On Dedekind domains and their generalizations (Krull domains)

Haleh Hamdi

Localization.

Definition 1. Let S be a *multiplicatively closed subset* of R, that is, $1_R \in S$ and for $a, b \in S$, $ab \in S$. The *localization of* R *at* S, denoted $S^{-1}R$ or R_S, is the set of equivalence classes of pairs (r, s) with $r \in R$ and $s \in S$ with equivalence relation $(a, s) \sim (a', s')$ if there is an element $t \in S$ such that $t(as' - a's) = 0$.
The equivalence class of (a, s) is denoted by $\frac{a}{s}$. We make $S^{-1}R$ a ring by defining

$$\frac{a}{s} + \frac{b}{t} = \frac{at + bs}{ts} \quad \text{and} \quad (\frac{a}{s}).(\frac{b}{t}) = \frac{ab}{st},$$

for $a, b \in R$ and $s, t \in S$.
For a nonzero ideal I of R,

$$IS^{-1}R = \{\frac{a}{s} \mid a \in I, s \in S\}.$$

Remark 2. Assume that $\alpha = \frac{a}{s} \in IS^{-1}R$. Then a need not to be in I, but $\alpha = \frac{a}{s} = \frac{b}{t}$ for some $b \in I$ and $t \in S$. For instance, let $S = \{3^i \mid i \in \mathbb{N}_0\}$, and consider $I = 6\mathbb{Z}$ of $\mathbb{Z}$. Then $\alpha = \frac{2}{3} = \frac{6}{3^2} \in 6S^{-1}\mathbb{Z}$. However, $2 \notin I$.

Note. Let R be an *integral domain*, and $S = R \setminus \{0\}$. Then $S^{-1}R$ is called the *quotient field* of R.

Proposition 3. *Let R be an integral domain, S a multiplicative closed subset of R, and I a nonzero ideal of R. Then the following statements hold.*

(1) *$IS^{-1}R = S^{-1}R$ if and only if I is a nonzero ideal with $I \cap S \neq \emptyset$.*
(2) *If Q is a primary ideal of R with $Q \cap S = \emptyset$, then $\frac{a}{s} \in QS^{-1}R$ implies $a \in Q$.*
(3) *Let J be an ideal of $S^{-1}R$. Then $J = (J \cap R)S^{-1}R$.*
(4) *The set of prime ideals of $S^{-1}R$ is the set of all $PS^{-1}R$ such that P is a prime ideal of R with $P \cap S = \emptyset$.*
(5) *Let P be a prime ideal of R, and $S = R \setminus P$. Then $S^{-1}R := R_P$ is a local domain with maximal ideal PR_P.*
(6) *For a nonzero ideal I of R, $I = \bigcap_{P \in \mathrm{Max}(R)} IR_P$. In particular, $R = \bigcap_{P \in \mathrm{Max}(R)} R_P$.*

Krull Dimension.

Definition 4. Let R be an integral domain. The *height* of a prime ideal P of R, denoted $\mathrm{ht}(P)$, is defined as

$$\mathrm{ht}(P) = \sup\{n \mid P_0 \subsetneq P_1 \subsetneq P_n = P\}.$$

The height of an ideal I of R is defined as

$$\mathrm{ht}(I) = \min\{\mathrm{ht}(P) \mid I \subseteq P\}.$$

The *Krull-dimension* of R, written $\dim R$, is defined as

$$\dim R = \sup\{\mathrm{ht}(P) \mid P \text{ is a prime ideal of } R\}.$$

For any prime ideal P of R, $\mathrm{ht}(P) = \dim R_P$. An integral domain R is of dimension one if each prime ideal of R is maximal.

Integral Extensions.

Definition 5. The extension $R \subseteq T$ is called an *integral extension* if every $b \in T$ is *integral* over R, that is, b is a root of a *monic* polynomial

$$X^n + a_{n-1}X^{n-1} + \ldots + a_1X + a_0$$

where $a_0, \ldots, a_{n-1} \in R$.
The set of all elements of K which are integral over R is called the *integral closure* of R, denoted by $\bar{R}$. If the integral closure of R is equal to R, then we say that R is *integrally closed*.

Theorem 6. *Let R be an integral domain with integral closure $\bar{R}$. Then*

$$\bar{R} = \bigcup\{(I :_K I) \mid I \text{ is a nonzero finitely generated } R\text{-submodule of } K\}.$$

Theorem 7. *Let $R \subseteq T$ be an integral extension. Then R is a field if and only field T is a field. Hence, Q is a maximal ideal of T if and only if $Q \cap R$ is a maximal ideal of R.*

Theorem 8. *Let R be an integral domain and S a m.c.s. of R. Then $\bar{R}_S = \overline{R_S}$.*

Proof. Let $x \in \bar{R}_S$. Then there exists $a \in \bar{R}$ and $s \in S$ s.t. $x = \frac{a}{s}$. Since $a \in \bar{R}$, $a^n + r_1a^{n-1} + \ldots + r_n = 0$ for some $r_i \in R$. By dividing by s^n, we get

$$\frac{a^n}{s^n} + \frac{r_1}{s}\frac{a^{n-1}}{s^{n-1}} + \ldots + \frac{r_n}{s^n} = 0$$

which implies that $x = \frac{a}{s} \in \overline{R_S}$. For the converse, let $x =\in \overline{R_S}$. Then

$$x^n + \frac{r_1}{s_1}x^{n-1} + \ldots + \frac{r_n}{s_n} = \frac{0}{1}.$$

Set $s := s_1 \cdots s_n$. By multiplying both sides by s^n, we get

$$(sx)^n + r'_1(sx)^{n-1} + \ldots + r'_{n-1}(sx) + r_n = 0$$

for some $r'_i \in R$ which implies that $sx \in \bar{R}$, and hence $x \in \bar{R}_S$. □

Almost Integrity.

Definition 9. The extension $R \subseteq T$ is called an *almost integral extension* if every $b \in T$ is *almost integral* over R, that is, there exists a finitely generated R-submodule F of T such that $b^n \in F$ for each $n \geq 1$.
The set $\tilde{R}$ of all elements of K which are almost integral over R is called the *complete integral closure* of R, and R is called *completely integrally closed* if $\tilde{R} = R$.

Theorem 10. *Let R be an integral domain with complete integral closure $\tilde{R}$. Then*

$$\tilde{R} = \bigcup\{(I :_K I) \mid I \text{ is nonzero } R\text{-submodule of } K\}.$$

Theorem 11. *Let R be an integral domain with complete integral closure $\tilde{R}$. Then*

$$\tilde{R} = \{x \in k \mid \text{there exists a nonzero } r \in R \text{ such that } rx^n \in R \text{ for each positive integer } n\}.$$

Fractional Ideals.

Definition 12. Let R be an integral domain with quotient field K. A subset I of K is said to be a *fractional ideal* of R if I is an R-submodule of K such that $aI \subseteq R$ for some nonzero element a of R.

The set $F(R)$ of all nonzero fractional ideals of R is a multiplicative commutative monoid with identity R which is closed under addition, intersection, multiplication, and ideal quotient.
For $I, J \in F(R)$, the *ideal quotient of I by J* is defined as

$$(I :_K J) := \{x \in K \mid xJ \subseteq I\}.$$

Invertible Ideals.

Definition 13. A fractional ideal I of R is *invertible* if there is a fractional ideal J of R such that $IJ = R$.
Equivalently, $I \in F(R)$ is invertible if and only if $II^{-1} = R$, where $I^{-1} := (R :_K I)$.

Theorem 14. *Let R be an integral domain with quotient field K. For $I_1, \ldots, I_n \in F(R)$, the ideal $I_1 \cdots I_n$ is invertible if and only if each I_i is invertible.*

Proof. It is trivial. $\square$

Theorem 15. *Let R be an integral domain and M an invertible ideal of R. If Q is a prime ideal of R properly contained in M, then $Q \subseteq M^n$ for each $n \in \mathbb{N}_0$.*

Proof. Since $Q \subset M$ and M is invertible, $Q = QMM^{-1}$, and hence $Q = AM$ where $A := QM^{-1} \subseteq R$. Since $Q \subsetneq M$ and Q is a prime ideal, $A \subseteq Q$. Hence, $Q = AM \subseteq QM \subseteq Q$, and so $Q = QM$. Thus, $Q = QM = QMM = QMMM = \ldots$ which implies that $Q \subseteq M^n$ for each $n \in \mathbb{N}_0$. $\square$

Theorem 16. *Every invertible fractional ideal of an integral domain R is finitely generated.*

Proof. Let I be an invertible ideal of R. Then $II^{-1} = R$. Hence, $1 = \sum_{i=1}^{n} a_i b_i$ for some $a_i \in I$ and $b_i \in I^{-1}$. For each $x \in I$, we can write $x = x.1 = x\sum_{i=1}^{n} a_i b_i = \sum_{i=1}^{n} a_i x b_i \subseteq a_1R + \ldots + a_nR$ because $xb_i \in R$. Hence, $I = a_1R + \ldots + a_nR$. $\square$

Theorem 17. *Every invertible ideal of R with finitely many maximal ideals is principal.*

Proof. Assume that I is an invertible ideal of R and $M_1, \ldots, M_n$ are distinct maximal ideals of R. For each $s = 1, \ldots, n$, $\bigcap_{i \neq s} M_i \nsubseteq M_s$. Hence, $I(\bigcap_{i \neq s} M_i) \nsubseteq IM_s$ since I is invertible. Thus, there exists $a_s \in I(\bigcap_{i \neq s} M_i) \setminus IM_s$. Set $a := a_1 + \ldots + a_n$. Then $a \in I$. For each $s = 1, \ldots, n$, $a - a_s = a_1 + \ldots + a_{s-1} \in IM_s$. Thus, $a \in I \setminus \bigcup_{i=1}^{n} IM_i$. Since I is invertible, $aI^{-1} \subseteq R$. It implies that $I^{-1} \subseteq a^{-1}R$. Thus, $I^{-1} = I^{-1}aa^{-1}R$. Put $J := I^{-1}a \subseteq R$. Then $R = II^{-1} = IJa^{-1}$ which implies that $IJ = aR$. Note that $J \nsubseteq M_i$ for each i because if $J \subseteq M_i$ for some i, then $aR = IJ \subseteq IM_i$. Thus, $J = R$, and hence $aR = IJ = I$. $\square$

Theorem 18. *A nonzero ideal I of R is invertible if and only if I is finitely generated and IR_M is principal for each maximal ideal M of R.*

Proof. ($\Rightarrow$) It is clear by Theorems 16 and 17.

