IDEAL THEORY AND PRÜFER DOMAINS

FELIX GOTTI

Valuation Domains I

For an integral domain R, we let $\mathrm{qf}(R)$ denote the quotient field of R.

Characterizations. The primary purpose of this subsection is to introduce valuation domains and provide several useful characterizations.

Definition 1. An integral domain R is called a *valuation domain* if for every nonzero $x \in \mathrm{qf}(R)$, either x or x^{-1} belongs to R.

We observe that if R is a valuation domain, then for all nonzero $x, y \in R$ either $xy^{-1} \in R$ or $yx^{-1} \in R$, which means that $y \mid_R x$ or $x \mid_R y$.

It is clear from the definition that every field is a valuation domain. In addition, if R is a valuation domain and S is an extension ring of R with $R \subseteq S \subseteq \mathrm{qf}(R)$, then S is also a valuation domain. Let us take a look at another example.

Example 2. For $p \in \mathbb{P}$, and consider the localization $\mathbb{Z}_{(p)}$ of $\mathbb{Z}$ at the prime ideal (p). The quotient field of $\mathbb{Z}_{(p)}$ is $\mathbb{Q}$. It is clear that for every nonzero rational number q, either $q \in \mathbb{Z}_{(p)}$ or $q^{-1} \in \mathbb{Z}_{(p)}$. As a result, $\mathbb{Z}_{(p)}$ is a valuation domain.

Example 3. What are the valuation domains of $\mathbb{C}(x)$? As in the previous example, we can readily see that $\mathbb{C}[x]_{(x-\alpha)}$ for any $\alpha \in \mathbb{C}$ are valuation domains of $\mathbb{C}(x)$. Indeed, these are the only valuation rings of $\mathbb{C}(x)$ containing $\mathbb{C}[x]$ (prove this!). However, there is a valuation domain of $\mathbb{C}(x)$ that does not contain $\mathbb{C}[x]$: the integral domain $R := \mathbb{C}[x^{-1}]_{(x^{-1})}$. To show that R is a valuation domain it suffices to observe that $x \mapsto x^{-1}$ induces an automorphism of $\mathbb{C}(x)$ sending $\mathbb{C}[x]_{(x)}$ to R.

A *fractional ideal* J of an integral domain R is an R-submodule of $\mathrm{qf}(R)$ for which there exists a nonzero $r \in R$ such that rJ is an ideal of R. A fractional ideal J is called *principal* if there exists $x \in \mathrm{qf}(R)$ such that $J = Rx$. In particular, every ideal (resp., principal ideal) of an integral domain is a fractional ideal (resp., principal fractional ideal).

Example 4. If R is an integral domain, and J is a finitely generated R-submodule of $\mathrm{qf}(R)$, then J is a fractional ideals. To check this, suppose that $J = Rq_1 + \cdots + Rq_n$ for some $q_1, \dots, q_n \in J$. For each $i \in [\![1, n]\!]$, we can write $q_i = a_i/b_i$ for some $a_i, b_i \in R$ with $b_i \neq 0$. After setting $b = b_1 \cdots b_n$, we see that $bq_1, \dots, bq_n \in R$. As a result, $bJ = Rbq_1 + \cdots + Rbq_n$ is an ideal of R. Hence J is a fractional ideal.

We can characterize a valuation domain in terms of its poset of (principal) ideals.

Proposition 5. *For an integral domain R, the following statements are equivalent.*

(a) *R is a valuation domain.*

(b) *The principal ideals of R are totally ordered by inclusion.*

(c) *The ideals of R are totally ordered by inclusion.*

(d) *The principal fractional ideals of R are totally ordered by inclusion.*

(e) *The fractional ideals of R are totally ordered by inclusion.*

Proof. (a) $\Leftrightarrow$ (b): For all $x, y \in R$, it is clear that $x \mid_R y$ if and only if $yR \subseteq xR$, whence the equivalence follows.

(b) $\Leftrightarrow$ (c): Clearly, (c) implies (b). For the direct implication, suppose that I_1 and I_2 are ideals of R such that $I_1 \nsubseteq I_2$. Take $x \in I_1 \setminus I_2$. Now take $y \in I_2$, and note that $y \nmid_R x$, which means that $xR \nsubseteq yR$. Since the principal ideals of R are totally ordered, $y \in yR \subseteq xR \subseteq I_1$. Thus, $I_2 \subseteq I_1$.

