A note about some equivalent conditions for Dedekind domain

@shiguxiaobei

September 12, 2024

We say an integral domain is a Dedekind domain if it is Noetherian, integrally closed and dimension one. And we can see every ideal of a Dedekind domain R is a (unique) product of prime ideals. Now we proof that the reverse is also true, namely,

Theorem 1.1. *If every ideal of an integral domain R is a product of prime ideals, then R is a Dedekind domain.*

Proof. (Zariski and Samuel)

We now divide the proof into six steps.

(i) If an ideal $\mathfrak{a} \subset R$ is a product of some invertible proper prime ideal, then this is the unique way of $\mathfrak{a}$ to decompose into prime ideals except for the order of the factors.

Let $\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_k = \mathfrak{q}_1 \cdots \mathfrak{q}_n$ where all $\mathfrak{p}_i, \mathfrak{q}_j$ are proper prime ideals and all $\mathfrak{p}_i$ are invertible. Let $\mathfrak{p}_1$ be minimal in all $\mathfrak{p}_i$, which means if some $\mathfrak{p}_i \subset \mathfrak{p}_1$ then $\mathfrak{p}_i = \mathfrak{p}_1$. We assume $\mathfrak{q}_1 \subset \mathfrak{p}_1$ and some $\mathfrak{p}_i \subset \mathfrak{q}_1$, then $\mathfrak{p}_i$ must be $\mathfrak{p}_1$ and $\mathfrak{q}_1 = \mathfrak{p}_1$. Since $\mathfrak{p}_1$ is invertible, $\mathfrak{p}_2 \cdots \mathfrak{p}_k = \mathfrak{q}_2 \cdots \mathfrak{q}_n$, we can repeat the argument to get what we want.

(ii) Every invertible proper prime ideal P of R is maximal.

Suppose that for some $a \notin R \backslash P$ we have $P + (a) \neq R$. Then $P + (a) = P_1 \cdots P_k$ and $P + (a^2) = Q_1 \cdots Q_n$ with P_i, Q_j are all proper prime ideals of R. Let

$$R' = R/P, P_i' = P_i/P, Q_j' = Q_j/P, a' = a + P$$

we have $a'R' = P_1' \cdots P_k', a'^2 R' = Q_1' \cdots Q_n'$. $a' \neq 0$ so each P_i', Q_j' is invertible and we have $(P_i' \cdots P_k')^2 = Q_1' \cdots Q_n'$. By (i), we may so number the Q_j that $Q_{2j-1} = Q_j = P_j$ $(n = 2k)$. Thus $P \subset P + (a^2) = (P + (a))^2 \subset P^2 + (a)$. Take $b \in P$, we have $b = c + da$ for soem $c \in P^2$, which implies $ad \in P, d \in P$. Hence $P \subset P^2 + Pa$, and get $R \subset (P^2 + Pa)P^{-1} = P + (a)$, a contradiction.

(iii) Every nonzero prime ideal of R is invertible.

If $P = R$, then P is invertible. If $P \neq R$, let $0 \neq a \in P$ and write $(a) = P_1 \cdots P_k$ with all P_i are proper prime ideals of$R$. a is invertible so each P_i is invertible and so maximal. Since $P_1 \cdots P_k \subset P$, some $P_i = P$ and P is invertible.

(iv) R is Noetherian and dimension one.

Note that an invertible ideal is finitely generated and the product of invertible ideals is invertible.

(v) For every proper prime ideal P of R, R_P is a valuation ring (VR).

We must show if $\frac{a}{s}, \frac{b}{t} \in R_P$, then $(\frac{a}{s}) \subset (\frac{b}{t})$ or $(\frac{b}{t}) \subset (\frac{a}{s})$. But we can assume $s, t \in R \backslash P$ and it is sufficient to show $aR_P \subset bR_P$ or $bR_P \subset aR_P$. Assume $a \neq 0 \neq b$, note that $(ab)(a, b) \subset$

$(a^2,b^2)(a,b)$ implies $(ab) \subset (a^2,b^2)$, then $ab = xa^2 + yb^2$ for some $x, y \in R$. Thus $(yb)(a,b) \subset (a)(a,b)$ and so $(yb) \subset (a), yb = au, ab = xa^2 + uab$. If $u \notin P$, then $a = \frac{by}{u} \in bR_P$ and if $u \in P$, then $b = \frac{ax}{1-u} \in aR_P$.