($\Leftarrow$) Let $I = (a_1, \dots, a_n)$. Assume on the contrary that I is not invertible, and hence $II^{-1} \subseteq M$ for some maximal ideal M of R. By hypothesis, $IR_M = aR_M$ for some $a \in I$. Then $a^{-1}IR_M \subseteq R_M$, and hence $sa^{-1}I \subseteq R$ for some $s \in R \backslash M$. Thus, $sa^{-1} \in I^{-1}$ which implies that $s = saa^{-1} \in aI^{-1} \in II^{-1} \subseteq M$; a contradiction. Thus, I is invertible. $\square$

Example 19. Let $R = F[X, Y]$ be a polynomial ring over a field F. Then $I = (X, Y)$ is a finitely generated ideal of R which is not invertible.

$\because$ If $f \in qf(R)$ such that $fI \subseteq R$, then $fXR + fYR \subseteq R$. Therefore, $fXR, fYR \subseteq fXR + fYR \subseteq R$ implies that $f \in X^{-1}R \cap Y^{-1}R = R$. Thus, $I^{-1} = R$, and hence $II^{-1} = I \neq R$.

Valuation Domains.

Definition 20. An integral domain R with quotient field K is called a *valuation domain* if for every nonzero $x \in K$, either x or x^{-1} belongs to R.

Theorem 21. *Let R be an integral domain. Then the following statements are equivalent:*

(1) R is a valuation domain.
(2) The fractional ideals of R are linearly ordered under inclusion.
(3) The principal ideals of R are linearly ordered under inclusion.

Proof. (1) $\Rightarrow$ (2) Let R be a valuation domain, and $F_1, F_2 \in F(R)$ such that $F_1 \nsubseteq F_2$. Then there exists $x \in F_1 \setminus F_2$. Let $y \in F_2$. Then $\frac{x}{y} \notin R$ (if so, $x \in yR$ which implies that $x \in F_2$; a contradiction). Since R is a valuation, $\frac{y}{x} \in R$, and hence $y \in xR \subseteq F_1$.

(2) $\Rightarrow$ (3) It is clear.

(3) $\Rightarrow$ (1) Let $x \in K$ such that $x \notin R$. Then $R \subseteq (x)$ by (3). It implies that $1 = xr$ for some $r \in R$, and so $x^{-1} \in R$. $\square$

Corollary 22. *A valuation domain R is* local*, that is, R has a unique maximal ideal. Also, finitely generated ideals of a valuation domain are principal.*

Theorem 23. *Valuation domains are integrally closed.*

Proof. Let $x \notin R$. We show that $x \notin \bar{R}$. Since R is a valuation domain, $R \subset xR$. Hence, $R \subsetneq (x) \subsetneq (x^2) \dots \subsetneq (x^{n-1})$. Thus, $x^n \neq a_0 + a_1x + a_2x^2 + \dots a_{n-1}x^{n-1} \in (x^{n-1})$ for any subset $\{a_0, \dots, a_{n-1}\}$ of R. Therefore, $x \notin \bar{R}$. $\square$

Lemma 24. *Let R be a valuation domain and I a proper nonzero ideal of R. Then $P := \bigcap_{n=1}^{\infty} A^n$ is a prime ideal of R.*

Proof. Let $x, y \in R \setminus P$. We show that $xy \notin P$. Since $x, y \notin P$, there exist positive integers n and m such that $x \notin A^n$ and $y \notin A^m$. Since R is valuation, $A^n \subsetneq xR$ and $A^m \subsetneq yR$. Thus, $yA^n \subsetneq yxR$ and $A^{n+m} \subsetneq A^n yR \subsetneq xyR$, and hence $xy \notin P$. $\square$

Theorem 25. *Let R be a valuation domain. Then R is of dimension one if and only if R is completely integrally closed.*

Proof. Let R be of dimension one, M the maximal ideal of R and $x \in K$ such that $x \notin R$. Then $y := x^{-1} \in R$. Since $P := \bigcap_{n=1}^{\infty} y^n R$ is a prime ideal of R and R is of dimension one, $P = M$ or $P = (0)$. If $P = M$, then $yR = y^2R$, and hence $y = dy^2$

for some $d \in R$ which implies that $dy = 1$. So, $y^{-1} = x \in R$; a contradiction. Hence, $P = (0)$. Therefore, for each nonzero $d \in R$, there exists a positive integer n such that $d \notin y^n R$. Thus, $dx^n \notin R$, and hence $x \notin \tilde{R}$. □

Prüfer Domains.

Definition 26. An integral domain R is called *Prüfer* if every nonzero finitely generated ideal of R is invertible.

Example 27. (1) Any PID is a Prüfer domain, for instance, the polynomial ring $F[X]$ over any field F.
(2) $T = \mathbb{Z} + X\mathbb{Q}[X] = \{f(x) \in K[X] \mid f(0) \in R\}$ is a Prüfer domain.

Theorem 28. *For an integral domain R, the following statements are equivalent:*
(1) R is a Prüfer domain.
(2) R_P is a valuation domain for every prime ideal P of R.
(3) R_M is a valuation domain for every maximal ideal M of R.

Proof. ► (1) ⇒ (2) Let P be a prime ideal of R and $x, y \in R_P$. Then $x = \frac{x_1}{s}$ and $y = \frac{y_1}{t}$ for some $x_i \in R$ and $s, t \in R \setminus P$. By assumption, (x_1, y_1) is invertible. Then $(x_1, y_1)R_P = x_1 R_P$ or $(x_1, y_1) = y_1 R_P$. Let $(x_1, y_1)R_P = x_1 R_P$. Then $yR_P = \frac{y_1}{t} R_P \subseteq (x_1, y_1)R_P = x_1 R_P = xR_P$.
► (2) ⇒ (1) It is clear.
► (3) ⇒ (1) Let I be a finitely generated ideal of R. For every maximal ideal M of R, IR_M is principal, and hence I is invertible. □

Corollary 29. *Prüfer domains are integrally closed.*

Proof. Let R be a Prüfer domain. For each maximal ideal M of R, R_M is a valuation domain, and hence integrally closed. Thus, $R = \bigcap_{M \in \mathrm{Max}(R)} R_M$ is integrally closed. □

Discrete Valuation Rings.

Definition 30. An integral domain V with quotient field K is called a *discrete valuation ring* (DVR) if there exists an onto map $v : K^* \to \mathbb{Z}$ with $K^* = K \setminus \{0\}$ satisfying the following conditions for each $x, y \in K^*$
(1) $v(x + y) \geq \min\{v(x), v(y)\}$,
(2) $v(xy) = v(x) + v(y)$,
(3) $v(1) = 0$,
such that
$$V = \{x \in K^* \mid v(x) \geq 0\},$$
and
$$M = \{x \in K^* \mid v(x) \geq 1\}$$
is the unique maximal ideal of V.

Note that for each $x \in K^*$, $0 = v(1) = v(xx^{-1}) = v(x) + v(x^{-1})$, and hence
$$v(x^{-1}) = -v(x).$$

Example 31. $\mathbb{Z}_{(p)} = \{\frac{a}{b} \mid a, b \in \mathbb{Z}, p \nmid b\}$ for prime number p is a DVR.

Theorem 32. *Let R be a valuation domain. Then the following statements are equivalent:*

(1) *R is a DVR.*
(2) *R is a PID.*
(3) *R is a Noetherian domain.*

Proof. Assume that K is the quotient field of R and M is the maximal ideal of R.
► (1) $\Rightarrow$ (2) Let $v : K^* \to \mathbb{Z}$ be the onto map satisfying the conditions of Definition 30. Since v is sunjective, there exists $t \in K^*$ such that $v(t) = 1$. Then $M = tR$.

$\because$ first $tR \subseteq M$ since M is the unique maximal ideal of R, and second for $a \in M$, we have $v(a) \geq 1 = v(t)$, and hence $v(at^{-1}) = v(a) - v(t) \geq 0$. It implies that $at^{-1} \in R$, and hence $a \in tR$.
Let $x \in M$ with $n := v(x) \geq 1$. Then,

$$v(\frac{x}{t^n}) = v(x) + v(t^{-n}) = v(x) - v(t^n) = n - n(1) = 0.$$

Thus, $xt^{-n} \notin M$, and hence xt^{-n} is unit. Let $x = t^n u$ with u a unit of R.
Now, let I be a nozero ideal of R. Then $\{v(a) \mid 0 \neq a \in I\}$ is a set of non-negative integers, and so has a smallest element, say m. If $m = 0$, then I contains a unit of R, so that $I = R$. If $m \geq 1$, then there exists an $x \in I$ such that $v(x) = m$; then $x = t^m u$ for some unit $u \in R$. Hence, $M^m = t^m R \subseteq I$. For any $x \in I$ with $v(x) = k$, $x = t^k u$ for some unit $u \in R$. Thus, $x = t^k u \in M^k \subseteq M^m$. Therefore, $I = M^m = t^m R$, and hence R is a PID.