(c) $\Rightarrow$ [(d) and (e)]: It suffices to check that (c) implies (e). Let J_1 and J_2 be two fractional ideals of R. Take $r_1, r_2 \in R$ such that $r_1 J_1$ and $r_2 J_2$ are ideals of R. Then $r_1 r_2 J_1$ and $r_1 r_2 J_2$ are also ideals of R, and so they must be comparable. Hence the fractional ideals J_1 and J_2 are also comparable.

[(d) or (e)] $\Rightarrow$ (b): This is obvious. □

Corollary 6. *Every valuation domain is a local ring.*

Proof. It follows from Proposition 5 that the ideals of R are totally ordered by inclusion. Therefore R must contain exactly one maximal ideal, namely, the union of all proper ideals. □

An integral domain R is called a *Bezout domain* if every finitely generated ideal of R is principal. Valuation domains can be characterized as the local Bezout domains.

Let us establish a further characterization of a valuation domain.

Proposition 7. *An integral domain is a valuation domain if and only if it is a local Bezout domain.*

Proof. For the direct implication, suppose that R is a valuation domain. Then R is local by Corollary 6. To show that R is a Bezout domain, let $I = (r_1, \dots, r_n)$ be a finitely generated ideal of R. Since $\{r_j R : j \in [\![1, n]\!]\}$ is a totally ordered, it has a maximum element, namely, rR for some $r \in \{r_1, \dots, r_n\}$. It is clear that $I = rR$. Hence R is a local Bezout domain.

For the reverse implication, suppose that R is a local Bezout domain. Take $a, b \in R$, and consider the ideal $I := Ra + Rb$. Let M be the maximal ideal of R. One can easily verify that the abelian group I/MI is indeed an R/M-module, that is, a vector space over the field R/M. Since I is finitely generated, it is principal and, therefore, the vector space I/MI has dimension one. So there exist $u, v \in R$ such that $ua + vb \in MI$, where either $u \in R^\times$ or $v \in R^\times$. So we can take $r, s \in M$ such that $ua + vb = ra + sb$, that is, $(u - r)a = (y - s)b$. Since $u - r \in R^\times$ or $y - s \in R^\times$, it follows that either $b \mid_R a$ or $a \mid_R b$. Hence R is a valuation domain. □

Corollary 8. *Every Noetherian valuation domain is a PID.*

A pair $(G, \leq)$, where G is an additive abelian group and $\leq$ is an order relation on G, is called an *ordered group* provided that $\leq$ is translation-invariant, that is, for all $a, b, c \in G$, the inequality $b \leq c$ implies that $a + b \leq a + c$. If $\leq$ is a total order, then we say that $(G, \leq)$ is a *totally ordered group* or a *linearly ordered group*. To easy notation we often write G instead of $(G, \leq)$. For an ordered group G, the set $G_+ := \{a \in G : a \geq 0\}$ is a submonoid of G, which is called the *nonnegative cone* of G. If G is a totally ordered group, then it follows immediately that, for every $a \in G \setminus \{0\}$, exactly one of the inclusions $a \in G_+$ and $-a \in G_+$ holds.

For a field F and a totally ordered (abelian) group G, a map $v \colon F \to G \cup \{\infty\}$, where ∞ is a symbol not in G such that $x \leq \infty$ and $x + \infty = \infty$ for all $x \in G$, is called a *valuation map* if the following conditions hold:

(1) $v(0) = \infty$,
(2) $v \colon F^\times \to G$ is a group homomorphism, and
(3) $v(x + y) \geq \min\{v(x), v(y)\}$ for all $x, y \in F$.

Here is the characterization of a valuation domain that suggests the chosen terminology.

Theorem 9. *For an integral domain R, the following statements are equivalent.*

(a) *R is a valuation domain.*
(b) *There exists a valuation map $v \colon \mathrm{qf}(R) \to G \cup \{\infty\}$ such that*

$$R = \{x \in \mathrm{qf}(R) : v(x) \geq 0\}.$$

Also, if v and R are as in part (b), then the maximal of R is $\{x \in \mathrm{qf}(R) : v(x) > 0\}$.

