. *Prove that every nonzero ideal of $\mathbb{Z}_p$ has the form $p^n \mathbb{Z}_p$ for some $n \in \mathbb{N}$. Deduce that $\mathbb{Z}_p$ is a DVR.*
4. *Prove that $\mathbb{Q}_p = \mathbb{Z}_p[1/p]$, and find a discrete valuation map $v \colon \mathbb{Q}_p \to \mathbb{Z} \cup \{\infty\}$ satisfying that $v^{-1}(\mathbb{N}_0 \cup \{\infty\}) = \mathbb{Z}_p$.*

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