► (2) $\Rightarrow$ (3) It is clear.

► (3) $\Rightarrow$ (2) Since in a valuation domain, the fractional ideals of R are linearly ordered under inclusion. Hence, any finitely generated ideal is principal.

► (2) $\Rightarrow$ (1) Since R is a PID, $M = xR$ for some $x \in R$. Set $I = \bigcap_{n=1}^{\infty} x^n R$. Then I is also a principal ideal. Let $I = yR$ for some $y \in R$. If we set $y = xz$, then from $y \in x^n R$, then $z \in x^{n-1} R$, and since this holds for every n we have $z \in I$, hence we can write $z = yu$. Since $y = xz = xyu$, $y(1 - xu) = 0$, and hence $y = 0$ since $x \in M$. Thus, $I = 0$. Therefore, for every nonzero element $a \in R$, there is an integer $n \geq 1$ such that $a \in x^n R$ but $a \notin x^{n+1} R$. Therefore, setting $\nu(a) = n$ and $v(x) = \nu(a) - \nu(b)$ for $x = \frac{a}{b} \in K^*$ gives a surjective map $v : K^* \to \mathbb{Z}$ with desired conditions of Definition 30. □

Corollary 33. *Then the following conditions are equivalent for an integral domain R:*

(1) *R is a DVR.*
(2) *R is a local PID.*
(3) *R is a local Noetherian domain of dimension at most one with principal maximal ideal.*
(4) *R is a one-dimensional integrally closed Noetherian local domain.*

Proof. ► (1) $\Rightarrow$ (2) It follows from Theorem 32.

► (2) $\Rightarrow$ (3) It is clear.

► (3) $\Rightarrow$ (1) Let $M = tR$ for some $t \in R$. By Krull's Intersection Theorem, $\bigcap_{i=1}^{\infty} M^i = (0)$. Let x be a nonzero element of R. Then there exists an integer $n \geq 1$ such that $x \in M^n \setminus M^{n+1}$. Since $x \in M^n$, $x = t^n u$ for some $u \in R$ so that $u \notin M$. By setting $\nu(x) = n$, it is not difficult to see that if $a, b, c, d \in R \setminus \{0\}$ satisfy $\frac{a}{b} = \frac{c}{d}$ then $\nu(a) - \nu(b) = \nu(c) - \nu(d)$. Therefore, setting $v(x) = \nu(a) - \nu(b)$ for $x = \frac{a}{b} \in K^*$ gives a surjective map $v : K^* \to \mathbb{Z}$ with desired conditions of Definition 30.

▶ (1) ⇒ (4) By Theorem 32, R is a PID, and hence $\dim R = 1$. Also, R is integrally closed because it is a valuation domain.

▶ (4) ⇒ (3) Let M be the maximal ideal of R. As R is Noetherian, $M \neq M^2$ by Nakayama's Lemma, and we can choose $t \in M \setminus M^2$. Clearly, $tR \subseteq M$ and we claim that equality holds. Since M is the unique non-zero prime ideal, $\sqrt{tR} = M$. Let n be a minimal positive integer such that $M^n \subseteq tR$. We claim that $n = 1$. Assume for a contradiction that $n \geq 2$, and $M^{n-1} \nsubseteq tR$. Then there exists an element $x \in M^{n-1}$ that is not in tR. Then $xM \subseteq M^n \subseteq tR$. Let $y := \frac{x}{t}$. Then $y \notin R$ since $yt = x \notin tR$. Since $xM \subseteq tR$, $yM \subseteq R$. If $yM = R$, then $ym = 1$ for some $m \in M$, and hence $xm = tym = t \in M^n \subset M^2$ contradicting the choice of t. Thus yM is a proper ideal of R, and hence $yM \subset M$. Since M is finitely generated, $y \in \bar{R} = R$; a contradiction. Therefore, $M^{n-1} \subseteq tR$ which contradicts the choice of n. □

Dedekind Domains.

Definition 34. An integral domain R is called *Dedekind* if each proper ideal of R can be expressed as a finite product of prime ideals of R.

Lemma 35. *If I is an invertible ideal of an integral domain R such that I can be expressed as a finite product of proper prime ideals of R, then this representation is unique.*

Proof. Assume that $I = P_1 \cdots P_n = Q_1 \cdots Q_m$. We establish proof by induction on n. Let $n = 1$. Then $P_1 = Q_1 \cdots Q_m \subseteq Q_i$ for each $i = 1, \ldots, m$. Since P_1 is a prime ideal, there exists Q_i, say Q_1, such that $Q_1 \subseteq P_1$. Hence, $P_1 = Q_1$, and so $P_1 = P_1 Q_2 \cdots Q_m$. Since P_1 is invertible, $R = Q_2 \cdots Q_m$. Hence, $m = 1$.

Now, assume that assertion is true for $n = k-1$, and $I = P_1 \cdots P_k = Q_1 \cdots Q_m$. Choose one of the P_i, say P_1, such that P_1 does not properly contain P_i for $i = 2, \ldots n$. It is clear that there exists Q_i, say Q_1, $Q_1 \subseteq P_1$ and $P_j \subseteq Q_1 \subseteq P_1$ for some j. By the choice of P_1, $P_j = Q_1 = P_1$. Thus, $P_1 \cdots P_k = P_1 Q_2 \cdots Q_m$. Since P_1 is invertible, $P_2 \cdots P_k = Q_2 \cdots Q_m$. By assumption, $k-1 = m-1$, and $Q_i = P_i$. Thus, $k = m$. □

Lemma 36. *Let R be an integral domain with unique maximal ideal M. If $ht(M) = 1$ and M is a principal ideal, then R is a PID.*

Proof. First we show that $\bigcap_{i=1}^{\infty} M^i = (0)$. Let $I := \bigcap_{i=1}^{\infty} M^i$ and $M = xR$ for some $x \in R$. Then $\sqrt{I} = M$ because M is of height one. Also, $M = \sqrt{(x)}$. Then there exists an integer i such that $M^i \subseteq I \subseteq M^{i+1} \subseteq M^i$. . Then $M^{i+1} = M^i$ implies $M^i = 0$ by Nakayama's Lemma. Thus $I = (0)$.

∵ Nakayama's Lemma: Let I be a finitely generated ideal of an integral domain R such that $J(R)I = I$. Then $I = 0$.
Now let J be a nonzero ideal of R. Since $\bigcap_{i=1}^{\infty} M^i = (0)$, there exists $n \in \mathbb{N}$ such that $J \subseteq M^n$ but $J \nsubseteq M^{n+1}$. Take $a \in J \setminus M^{n+1}$, and write $a = ux^n$ for some $u \in R$. Since $a \notin M^{n+1}$, we obtain that $u \notin M$, and hence $u^{-1} \in R$ as R is local. Thus, $x^n = u^{-1}a \in J$. This implies that $J = M^n$ is a principal ideal. □

Theorem 37. *Let R be a Dedekind domain. Then every invertible prime ideal P of R is a maximal ideal.*

Proof. Let $a \in R \setminus P$. We must show that $P + aR = R$ ($P \subset P + aR \subseteq R$). Suppose not, and $P + aR \subset R$. By assumption, $P + aR = P_1 \cdots P_m$ and $P + a^2R = Q_1 \cdots Q_n$ for some prime ideals P_i and Q_i of R. Let $\pi : R \to R/P$ be the canonical epimorphism. Consider the principal ideals of R/P generated by $\pi(a)$ and $\pi(a^2)$. Clearly,

$$(\pi(a)) = \pi(P_1) \cdots \pi(P_m) = (\pi((a) + P))$$

and

$$(\pi(a^2)) = \pi(Q_1) \cdots \pi(Q_n) = (\pi((a^2) + P)).$$

$\because$ If $y \in \pi((a) + P)$, then $y = \pi(x)$ for some $x = ra + z$ where $r \in R$ and $z \in P$. So $y = \pi(x) = x + P = ra + z + P = ra + P = \pi(ra) \subseteq \pi(a)$.
Since $P \subseteq P_i$ and $P \subseteq Q_i$, $\pi(P_i)$ and $\pi(Q_i)$ are prime ideals in R/P. Since principal ideals $(\pi(a))$ and $(\pi(a^2))$ are invertible, each $\pi(P_i)$ and $\pi(Q_i)$ are invertible. Hence,

$$\pi(Q_1) \cdots \pi(Q_n) = (\pi(a^2)) = (\pi(a))^2 = \pi(P_1)^2 \cdots \pi(P_m)^2.$$

By Lemma 35, $n = m$ and $\pi(Q_i) = \pi(P_i)^2$ for each i. It implies that

$$P + a^2R = Q_1 \cdots Q_n = P_1^2 \cdots P_n^2 = (P_1 \cdots P_n)^2 = (P + aR)^2.$$

Therefore,

$$P \subseteq P + a^2R = (P + aR)^2 = P^2 + aP + a^2R \subseteq P^2 + aR.$$

For each $x \in P$, $x = p + ar$ for some $p \in P^2$ and $r \in R$. Thus, $ar = x - p \in P$, and hence $r \in P$. Therefore, $P \subseteq P^2 + aP \subseteq P$, and so $P = P^2 + aP$. Since P is invertible, $R = P + aR$; a contradiction. Thus, P is a maximal ideal of R. □

Theorem 38. *Assume that R is an integral domain with quotient field K. Then the following statements are equivalent:*

(1) R is a Dedekind domain.
(2) Every nonzero prime ideal of R is invertible.
(3) R is a Noetherian Prüfer domain.
(4) R is a one dimensional integrally closed Noetherian domain.
(5) R_M is a Noetherian valuation domain for each maximal ideal M of R and each nonzero element of R is contained in only finitely many maximal ideals of R.
(6) R is a Noetherian domain and R_M is a DVR for each maximal ideal M of R.