Proof. (a) ⇒ (b): Assume that R is a valuation domain, and set $G := \mathrm{qf}(R)^\times / R^\times$. We will write G additively, that is, $xR^\times + yR^\times = xyR^\times$ for all $x, y \in \mathrm{qf}(R)^\times$. Now define the binary relation $\leq$ on G as follows: $xR^\times \leq yR^\times$ if $yx^{-1} \in R$. Using that $yx^{-1} \in R$ if and only if $Ry \subseteq Rx$ for all $x, y \in \mathrm{qf}(R)^\times$, one can readily check that $\leq$ is an order relation on G compatible with the addition, and it follows from Proposition 5 that G is indeed a totally ordered group. Also, we see that $G_+ = \{xR^\times : x \in R \setminus \{0\}\}$.

Now we can define $v \colon \mathrm{qf}(R) \to G \cup \{\infty\}$ by $v(0) = \infty$ and $v(x) = xR^\times$ if $x \neq 0$. It is clear that $v \colon \mathrm{qf}(R)^\times \to G$ is a group homomorphism. Observe that the inequality $v(x+y) \geq \min\{v(x), v(y)\}$ follows immediately when at least one of the elements x, y, and $x+y$ equals zero. Now take $x, y \in \mathrm{qf}(R)^\times$ with $x + y \neq 0$ and assume, without loss of generality, that $xR^\times \le yR^\times$. Since $1 + y/x \in R$, the element $(1 + y/x)R^\times$ belongs to G_+ and, therefore,

$$v(x+y) = x(1+y/x)R^\times = xR^\times + (1+y/x)R^\times \ge xR^\times = v(x).$$

Hence $v(x + y) \ge \min\{v(x), v(y)\}$ for all $x, y \in \mathrm{qf}(R)$, which is the third defining condition of a valuation map. Thus, v is a valuation map. The last part of statement (b) can be readily deduced from the fact that $G_+ = \{xR^\times : x \in R \setminus \{0\}\}$.

(b) $\Rightarrow$ (a): Suppose that $v\colon \mathrm{qf}(R) \to G \cup \{\infty\}$ is a valuation map satisfying that $R = \{x \in \mathrm{qf}(R) : v(x) \ge 0\}$. Take $x, y \in R$ to be nonzero elements. Then either $v(xy^{-1}) \in G_+$ or $v(yx^{-1}) \in G_+$, which implies that either $xy^{-1} \in R$ or $yx^{-1} \in R$. Hence $y \mid_R x$ or $x \mid_R y$. As a consequence, R is a valuation domain.

For the final statement, one can easily check that $M := \{x \in R : v(x) > 0\}$ is an ideal of R. If a nonzero $u \in R$ has a positive valuation, then $v(u^{-1}) = -v(u) < 0$, and so $u \notin R^\times$. In addition, if $v(u) = 0$, then $v(u^{-1}) = 0$, which means that $u \in R^\times$. Hence $R^\times = R \setminus M$, which means that M is a maximal ideal. □

With notation as in the proof of Theorem 9, the group G is called the *group of divisibility* of the integral domain R.

Primes and Primary Ideals. We proceed to discuss prime and primary ideals in the special setting of valuation domains.

Proposition 10. *In a valuation domain, every proper radical ideal is prime.*

Proof. Let R be a valuation domain, and let I be a proper radical ideal of R. Then $I = \mathrm{Rad}\, I$ is the intersection of all minimal prime ideals over I. Since the ideals of R form a chain, there is only one minimal prime ideal P over I. Hence we find, *a posteriori*, that $I = P$, and so I is prime. □

Proposition 11. *Let R be a valuation domain, and let I be an ideal of R. Then $\bigcap_{n\in\mathbb{N}} I^n$ is a prime ideal of R that contains each prime ideal properly contained in I.*

Proof. Set $J := \bigcap_{n\in\mathbb{N}} I^n$. Take $x, y \in R$ such that $xy \in J$, and then take $n \in \mathbb{N}$ such that $x, y \notin I^n$. Since R is a valuation domain, $I^n \subseteq (x) \cap (y)$. Thus, $I^n(y) \subseteq (xy)$. Moreover, $I^n(y) \ne (xy)$ because $x \notin I^n$. Then $I^{2n} \subseteq I^n(y) \subsetneq (xy)$. This implies that $xy \notin I^{2n}$, and so $xy \in J$. Hence J is prime.

To argue the last statement, suppose that P is a prime ideal properly contained in I. Since P is prime, $I^n \nsubseteq P$ for any $n \in \mathbb{N}$. As R is a valuation domain, $P \subseteq I^n$ for every $n \in \mathbb{N}$, which means that $P \subseteq J$. □

Before discussing the configuration of primary ideals inside a valuation domain, we need the following lemma.