(vi) R is integrally closed.

R_P is a VR for all prime ideal $P \subset R$ and thus each is integrally closed. If a is integral on R, then on each R_P and belongs to each R_P. Hence $a \in \bigcap_P R_P = R$.

the last equality is valid for every $R-$ module M, namely $M = \bigcap_{\mathfrak{p}} M_{\mathfrak{p}} = \bigcap_{\mathfrak{m}} M_{\mathfrak{m}}$. $\subset$ is obvious and now take $x \in \bigcap_{\mathfrak{m}} M_{\mathfrak{m}}$, the set $\mathfrak{a} = \{a \in R \mid ax \in M\}$ is a ideal of R and it is not contained in any maximal ideal $\mathfrak{m}$ since $\mathfrak{a} \in \mathfrak{m}$ implies $x \notin M_{\mathfrak{m}}$. Thus $\mathfrak{a} = R$ and $x \in M$.

□

Remark 1.2 (Valuation Ring and DVR)**.**

We say an integral domain V is a valuation ring if A, B are ideals of V, then either $A \subset B$ or $B \subset A$. For an integral domain V, TFAE:

(1) V is a VR ;

(2) If $a, b \in V$ then either $(a) \subset (b)$ or $(b) \subset (a)$;

(3) If $x \in \text{Frac}(V)$ then either $x \in V$ or $x^{-1} \in V$.

By (3), we can get each VR is integrally closed.

Let K be a field and we say a map $v : K\backslash\{0\} \to \mathbb{Z}$ is a discrete valuation on K if it satisfies $v(xy) = v(x) + v(y)$ and $v(x+y) \geq \min\{v(x), v(y)\}$. Denote the valuation ring of v by $A = \{x \in K \mid x = 0 \text{ or } v(x) \geq 0\}$. We call an integeral domain A is a discrete valuation ring (DVR), if there is a discrete valuation v on $\text{Frac}(A)$ whose valuation ring is A .

For an integral domain A, TFAE:

(1) A is a DVR;

(2) A is a PID with a unique nonzero prime ideal.

(3) A is an integrally closed noetherian local ring of dimension one.

(4) A is a regular noetherian local ring of dimension one.

(5) A is a noetherian local ring whose maximal ideal is nonzero and principal.

(6) A is a maximal noetherian ring of dimension one.

"A is maximal" means that there are no intermediate rings strictly between A and its fraction field. See [3, §23] for more details.

From Prop 1.1, we can get more:

Theorem 1.3. *Let R is an integral domain, TFAE:*

(i) R is a Dedekind domain.

(ii) every nonzero ideal of R is invertible.

(iii) the set of nonzero fractional ideals of R: $\mathcal{F}(R)$, is a group with respect to multiplication.

Proof. We only need to show $(iii) \implies (i)$. Let C be the set of all nonzero proper ideals of R which are not products of prime ideals. Suppose $C \neq \emptyset$. R is noetherian for every nonzero ideal of

R is invertible, thus C has a maximal element A . Let $A \subset \mathfrak{m}$ for some maximal ideal of R ,then $A \neq \mathfrak{m}$ and $A \subset A\mathfrak{m}^{-1} \subset R$. If $A \subsetneq A\mathfrak{m}^{-1}$, then $A\mathfrak{m}^{-1}$ a product of prime ideals of R and so as $A = (A\mathfrak{m}^{-1})\mathfrak{m}$. So $A = A\mathfrak{m}^{-1}, \mathfrak{m} = R$, a contradiction. □

Through the unique decomposition property of ideals, we can derive some special properties of Dedekind domain.