Proof. ► (1) ⇒ (2) Let Q be a nonzero prime ideal of R and $x \in Q$ a nonzero element. By assumption, $xR = P_1 \cdots P_n$ for some prime ideals $P_1, \dots, P_n$ of R. Since xR is invertible, each P_i is invertible, and hence each P_i is a maximal ideal of R by Theorem 37. Note that $P_1 \cdots P_n = xR \subseteq Q$ implies that $P_i \subseteq Q$ for some i, and hence $P_i = Q$ and Q is invertible.

► (2) ⇒ (3) Since each prime ideal of R is invertible, each prime ideal is finitely generated, and hence R is a Noetherian domain by Cohen's Theorem. Let M be a maximal ideal of R. Since M is invertible, MR_M is principal by Theorem 18. Hence, R_M is a PID by Lemma 36. Thus, R_M is a DVR by Theorem 33, and hence R is a Prüfer domain by Theorem 28.

► (3) ⇒ (4) We note that each Prüfer domain is integrally closed. Let P be a prime ideal of R and put $Q := PR_P$. Since P is invertible, Q is invertible, and hence principal. Since R_P is Noetherian, by Krull's Principal Ideal Theory, $\mathrm{ht}(P) = \mathrm{ht}(Q) = 1$, and hence $\dim R = 1$.

▶ (3) ⇒ (5) First note that $\dim R = 1$ by (3) ⇒ (4), and hence each prime ideal of R is a maximal ideal. It is clear that R_M is a Noetherian valuation domain for each maximal ideal M of R. Let x be a nonzero element of R. Since R is Noetherian, xR has a primary decomposition, say $xR = Q_1 \cap \ldots \cap Q_n$, where each Q_i is primary. Let $P_i = \sqrt{Q_i}$. Then $x \in Q_i \subseteq P_i$. Let P be a maximal ideal of R containing x. Then $Q_1 \cap \ldots \cap Q_n = xR \subseteq P$, and hence

$$\sqrt{Q_1 \cap \ldots \cap Q_n} = \sqrt{Q_1} \cap \ldots \cap \sqrt{Q_n} = P_1 \cap \ldots \cap P_n \subseteq P.$$

Since $P_1 \cdots P_n \subseteq P_1 \cap \ldots \cap P_n \subseteq P$, $P_i \subseteq P$ for some $i = 1, \ldots, n$. Therefore, $P = P_i$.

▶ (5) ⇒ (3) By Theorem 28, R is a Prüfer domain. Let I be a nonzero ideal of R, $a \in I$, and $P_1, \ldots, P_n$ maximal ideals of R containing a. Let $IR_{P_i} = J_i R_{P_i}$ for some finitely generated subideal J_i of I. Set $J := J_1 + \ldots + J_n + aR$. Then $JR_M = IR_M$ for each maximal ideal M of R. Thus,

$$I = \bigcap_{M \in \mathrm{Max}(R)} IR_M = \bigcap_{M \in \mathrm{Max}(R)} JR_M = J,$$

and hence I is finitely generated.

▶ (3) ⇒ (6) Since R is a Prüfer domain, R_M is a valuation domain for each maximal ideal M of R by Theorem 28. Thus, R_M is a DVR by Theorem 32.

▶ (3) ⇒ (1) Let I be a proper ideal of R. By (3) ⇒ (5), there exist finitely many maximal ideals $M_1, \ldots, M_n$ of R such that $I \subseteq M_i$. Thus,

$$I = \bigcap_{i=1}^{n} (IR_{M_i} \cap R).$$

By (3) ⇒ (6), R_{M_i} is a DVR. For each $i = 1, \ldots, n$, $IR_{M_i} = M_i^{n_i} R_{M_i}$ which implies that

$$I = \bigcap_{i=1}^{n} M_i^{n_i} = \prod_{i=1}^{n} M_i^{n_i}$$

since $M_i^{n_i} R_{M_i} \cap R = M_i^{n_i}$ and $M_i^{n_i}$s are pairwise comaximal.

▶ (6) ⇒ (2) It is clear.

▶ (2) ⇒ (6) We saw it in (2) ⇒ (3).

▶ (4) ⇒ (6) It follows from Theorem 33 because for each maximal ideal M of R, R_M is i.c. local Noetherian domain with $\dim R_M = \mathrm{ht}(M) = 1$.

□

Corollary 39. *In a Dedekind domain R, each nonzero proper ideal I of R is* uniquely *expressible as a finite product of proper prime ideals.*

Injective Modules over Dedekind Domains. Now let's see how Dedekind domains affect injectivity.

Definition 40. Let R be a commutative ring. An R-module E is said to be *injective* if, for any monomorphism $i : A \to B$ of R-modules and any R-homomorphism $f : A \to E$, there exists an R-homomorphism $g : B \to E$ such that $goi = f$.

Theorem 41 (Baer Criterion). *An R-module E is injective if and only if every R-map $f : I \to E$, where I is an ideal in R, can be extended to R.*

Proof. Let $i : A \to B$ be a any monomorphism of R-modules and $f : A \to E$ an R-homomorphism. We should show that there exists an R-homomorphism $g : B \to E$ such that $goi = f$. We are going to use Zorn's Lemma. Let X be the set of all ordered pairs (A', g') where $A \subseteq A' \subseteq B$ and $g' : A' \to E$ such that $g'(x) = f(x)$ for each $x \in A$. Note that $X \neq \emptyset$ because $(A, f) \in X$. Partially order X by defining

$$(A', g') \prec (A'', g'')$$

if and only if $A' \subseteq A''$ and g' extends g''. It is clear that chains in X have upper bounds in X; hence, by Zorn's Lemma, there exists a maximal element (A_0, g_0) in X. If $A_0 = B$, then we are done. So we may assume that there is some $b \in B$ with $b \notin A_0$. Define

$$I := (A_0 :_R b).$$

Define $h : I \to E$ by $h(r) = g_0(rb)$. By hypothesis, there is a map $h^* : R \to E$ extending h. Finally, define $A_1 = A_0 + (b)$ and $g_1 : A_1 \to E$ by

$$g_1(a_0 + rb) = g_0(a_0) + rh^*(1)$$

where $a_0 \in A_0$ and $r \in R$. We show that g_1 is well-defined. Let $a_0 + br = a_0' + br'$ for $a_0, a_0' \in A_0$ and $r, r' \in R$. Then $b(r - r') = a_0' - a_0 \in A_0$ which implies that $r - r' \in I$. Thus,

$$h^*(r - r') = h(r - r') = g_0((r - r')b) = g_0(a_0' - a_0) = g_0(a_0') - g_0(a_0).$$

Therefore,

$$g_0(a_0) + rh^*(1) = g_0(a_0') + r'h^*(1).$$

Clearly, $g_1(a_0) = g_0(a_0)$ for all $a_0 \in A_0$, so that the map g_1 extends g_0. We conclude that $(A_0, g_0) \prec (A_1, g_1)$, contradicting the maximality of (A_0, g_0). Thus, $A_0 = B$, and E is injective. The converse is clear by the definition. $\square$

Theorem 42. *Let R be a commutative ring and M an R-module. Then M is an injective R-module if and only if $Hom_R(-, M)$ is an exact functor.*

Proof. Note that $\mathrm{Hom}_R(-, M)$ is a left exact functor, in general.
$\Rightarrow$ Let M be an injective R-module, and

$$0 \to A \to^i B \to^p C \to 0$$

be an exact sequence of R-modules. Applying $\mathrm{Hom}(-, M)$, we have the following sequence:

$$0 \to \mathrm{Hom}(C, M) \to^{op} \mathrm{Hom}(B, M) \to^{oi} \mathrm{Hom}(A, M).$$

Then for given R-homomorphism $f : A \to M$, there exists an R-homomorphism $g : B \to M$ with $(oi)(g) = goi = f$. Thus, oi is surjective.

$\Leftarrow$ Let $i : A \to B$ be an R-monomorphism, and $f : A \to M$ an R-homomorphism. Since $\mathrm{Hom}_R(-, M)$ is an exact functor, we have the following sequence:

$$0 \to \mathrm{Hom}(C := B/A, M) \to^{op} \mathrm{Hom}(B, M) \to^{oi} \mathrm{Hom}(A, M) \to 0.$$

Since oi is surjective, for given R-homomorphism $f : A \to M$, there exists an R-homomorphism $g : B \to M$ with $(oi)(g) = goi = f$. Thus, M is injective. $\square$

Definition 43. Let R be an integral domain and M an R-module. For $r \in R$ and $m \in M$, we say that m is divisible by r if there is an $m' \in M$ with $m = rm'$. We say that M is a *divisible module* if each $m \in M$ is divisible by every nonzero $r \in R$.