Lemma 12. *Let R be a valuation domain, and let I be a proper ideal of R. If J is an ideal of R such that $I \subsetneq \mathrm{Rad}\, J$, then J contains a power of I.*

Proof. Exercise. ☐

Recall that an ideal I of R is idempotent if $I^2 = I$. We conclude this lecture with the following result about primary ideals of a valuation domain.

Theorem 13. *Let R be a valuation domain, and let P be a prime ideal of R. Then the following statements hold.*

(1) *The product of P-primary ideals is a P-primary ideal.*
(2) *If P is not idempotent, then the P-primary ideals of R are the powers of P.*
(3) *The intersection of all P-primary ideals of R is a prime ideal that contains each prime ideal properly contained in P.*

Proof. (1) Let Q_1 and Q_2 be P-primary ideals of R. Then $\operatorname{Rad}(Q_1Q_2) = (\operatorname{Rad} Q_1) \cap (\operatorname{Rad} Q_2) = P$. To argue that Q_1Q_2 is a primary ideal, take $x, y \in R$ such that $xy \in Q_1Q_2$ but $x \notin \operatorname{Rad}(Q_1Q_2) = P$. We claim that $(x)Q_1 = Q_1$. Since $x \notin Q_1$, the fact that R is a valuation domain implies that $Q_1 \subsetneq (x)$. Set $J := (Q_1 : (x))$. Observe that the inclusion $Q_1 \subseteq (x)$ implies that $J \subseteq ((x) : (x)) = R$, and so J is an ideal of R. Observe, in addition, that $J = x^{-1}Q_1$, that is, $Q_1 = (x)J$. Now the fact that Q_1 is primary with $x \notin P = \operatorname{Rad} Q_1$ ensures that $J \subseteq Q_1$. Therefore $Q_1 = J$, and so $(x)Q_1 = (x)J = Q_1$, as claimed. Then we see that $xy \in Q_1Q_2 = (x)Q_1Q_2$, which implies that $y \in Q_1Q_2$. Hence Q_1Q_2 is primary.

(2) Suppose that P is not idempotent, that is, $P^2 \subsetneq P$. By part (1), the powers of P are P-primary ideals. On the other hand, let Q be a P-primary ideal. Since P^2 is contained in $\operatorname{Rad} Q$, Lemma 12 guarantees that Q contains a power of P^2, and so we can take $n \in \mathbb{N}$ such that $P^n \subseteq Q$ but $P^{n-1} \not\subseteq Q$. Take $x \in P^{n-1}$ such that $x \notin Q$. The inclusion $Q \subsetneq (x)$ holds because R is a valuation domain. Set $J := (Q : (x))$, and observe that J is an ideal of R and $Q = (x)J$ (see previous paragraph). Since Q is P-primary and $x \notin Q$, the inclusion $J \subseteq P$ holds, whence $Q = (x)J \subseteq P^{n-1}P = P^n$. Thus, each P-primary ideal of R is a power of P.

(3) Assume that P is not the only P-primary ideal of R. Let I be the intersection of all P-primary ideals, and let Q be a P-primary ideal different from P. By part (1), the ideal Q^n is P-primary for every $n \in \mathbb{N}$ and, therefore, $I \subseteq \bigcap_{n\in\mathbb{N}} Q^n$. Observe that, by Lemma 12, every P-primary ideal contains a power of Q, and so $I = \bigcap_{n\in\mathbb{N}} Q^n$. It follows now by Proposition 11 that I is a prime ideal of R that contains each prime ideal properly contained in Q. Finally, suppose that P' is a prime ideal of R such that $P' \subsetneq P$. Then for each $n \in \mathbb{N}$, the fact that Q^n is P-primary guarantees that $Q^n \not\subseteq P'$ and, as R is a valuation domain, $P' \subseteq Q^n$. Thus, $P' \subseteq \bigcap_{n\in\mathbb{N}} Q^n = I$. ☐

Exercises

Exercise 1. *Let R be a valuation domain, and let I be a proper ideal of R. If J is an ideal of R such that $I \subsetneq \operatorname{Rad} J$, then $I^n \subseteq J$ for some $n \in \mathbb{N}$.*

Exercise 2. *Let R be a valuation domain, and let P be a nonzero prime ideal of R. Show that if R contains a finitely generated P-primary ideal, then P is the maximal ideal of R.*

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