Lemma 1.4. *(Finite approximation) Let I be a nonzero fractional ideal in a Dedekind domain R and let $\mathfrak{p}_1, \cdots, \mathfrak{p}_n$ be a finite set of nonzero prime ideals of A. Then I contains an element x_I for which $v_{\mathfrak{p}_i}(x) = v_{\mathfrak{p}_i}(I)$ for all i.*

Proof. We only need to consider the case I is nonzero ideals of R since if we write $I = \frac{J}{s}$ for $s \in R$, then x_I can be taken as x_J/s. Let $\mathfrak{a}_i = \mathfrak{p}_1 \cdots \mathfrak{p}_{i-1}\mathfrak{p}_{i+1}\mathfrak{p}_n$ and choose $a_i \in I$ such that $0 \neq a_i \in \mathfrak{a}_i I$ but $a_i \notin \mathfrak{p}_i I$ (Note that $\mathfrak{a}_i I \cap \mathfrak{p}_i I \subsetneq \mathfrak{a}_i I$ so a_i exists). Thus we have $v_{\mathfrak{p}_i}(a_i) = v_{\mathfrak{p}_i}(I)$ and for $j \neq i$, $v_{\mathfrak{p}_j}(a_i) \geq v_{\mathfrak{p}_j}(\mathfrak{a}_i I) > v_{\mathfrak{p}_j}(I)$. We define $x_I = a_1 + \cdots + a_n$, then $v_{\mathfrak{p}_i}(x_I) = v_{\mathfrak{p}_i}(a_i) = v_{\mathfrak{p}_i}(I)$. □

Proposition 1.5. *Let I be a nonzero ideal in a Dedekind domain R, then every ideal in R/I is principal.*

Proof. Let $\varphi : R \to R/I$ be the quotient map. For each ideal $\widetilde{J} \subset R/I$, let $J = \varphi^{-1}(\widetilde{J})$ so $I \subset J$. By Lemma 1.4 , we can take $x_J \in J$ s.t. $v_{\mathfrak{p}}(x_J) = v_{\mathfrak{p}}(J)$ for every $\mathfrak{p} \mid I$. Then $v_{\mathfrak{q}}((x_J) + I) = \min\{v_{\mathfrak{q}}(x_J), v_{\mathfrak{q}}(I)\} = v_{\mathfrak{q}}(J)$ for every prime ideal $\mathfrak{q} \subset R$. Hence $\widetilde{J} = (\varphi(x_J))$ is principal. □

Proposition 1.6. *For every ideal I in Dedekind domain R there is an ideal J in R such that IJ is principal.*

Proof. Let $0 \neq a \in I = \mathfrak{p}_1^{k_1} \cdots \mathfrak{p}_n^{k_n}$, then $(a) = \mathfrak{p}_1^{l_1} \cdots \mathfrak{p}^{l_n}\mathfrak{q}_1^{m_1} \cdots \mathfrak{q}_s^{m_s}$ with $l_i \geq k_i$. Take $J = \mathfrak{p}_1^{l_1-k_1} \cdots \mathfrak{p}^{l_n-k_n}\mathfrak{q}_1^{m_1} \cdots \mathfrak{q}_s^{m_s}$. □

Most Dedekind domains are not PIDs, so a typical Dedekind domain will contain ideals that require more than one generator. But it turns out that two generators always suffice, and we can even pick one of them arbitrarily.

Proposition 1.7. *For every nonzero ideal I in Dedekind domain R and nonzero $a \in I$ we have $I = (a, b)$ for some $b \in I$.*

Proof. With notation in Prop 1.6, take $x \equiv b_i \mod \mathfrak{p}_i^{k_i+1}$ and $x \equiv c_i \mod \mathfrak{q}_j$ for $b_i \in \mathfrak{p}_i^{k_i} \backslash \mathfrak{p}_i^{k_i+1}$ and $c_j \in R \backslash \mathfrak{q}_j$ by the Chinese Remainder Theorem. Then $v_{\mathfrak{q}}[(a, x)] = \min\{v_{\mathfrak{q}}(a), v_{\mathfrak{q}}(x)\} = v_{\mathfrak{q}}(I)$ for every prime ideal $\mathfrak{q}$,which implies that $I = (a, b)$. □

Remark 1.8 (Dedekind domain, UFD and PID).