Lemma 44. *Every quotient of a divisible module is divisible.*

Proof. Assume that M is a divisible module, N is a submodule of M and $m+N \in M/N$ where $m \in M$. Let $r \in R$. Then there exists $x \in M$ such that $m = rx \in M$. So,

$$m + N = (rx) + N = r(x + N)$$

for some $x + N \in M/N$. Hence, M/N is divisible R-module. □

Theorem 45. *If R is an integral domain, then every injective R-module is a divisible module.*

Proof. Suppose that M is an injective R-module. Let $m \in M$ and $0 \neq r \in R$. Define the well-defined function $f : Rr \to M$ by $f(tr) = tm$. Note that for every $s, t \in R$:

(1) $f(tr + sr) = f((t + s)r) = (t + s)m = tm + sm = f(tr) + f(sr)$,
(2) $f(t(sr)) = f((ts)r) = (ts)m = t(sm) = tf(sm)$.

So f is an R-homomorphism. Since M is injective, there is an R-homomorphism $g : R \to M$ such that $g(x) = f(x)$ for any $x \in (r)$. Thus,

$$m = 1_R m = f(1_R r) = g(1_R r) = rg(1_R),$$

where $g(1_R) \in M$. Hence, M is divisible. □

Example 46. Let $R = \mathbb{Z}[X]$ be the polynomial ring over $\mathbb{Z}$ with quotient filed $K = \mathbb{Q}(X)$. Set $M = K/R$. Clearly, M is divisible non-injective R-module.

Theorem 47. *If R is a PID, then injectivity and divisibility coincide.*

Proof. Let E be a divisible R-module. We use Baer's Criterion. Assume that $f : I \to E$ is an R-map, where I is a nonzero ideal of R. By hypothesis, $I = Ra$ for some nonzero $a \in I$. Since E is divisible, there is an $e \in E$ with $f(a) = ae$. Define $h : R \to E$ by $h(s) = se$ for all $s \in R$. It is easy to check that h is an R-map. If $s = ra \in I$, then

$$h(s) = h(ra) = rae = rf(a) = f(ra).$$

Therefore, E is injective. □

Theorem 48. *Let R be a commutative ring. Then direct sum of divisible modules is divisible.*

Proof. It is clear. □

Theorem 49. *In a Dedekind domain, an R-module M is injective if and only if it is divisible.*

Proof. ($\Rightarrow$) By Theorem 45, injective R-modules are divisible.

($\Leftarrow$) Suppose that M is divisible. Let $f : I \to M$ be an R-homomorphism, where I is an ideal of R. We show that there exists an R-homomorphism $g : R \to M$ such that $g(x) = f(x)$ for any $x \in I$. Since R is a Dedekind domain, I is invertible. Hence, there exist $a_i \in I$ and $b_i \in I^{-1}$ such that $\Sigma_{i=1}^n a_i b_i = 1$. Since M is divisible, there exists $m_i \in M$ with $f(a_i) = a_i m_i$ for $i = 1, \ldots, n$. Note that for every $a \in I$,

$$a = a.1 = \Sigma_{i=1}^n a a_i b_i,$$

and hence

$$f(a) = f(\Sigma_{i=1}^n a a_i b_i) = \Sigma_{i=1}^n a b_i f(a_i) = a\Sigma_{i=1}^n b_i a_i m_i.$$

Define $m := \Sigma_{i=1}^{n} b_i a_i m_i$. Then $m \in M$ and $f(a) = am$ for every $a \in I$. Now, we can define $g : R \to M$ by $g(r) = rm$. Then for every $a \in I$,

$$g(a) = am = f(a).$$

□

Definition 50. Let R be a commutative ring.

(1) An R-module F is said to be *free* if F is isomorphic to a direct sum of copies of R. That is, there is a (possibly infinite) index set B with $F = \oplus_{b\in B} R_b$, where $R_b =< b >\cong R$ for all $b \in B$. We call B a basis of F.

(2) An R-module P is said to be *projective* if, for any R-epimorphism $\pi : A \to B$ of R-modules and any R-homomorphism $f : P \to B$, there exists an R-homomorphism $g : P \to A$ such that $\pi o g = f$.

Theorem 51. *Let R be a commutative ring and M an R-module.*

(1) Every free module is projective.

(2) M is the quotient of a free module.

(3) If M is a direct summand of a free module, then M is projective.

Proof. ► (1) Let F be a free R-module with basis $B = \{x_i \mid i \in I\}$. If $\pi : M \to N$ is an R-epimorphism and $f : F \to N$ is an R-homomorphism, then for each $f(x_i) \in N$, there exists $y_i \in M$ so that $\pi(y_i) = f(x_i)$ for all $i \in I$. Let $g : F \to M$ be an R-homomorphism defined by $g(x_i) = y_i$. Then $\pi o g = f$. Hence, F is projective.

►(2) First we show that if F is a free R-module with basis X and $f : X \to M$ is an R-hompmorphism, then there exists an R-homomorphism $g : F \to M$ such that $g(x) = f(x)$ for any $x \in X$. Let $u \in F$. Then $u = \Sigma_{i=1}^{n} r_i x_i$ such that $r_i \in R$ and $x_i \in X$. Define $g : F \to M$ by

$$g(u) = g(\Sigma_{i=1}^{n} r_i x_i) = \Sigma_{i=1}^{n} r_i f(x_i).$$

It is clear that g is well-defined because x_i are linearly independent, and $g(x) = f(x)$ for any $x \in X$.

Now, choose a generating set X of M, that is, $M = RX$, (note that such X exists, for example, $X = M$). Let $F = \oplus_{x\in X} R$ is free R-module the basis $Y = \{e_x\}_{x\in X}$ where $e_x = (0, 0, \ldots, 1, 0, \ldots 0)$. Let $f : Y \to M$ with $f(e_x) = x$. Then there is an R-map $g : F \to M$ with $g(e_x) = f(e_x) = x$ for all $x \in Y$. Since g is a surjuective, $F/\operatorname{Ker}(g) \cong M$.

►(3) Let $\pi : B \to C$ be an R-epimorphism f R-modules and $f : M \to C$ an R-homomorphism of R-modules. Suppose that M is a direct summand of a free module F, so there are maps $q : F \to M$ and $j : M \to F$ with $qj = 1_M$. The composite foq is a map $F \to C$; since F is free, it is projective, and so there is a map $h : F \to B$ with $poh = foq$. Define $g : M \to B$ by $g = hj$. Then for each $x \in M$,

$$pog(x) = pohoj(x) = foqoj(x) = fo1_M(x) = f(x).$$

□

Theorem 52. *Let R be an integral domain with quotient field K and I an ideal of R. Then I is invertible if and only if I is projective.*

Proof. Let I be an invertible ideal of R. Then $1 = \Sigma_{i=1}^{n} a_i b_i$ for some $a_i \in I$ and $b_i \in I^{-1}$. Define

$$\phi_i : I \to R$$

by $\phi_i(a) = b_i a$. If $a \in I$, then

$$a = \Sigma_{i=1}^n a a_i b_i = \Sigma_{i=1}^n a_i \phi_i(a).$$

There exists a free R-module F with basis $\{e_i\}_{i\in\Lambda}$ such that R-homomorphism

$$\psi : F \to I$$

by $\psi(e_i) = a_i$ is surjective. Define

$$\phi : I \to F$$

by

$$\phi(x) = \Sigma_{i=1}^n \phi_i(x) e_i.$$

Then $\psi o \phi(x) = x$ for each $x \in I$. Thus, the exact sequence

$$0 \to \mathrm{Ker}(\psi) \to F \to I \to 0$$

splits, and hence $F \cong I \oplus \mathrm{Ker}(\psi)$. Therefore, I is projective.

For the converse, let I be projective. There is a free module F such that

$$\psi : F \to I$$

is surjective. Since I is projective, there exists

$$\phi : I \to F$$

such that $\psi o \phi(x) = x$ for any $x \in I$. Let $\{e_i\}_{i\in\Lambda}$ be a basis for F and define

$$a_i = \psi(e_i).$$

If $x \in I$, then $\phi(x) \in F$, and hence $\phi(x) = \Sigma r_i e_i$ for some $r_i \in R$ and almost all $r_i = 0$. Define

$$\phi_i : I \to R$$

by $\phi_i(x) = r_i$. Note that $\phi_i(x) = 0$ for almost all i. Thus, for $x \in I$,

$$x = \psi o \phi(x) = \psi(\Sigma r_i e_i) = \Sigma r_i \psi(e_i) = \Sigma \phi_i(x) a_i.$$

Hence, I is generated by $\{a_i\}_i$. Now, let $0 \neq b \in I$, and define $q_{i(b)} \in K$ by

$$q_{i(b)} = \frac{\phi_i(b)}{b}.$$

Note that $q_{i(b)} I \subseteq R$.

$\because$ If $a \in I$, then

$$a q_{i(a)} = a \frac{\phi_i(a)}{a} = \phi_i(a) \in R.$$

Also, for each $b \in I$, we have

$$b = \Sigma \phi_i(b) a_i = \Sigma q_{i(b)} b a_i = b \Sigma q_{i(b)} a_i.$$

By canceling b, $1 = \Sigma q_{i(b)} a_i \subseteq II^{-1}$, and hence I is invertible. $\square$

Corollary 53. *In a Dedekind domain, all ideals are projective modules.*

Theorem 54. *Every R-module M can be imbedded as a submodule of an injective R-module.*

Proof. First, we show that every $\mathbb{Z}$-module can be embedded in a divisible $\mathbb{Z}$-module. Let G be a $\mathbb{Z}$-module. Then there exists a free $\mathbb{Z}$-module $F = \oplus_i \mathbb{Z}$ such that $f : F \to G$ is a $\mathbb{Z}$-surjective. Hence, $G \cong F/K$ for some submodule K of F. Now,

$$G \cong F/K = (\oplus\mathbb{Z})/K \subseteq (\oplus\mathbb{Q})/K.$$

We know that Q is a divisible $\mathbb{Z}$-module.

$\because$ Let $i : n\mathbb{Z} \to Z$ be a $\mathbb{Z}$-monomorphism, and $f : n\mathbb{Z} \to Q$ a $\mathbb{Z}$-homomorphism. Let $x \in n\mathbb{Z}$. Then $x = na$ for some $a \in \mathbb{Z}$. Put $c := \frac{f(na)}{na}$, and define $g : \mathbb{Z} \to Q$ by $g(a) = ac$. It is clear that g is well-defined and for $na \in n\mathbb{Z}$,

$$goi(na) = g(na) = nac = na.\frac{f(na)}{na} = f(na).$$

It implies that $\oplus\mathbb{Q}$ is a divisible $\mathbb{Z}$-module, and hence $(\oplus\mathbb{Q})/K$ is divisible $\mathbb{Z}$-module. Since $\mathbb{Z}$ is a PID, $(\oplus\mathbb{Q})/K$ is injective $\mathbb{Z}$-module.

Next, we show that if M is an injective $\mathbb{Z}$-module, then $\mathrm{Hom}_{\mathbb{Z}}(R, M)$ is an injective R-module. We note that $\mathrm{Hom}_{\mathbb{Z}}(R, M)$ is an R-module and

$$\mathrm{Hom}_R(-, \mathrm{Hom}_{\mathbb{Z}}(R, M)) \cong_{\mathbb{Z}} \mathrm{Hom}_{\mathbb{Z}}(- \otimes_R R, M) \cong_{\mathbb{Z}} \mathrm{Hom}_{\mathbb{Z}}(-, M).$$

Since M is an injective $\mathbb{Z}$-module, $\mathrm{Hom}_R(-, \mathrm{Hom}_{\mathbb{Z}}(R, M))$ is exact functor. It implies that $\mathrm{Hom}_{\mathbb{Z}}(R, M))$ is an injective R-module. Finally, we are ready to prove the theorem. Let M be an R-module. Then M is a $\mathbb{Z}$-module. Hence, M can be embedded in an injective $\mathbb{Z}$-module, say E. Let $f : M \to E$ be the monomorphism. Note that for each $x \in M$, the map

$$\phi_x : R \to M$$

defined by $\phi_x(r) = rx$ is a $\mathbb{Z}$-homomorphism. Consider

$$\phi : M \to \mathrm{Hom}_{\mathbb{Z}}(R, E)$$

defined by $\phi(x) = f\phi_x$. It is easy to show that ϕ is an R-monomorphism. Hence, M can be embedded in an injective R-module.

$\because [0 = 0(1_R) = \phi(m)(1_R) = f(1_R m) = f(m)] \Rightarrow m = 0.$ □

Lemma 55. *An R-module P is projective if and only if for every R-epimorphism $g : Q \to D$, where Q is injective, and for every R-homomorphism $f : P \to D$, there exists an R-homomorphism $h : P \to Q$ such that $gh = f$.*

Proof. If P is a projective R-module, then we are done by the definition. Conversely, let $g : A \to B$ be an R-epimorphism, and let $f : P \to B$ be an R-homomorphism. Note that A can be embedded in an injective R-module Q, so $\sigma : A \to Q$ and $\iota : \mathrm{Ker}(g) \to A$ are R-monomorphisms and $\pi : Q \to Q/\operatorname{Im}(\sigma\iota)$ is an R-epimorphism. We will find an R-monomorphism $\psi : B \to Q/\operatorname{Im}(\sigma\iota)$.

Note that for every $b \in B$, there exists $a \in A$ such that $g(a) = b$ since g is an R-epimorphism. Define $\psi : B \to Q/\operatorname{Im}(\sigma\iota)$ by

$$\psi(b) = \sigma(a) + \operatorname{Im}(\sigma\iota).$$

Note that ψ is well-defined because $\psi(0) = \sigma(x) + \operatorname{Im}(\sigma\iota)$ for some $x \in \mathrm{Ker}(g)$, meaning that $\iota(x) = x$ and

$$\psi(0) = \sigma\iota(x) + \operatorname{Im}(\sigma\iota) = 0 + \operatorname{Im}(\sigma\iota) = \operatorname{Im}(\sigma\iota).$$

We will now show that ψ is an R-homomorphism. Firstly, consider $b \in B$ and $r \in R$, so

$$r\psi(b) = r(\sigma(a) + \mathrm{Im}(\sigma\iota)) = r\sigma(a) + \mathrm{Im}(\sigma\iota) = \sigma(ra) + \mathrm{Im}(\sigma\iota)$$

for some $a \in A$ such that $g(a) = b$. Since $g(ra) = rg(a) = rb$,

$$\psi(rb) = \sigma(ra) + \mathrm{Im}(\sigma\iota).$$

Thus, $r\psi(b) = \psi(rb)$.

Secondly, consider $b_1, b_2 \in B$, so

$$\psi(b_1)+\psi(b_2) = (\sigma(a_1)+\mathrm{Im}(\sigma\iota))+(\sigma(a_2)+\mathrm{Im}(\sigma\iota)) = (\sigma(a_1)+\sigma(a_2))+\mathrm{Im}(\sigma\iota) = \sigma(a_1+a_2)+\mathrm{Im}(\sigma\iota)$$

for some $a_1, a_2 \in A$ such that $g(a_1) = b_1$ and $g(a_2) = b_2$. Since $g(a_1 + a_2) = g(a_1) + g(a_2) = b_1 + b_2$,

$$\psi(b_1 + b_2) = \sigma(a_1 + a_2) + \mathrm{Im}(\sigma\iota).$$

Thus,

$$\psi(b_1) + \psi(b_2) = \psi(b_1 + b_2).$$

Therefore, ψ is an R-homomorphism.

To show that ψ is one-to-one, let $x \in \mathrm{Ker}(\psi)$, so

$$0 = \psi(x) = \sigma(a) + \mathrm{Im}(\sigma\iota)$$

for some $a \in A$ such that $g(a) = x$. Then $\sigma(a) \in \mathrm{Im}(\sigma\iota)$ which implies that there exists $z \in \mathrm{Ker}(g)$ such that $\sigma\iota(z) = \sigma(z) = \sigma(a)$. Since σ is an R-monomorphism, $z = a$, so $x = g(a) = g(z) = 0$. Thus, ψ is an R-monomorphism.

Also, note that

$$\psi g(a) = \sigma(a) + \mathrm{Im}(\sigma\iota) = \pi\sigma(a).$$

By assumption, there exsits an R-homomorphism $\theta : P \to Q$ such that $\pi\theta = \psi f$. We will show that $\mathrm{Im}(\theta) \subseteq \mathrm{Im}(\sigma)$. Let $x \in P$, so

$$\theta(x) + \mathrm{Im}(\sigma\iota) = \pi\theta(x) = \psi f(x) = \sigma(a) + \mathrm{Im}(\sigma\iota)$$

for some $a \in A$ such that $g(a) = f(x)$. Then $\theta(x) - \sigma(a) \in \mathrm{Im}(\sigma\iota)$, implying that there exists $z \in \mathrm{Ker}(g)$ such that $\sigma\iota(z) = \theta(x) - \sigma(a)$. Thus,

$$\theta(x) = \sigma\iota(z) + \sigma(a) = \sigma(z) + \sigma(a) = \sigma(z + a).$$

So, for every $x \in P$, $\theta(x) \in \mathrm{Im}(\sigma)$, meaning that $\mathrm{Im}(\theta) \subseteq \mathrm{Im}(\sigma)$.

Observe that for every $x \in P$, there exists $a \in A$ such that $\theta(x) = \sigma(a)$. Hence, define

$$\gamma : P \to A$$

by

$$\gamma(x) = a.$$

Note that γ is well-defined because there exists $z \in A$ such that $\sigma(z) = \theta(0) = 0$. Since σ is an R-monomorphism, $z = 0$ and $\gamma(0) = 0$. We will now show that γ is an R-homomorphism.

Firstly, consider $x \in P$ and $r \in R$, so $r\gamma(x) = ra$ for some $a \in A$ such that $\sigma(a) = \theta(x)$. Since $\theta(rx) = r\theta(x) = r\sigma(a) = \sigma(ra)$, $\gamma(rx) = ra$. Thus, for every $x \in P$,

$$r\gamma(x) = \gamma(rx).$$

Secondly, consider $x_1, x_2 \in P$, so $\gamma(x_1) + \gamma(x_2) = a_1 + a_2$ for some $a_1, a_2 \in A$ such that $\sigma(a_1) = \theta(x_1)$ and $\sigma(a_2) = \theta(x_2)$. Since

$$\theta(x_1 + x_2) = \theta(x_1) + \theta(x_2) = \sigma(a_1) + \sigma(a_2) = \sigma(a_1 + a_2),$$

we have $\gamma(x_1 + x_2) = a_1 + a_2$. Thus,

$$\gamma(x_1) + \gamma(x_2) = \gamma(x_1 + x_2)$$

for every $x_1, x_2 \in P$. Therefore, γ is an R-homomorphism.