We notice that Dedekind domain $\bigcap$ UFD = PID. *Since in UFD irreducible elements are exactly prime elements, and the principal ideals generated by the latter is always nonzero prime ideals, then we can deduce that every prime ideal is principal. Now we can use the ideal decomposition properties in Dedekind domain, or use the fact that in UFD, all prime ideals are principal iff it is a PID.*

Actually,(P.L.Clark) An integral domain whose every prime ideal is principal is a PID[1]. *Simi-*

[1] See https://math.stackexchange.com/questions/168082

lar,(I.S.Cohen) A ring whose every prime ideal is finitely generated is Noetherian[2].

We point out each of Prop 1.5,1.6,1.7 is a sufficient condition for an integral domain to be a Dedekind domain, i.e.

Theorem 1.9. *Let R is an integral domain, TFAE:*

(i) R is a Dedekind domain.

(ii) R/I is PID for every nonzero ideal I.

(iii) For every ideal I there is an ideal J such that IJ is principal.

(iv) For every nonzero ideal I and nonzero $a \in I$ we have $I = (a, b)$ for some $b \in I$.

See [2] for more details.

Remark 1.10 (Prufer domain)**.**

We can also define the "almost Dedekind domain": Prufer domain. An integral domain R is a Prufer domain if each nonzero finitely generated ideal of R is invertible. And for an integral domain R, A, B, C are arbitrary ideals of R, TFAE:

(1) R is a Prufer domain.

(2) Every nonzero ideal of R generated by two elements is invertible.

(3) If $AB = AC$ with A is f.g. and nonzero, then $B = C$.

(4) For every proper prime ideal P of R , R_P is a valuation ring.

(5) $A(B \cap C) = AB \cap AC$.

(6) $(A + B)(A \cap B) = AB$.

(7) $A \cap (B + C) = A \cap B + A \cap C$.

(8) If $A \subset C$ with C f.g., then there is some B s.t. $A = BC$.

(9) $(A + B) : C = A : C + B : C$ if C f.g.

(10) $C : (A \cap B) = C : A + C :$ Bfor all ideals A, B, C of R if A and B f.g.

(11) Every overring of R is flat R-module.

(12) Every overring of R is integrally closed.

If R is an integral domain, any ring T such that $R \subset T \subset \mathrm{Frac}(R)$ is called an overring of R. About these equivalent conditions, See [1, Thm 6.6, Thm 6.10, Thm 6.13] for more details.

We shall give a number of equivalent conditions for a Noetherian integral domain to be a Dedekind domain, which remind us each of them is not ordinary. We can remember them as properties of Dedekind domain.

Theorem 1.11. *If R is a Noetherian integral domain, A, B, C are arbitrary ideals of R , $\mathfrak{m}$ is an arbitrary proper maximal ideal of R, TFAE:*

(1) R is Dedekind domain

(2) Every nonzero ideal of R generated by two elements is invertible.

[2] See https://math.stackexchange.com/questions/2555402

(3) If $AB = AC$ with $A \neq 0$, then $B = C$.

(4) each $R_{\mathfrak{m}}$ is a valuation ring.

(5) $A(B \cap C) = AB \cap AC$.

(6) $(A + B)(A \cap B) = AB$.

(7) $A \cap (B + C) = A \cap B + A \cap C$.

(8) If $A \subset C$, then there is some B s.t. $A = BC$.

(9) $(A + B) : C = A : C + B : C$ if C f.g.

(10) $C : (A \cap B) = C : A + C : B$

(11) there are no ideals of R strictly betwem $\mathfrak{m}$ and $\mathfrak{m}^2$.

(12) every $\mathfrak{m}$-primary ideal of R is a power of $\mathfrak{m}$.

(13) the set of $\mathfrak{m}$-primary ideals of R is totally ordered by inclusion.

(14) Every overring of R is flat R-module.

(15) Every overring of R is integrally closed.

Proof. We point out many of these conditions come from the fact the difference between Dedekind domain and Prufer domain is precisely whether ”Noetherian” or not. See [1, Thm 6.20] for more details. □

References

[1] Larsen, M.D., & McCarthy, P.J. (1973). Multiplicative theory of ideals. American Mathematical Monthly, 80, 94.

[2] https://math.mit.edu/classes/18.785/2015fa/LectureNotes3.pdf

[3] Allen Altman and Steven Kleiman, A term of commutative algebra, Worldwide Center of Mathematics, 2013.