Lastly, we will show that $f = g\gamma$. For every $x \in P$, notice that

$$\psi f(x) = \pi\theta(x) = \pi\sigma(a) = \psi g(a)$$

for some $a \in A$ such that $\sigma(a) = \theta(x)$. Since $g\gamma(x) = g(a)$, $\psi f(x) = \psi g\gamma(x)$, which means that $f = g\gamma$ because ψ is an R-monomorphism. □

Theorem 56. *The following statements are equivalent for an integral domain R.*

(1) R is a Dedekind domain.
(2) Every quotient of an injective module is injective.
(3) Every submodule of a projective module is projective.

Proof. ▶ (1) ⇒ (2) Assume that N is a submodule of an injective R-module M. Then M is divisible, so M/N is divisible. Thus, M/N is injective R-module.

▶ (2) ⇒ (3) Let A be a submodule of a projective R-module P. Consider an R-epimorphism $g : Q \to B$, where Q is injective, and an R-homomorphism $f : A \to B$. Let $\iota : A \to P$ be the inclusion mapping. Consider the exact sequence

$$0 \to \operatorname{Ker}(g) \to Q \to^{g} B \to 0.$$

Then $B \cong Q/\operatorname{Ker}(g)$ is injective by (2). Thus, there exists an R-homomorphism $h : P \to B$ such that $h\iota = f$. Hence, there exists an R-homomorphism $\eta : P \to Q$ such that $g\eta = h$. Thus, $\eta\iota : A \to Q$ is an R-homomorphism such that $g\eta\iota = h\iota = f$. Hence, A is projective by Lemma.

▶ (3) ⇒ (1) Let I be a nonzero ideal of R. Since R is a free R-module, and so it is projective. Therefore, its submodules are projective. Thus, I is projective. Since R is an integral domain, I is invertible. Thus, R is a Dedekind domain. □

Corollary 57. *Let R be an integral domain such that every divisible R-module is injective. Then R is a Dedekind domain.*

Proof. Let M be an injective module and N a submodule of M. Then M/N is a divisible R-module, and hence an injective R-module by assumption. Thus, R is a Dedekind domain by Theorem. □

The v- and t-operations.

Definition 58. For a fractional ideal I of R, set $I^{-1} := (R :_K I)$. The *v-closure* of I is defined as

$$I_v := (I^{-1})^{-1}.$$

Clearly, $I \subseteq I_v \subseteq R$ for any ideal I of R. If $I = I_v$, then I is called *divisorial*.

Lemma 59. *Let R be an integral domain and I a nonzero ideal of R. Then I_v is the intersection of principal fractional ideals of R containing I.*

Proof. Let $\{(x_\lambda)\}_{\lambda\in\Lambda}$ be the family of principal fractional ideals of R containing I. Since $I \subseteq (x_\lambda)$ for each $\lambda \in \Lambda$, $x_\lambda^{-1} I \subseteq R$, and hence $x_\lambda^{-1} \in I^{-1}$. For each $y \in I_v$, $yI^{-1} \subseteq R$. Hence, $yx_\lambda^{-1} \in R$ which implies that $y \in (x_\lambda)$, and hence $I_v \subseteq \bigcap_{\lambda\in\Lambda}(x_\lambda)$.
For the reverse containment, let $y \in \bigcap_{I\subseteq(x_\lambda)}(x_\lambda)$ such that $y \notin I_v$. Then $yI^{-1} \nsubseteq R$, and hence $yt \notin R$ for some $t \in I^{-1}$. Thus, $y \notin (t^{-1})$. Note that $t \in I^{-1}$ implies that $tI \subseteq R$ so that $I \subseteq (t^{-1})$. Thus, $y \in (t^{-1})$; a contradiction. □

Theorem 60. *Let R be an integral domain, I and J nonzero fractional ideals of R. Then the following hold:*

(1) $R_v = R$ and $(xI)_v = xI_v$.
(2) $I \subseteq I_v$; $I \subseteq J$ implies $I_v \subseteq J_v$.
(3) $(I_v)_v = I_v$.
(4) $(I + J)_v = (I_v + J_v)_v$, $I_v \cap J_v = (I_v \cap J_v)_v$ and $(IJ)_v = (I_vJ)_v = (I_vJ_v)_v$.
(5) $(I_v :_K J_v) = (I_v :_K J) = (I_v :_K J)_v$.

Lemma 61. *Let R be an integral domain. For each ideal I of R there exists a finitely generated subideal J of I such that $I_v = J_v$ if and only if the ascending chain condition holds on divisorial ideals of R.*

Proof. ($\Rightarrow$) Let $I_1 \subseteq I_2 \subseteq \dots$ be an ascending chain of proper divisorial ideals of R and $I := \bigcup_\alpha I_\alpha$. Then there exists a finitely generated subideal J of I such that $I_v = J_v$ by assumption. Let $J = (x_1, \dots, x_t)$. For each $i = 1, \dots, t$, $x_i \in I_{\alpha_i}$ for some α_i. Let $\alpha = \mathrm{Max}\{\alpha_1, \dots, \alpha_n\}$. Then $x_1, \dots, x_t \in I_\alpha$. It is clear that for each $i \geq \alpha$, $I_\alpha \subseteq I_i$. Since $J \subseteq I_\alpha$, $I_i \subseteq I_v = J_v \subseteq I_\alpha$. Hence, $I_\alpha = I_i$ for each $i \geq \alpha$.

($\Leftarrow$) Let I be an ideal of R, and

$$\sum := \{H_v \mid H \text{ is finitely generated, } H \subseteq I\}.$$

By the acc on divisorial ideals, $\sum$ has a maximal element; say J_v. We show that $J_v = I_v$. Clearly, $J_v \subseteq I_v$. Let $I_v \nsubseteq J_v$. Then $I \nsubseteq J$. Pick $x \in I \setminus J$ and consider the ideal $F := J + xR$. Then $F_v \in \sum$ and $J_v \subsetneq F_v = (J + xR)_v$; a contradiction. Hence, $I_v = J_v$. □

Theorem 62. *Let R be an integral domain with quotient field K, and P a prime ideal of R. Then the following statements hold:*

(1) $R_P = \{x \in K \mid x^{-1}R \cap R \nsubseteq P\} \cup \{0\}$.
(2) If R_P is not a valuation domain, then there exists a nonzero $x \in K$ such that

$$(xR \cap R) + (x^{-1}R \cap R) \subseteq P.$$

(3) If $P^{-1} \nsubseteq \tilde{R}$, then R_P is a DVR.
(4) If R is completely integrally closed and P is a divisorial ideal, then R_P is a DVR.

Proof. (1) ($\subseteq$) Let $x \in R_P$ be a nonzero element. Then there exists $s \in R \setminus P$ such that $sx \in R$. Hence, $s \in x^{-1}R \cap R$ such that $s \notin P$.
($\supseteq$) Let $x \in K$ be a nonzero element such that $x^{-1}R \cap R \nsubseteq P$. Then there exists $y \in x^{-1}R \cap R$ such that $y \notin P$. Thus, $y = x^{-1}r$ for some $r \in R$, and hence $x = \frac{r}{y} \in R_P$.

(2) Since R_P is not a valuation domain, there exists a nonzero $x \in K$ such that neither x nor x^{-1} is in R_P. Therefore, (1) implies that $(xR\cap R)+(x^{-1}R\cap R) \subseteq P$.

(3) If R_P is not a valuation domain, then $P^{-1} \subseteq (I :_K I)$ for some fractional ideal I of R.

$\because P^{-1} \subseteq (R : xR \cap R + x^{-1}R \cap R) = (R : (xR \cap R)) \cap (R : (x^{-1}R \cap R))$. Note that $x(x^{-1}R \cap R) = xR \cap R$. Therefore,

$$(R : (xR \cap R)) \cap (R : (x^{-1}R \cap R)) = ((xR \cap R) : (xR \cap R)).$$

It implies that $P^{-1} \subseteq \tilde{R}$; a contradiction. Hence, R_P is a valuation domain. Let $a \in P^{-1} \setminus \tilde{R}$. Then $a \notin (P : P)$ and $aPR_P \subseteq R_P$. If $aPR_P \subseteq PR_P$, then $aP \subseteq R \cap PR_P = P$, and hence $a \in (P : P)$; a contradiction. Thus, $aPR_P = R_P$, an hence $PR_P = a^{-1}R_P$ is principal.

Now we show that P is of height one. Let Q be a nonzero prime ideal of R such that $Q \subsetneq P$ and let $x \in P \setminus Q$. Then $x(R : P) \subseteq R$ and $xQ(R : P) \subseteq Q$; whence $Q(R : P) \subseteq Q$ and $(R : P) \subseteq (Q : Q) \subseteq \tilde{R}$; a contradiction. Thus, $\mathrm{ht}(P) = 1$. Lemma 36 implies that R_P is a PID and hence a DVR.

(4) If P is a divisorial ideal, then $P^{-1} \nsubseteq R = \tilde{R}$. Hence, R_P is a valuation domain by (3). It follows that P has height one. □

The *t-closure* of I is defined as

$$I_t := \bigcup J_v$$

where J ranges over the set of finitely generated subideals of I.
Clearly, $I \subseteq I_t \subseteq I_v \subseteq R$ for any ideal of R. For a *finitely generated* ideal I of R, $I_t = I_v$. If $I = I_t$, then I is called a *t-ideal.* A fractional ideal I of R is said to be *t-invertible* if $(II^{-1})_t = R$. The maximal element of the set of all t-ideals of R is called a *maximal t-ideal* of R. The set of maximal t-ideals of R is written by $\mathrm{Max}^t(R)$.

Theorem 63. *Let R be an integral domain, I and J nonzero fractional ideals of R. Then the following hold:*

1. *$R_t = R$ and $(xI)_t = xI_t$.*
2. *$I \subseteq I_t$ and $I \subseteq J$ implies $I_t \subseteq J_t$.*
3. *$(I_t)_t = I_t$.*
4. *$(I + J)_t = (I_t + J_t)_t$, $I_t \cap J_t = (I_t \cap J_t)_t$, and $(IJ)_t = (I_tJ_t)_t = (I_tJ)_t$.*
5. *$(I_t :_K J_t) = (I_t :_K J) = (I_t :_K J)_t$.*

Theorem 64. *Let R be an integral domain.*

1. *$\mathrm{Max}^t(R)$ is nonempty.*
2. *Each maximal t-ideal of R is a prime ideal.*
3. *For each nonzero ideal I of R, $I_t = \bigcap_{P \in \mathrm{Max}^t(R)} I_tR_P$. In particular,*

$$R = \bigcap_{P \in \mathrm{Max}^t(R)} R_P.$$

4. *For each nonzero divisorial I of R, if $P \in \mathrm{Min}(I)$, then P is a t-ideal.*

Proof. ► (1) Assume that $\sum$ is the set of all nonzero t-ideals of R. Let I be the union of an ascending chain I_α such that $I_\alpha \in \sum$. Let $x \in I_t$. Then there exists a finitely generated ideal $(x_1, \ldots, x_n) \subseteq I$ such that $x \in (x_1, \ldots, x_n)_v$. Since $(x_1, \ldots, x_n) \subseteq I$, there exists an α such that $(x_1, \ldots, x_n) \subseteq I_\alpha$, and hence $x \in (x_1, \ldots, x_n)_t \subseteq I_\alpha \subseteq I$. Thus, $I \in \sum$. Hence, by Zorn's lemma $\sum$ has a maximal element, recall that Zorn's lemma states that a partially ordered set containing an upper bound for every chain (that is, every totally ordered subset) necessarily contains at least one maximal element.

▶ (2) Let M be a maximal t-ideal of R, $x, y \in R$ with $xy \in M$ and $x \notin M$. Then $M \subsetneq (M + xR) \subseteq R$. It implies that $M \subset (M + xR)_t \subseteq R$. Since M is a maximal ideal $(M + xR)_t = R$. Thus,

$$yR = y(M + xR)_t \subseteq (y(M + xR)_t)_t = (yM + yxR)_t \subseteq M.$$

Hence, $y \in M$.

▶ (3) It is enough to show that for a t-ideal I of R, $\bigcap_{P \in \mathrm{Max}^t(R)} I_P \subseteq I$. Let $x \in \bigcap_{P \in \mathrm{Max}^t(R)} I_P$. For any $P \in \mathrm{Max}^t(R)$, $x = \frac{a(P)}{b(P)}$ for some $a(P) \in I$ and $b(P) \in R \setminus P$. Then $b(P) \in (I :_R xR)$, and hence $(I : xR) \nsubseteq P$ for all $P \in \mathrm{Max}^t(R)$. Since $(I :_R xR)$ is a t-ideal, $(I :_R xR) = R$ which implies that $x \in I$.

▶ (4) Let $x \in P_t$. Then there exists a finitely generated subideal J of P such that $x \in J_v$. Since $P \in \mathrm{Min}(I)$, $PR_P \in \mathrm{Min}(IR_P)$, and hence $\sqrt{IR_P} = PR_P$. Thus, $J^n R_P \subseteq P^n R_P \subseteq IR_P$ for some integer $n \geq 1$. Hence, there exists $s \in R \setminus P$ such that $sJ^n \subseteq I$. Thus,

$$s(J_v)^n \subseteq (s(J_v)^n)_v = (sJ^n)_v \subseteq I_v = I \subseteq P.$$

Since $s \notin P$, $J_v \subseteq P$, and hence $x \in P$. □

Remark 65. Let R be an integral domain. Then $\mathrm{Max}^v(R)$ need not to be nonempty. For instance, if R is a valuation domain with maximal ideal M which is not principal, then $\mathrm{Max}^v(R) = \emptyset$.

∵ Let M be a maximal ideal of a valuation domain R which is non-principal. We claim that M is not divisorial. If so, then $R \subsetneq (R : M)$. Hence, there exists an $x \in M^{-1} \setminus R$. Thus, $M_v = M \subseteq x^{-1}R \subsetneq R$, and hence $M = x^{-1}R$, a contradiction. Therefore, M is not a divisorial ideal. If $Q \in \mathrm{Max}^v(R)$ such that $M \subsetneq Q \subseteq R$, then $Q = R$; a contradiction.

Theorem 66. *A nonzero ideal I of R is t-invertible if and only if $I_t = J_t$ for some finitely generated J of R and $I_t R_M$ is principal for each maximal t-ideal M of R.*

Proof. ($\Rightarrow$) Let I be t-invertible. Then $(II^{-1})_t = R$. Hence, $1_R \in H_v$ for some finitely generated subideal H of II^{-1}. Assume that $H = (x_1, \ldots, x_t)$ such that $x_i = \sum_{j=1}^{n_i} a_{ij} b_{ij}$ for some $a_{ij} \in I$ and $b_{ij} \in I^{-1}$. For $i = 1, \ldots, n$, and $j = 1, \ldots, n_t$, put $F := \sum Ra_{ij} \subseteq R$ and $G := \sum Rb_{ij} \subseteq (R : I)$. Then we have

$$R = H_v \subseteq (FG)_v \subseteq (IG)_v \subseteq (I(R : I))_v \subseteq R.$$

Thus, $(FG)_v = (IG)_v = R$, and it follows that $G_v = (R : I)$ and $F_v = (R : G)$. Hence,

$$I_v = (I^{-1})^{-1} = (G_v)^{-1} = ((G^{-1})^{-1})^{-1} = (G^{-1})_v = F_v = F_t.$$

It implies $I_t = F_t$ because

$$F_t \subseteq I_t \subseteq I_v = F_t.$$

Note that if I is t-invertible, then I^{-1} is also t-invertible. So let $I_t = J_t$ and $(I^{-1})_t = H_t$ for some finitely generated ideals J and H of R. Since $(JH)_t = R$, $JH \nsubseteq M$ for each $M \in \mathrm{Max}^t(R)$. Hence, $(JH)R_M = (JR_M)(HR_M) = R_M$. It follows that JR_M is invertible and finitely generated, hence principal. Finally,

$$I_t R_M = J_t R_M = (JR_M)_t = JR_M.$$

$\because (IR_P)^{-1} = (R_P : IR_P) = (R : I)R_P = I^{-1}R_P$ because I is f.g.

$$K := IR_P \Longrightarrow K^{-1} = I^{-1}R_P,$$

$$(IR_P)_v = (K^{-1})^{-1} = I_v R_P.$$

($\Leftarrow$) Assume that $I_t = J_t$ for some finitely generated subideal J of I. Let $II^{-1} \subseteq P$ for some maximal t-ideal P of R. By assumption IR_P is principal, so let $IR_P = aR_P$ for some $a \in I$. Then

$$a^{-1}J \subseteq a^{-1}I \subseteq a^{-1}IR_M \subseteq R_M.$$

Thus, there exists $s \in R \setminus M$ such that $sa^{-1}J \subseteq R$ since J is finitely generated. It implies that $sa^{-1}I_t = sa^{-1}J_t \subseteq R$. Hence, $sa^{-1} \in I^{-1}$ so $s \in aI^{-1} \subseteq II^{-1} \subseteq P$; a contradiction. $\square$

Theorem 67 (Exercise)**.** *Let R be an integral domain such that the acc holds for divisorial ideals of R. Then there are only finitely many prime t-ideal of R minimal over I.*

Proof. Assume that I is a nonzero t-ideal of R. Then $I_v = J_v$ for some finitely generated subideal J of R since the acc holds. Thus, $I = I_t \subseteq I_v = J_v = J_t \subseteq I_t = I$, and hence I is divisorial and each minimal prime ideal P of I is a t-ideal. Let

$$\Sigma = \{P_1 \cdots P_n \mid P_i \in \mathrm{Min}(I)\}.$$

Consider the set

$$\Lambda = \{J \triangle R \mid J = J_t, I \subseteq J, \text{ and } C \nsubseteq J \text{ for each } C \in \Sigma\}.$$

Since for each $J \in \Lambda$, $J = L_t$ for some finitely generated subideal L of J, T is inductive. By Zorn's Lemma, T has an maximal element, say Q. It is easy to see that Q is a prime ideal. There exists a prime ideal Q_0 of R such that $Q_0 \in \mathrm{Min}(I)$ and $Q_0 \subseteq Q$. Thus, $Q_0 \in \Sigma$; a contradiction. Therefore, there exists $C = P_1 \cdots P_n \in \Sigma$ such that $C \subseteq I$. Thus, any prime ideal P minimal over I contains some P_i, and so $\{P_1, \ldots, P_n\}$ is the set of all minimal prime ideals of I. $\square$

Krull Domains.

Definition 68. An integral domain R is called a *Krull domain* if

(1) $R = \bigcap_\alpha V_\alpha$ where V_αs are rank one discrete valuation rings, that is, principal ideal domain with exactly one maximal ideal.
(2) For each nonzero element x of R, there is at most a finite number of V_α such that x is not unit in V_α.

Example 69. $\mathbb{Z}$ is a Krull domain because

(1) $\mathbb{Z} = \bigcap \mathbb{Z}_{(p)}$ where p is a prime number.
(2) each nonzero element x of $\mathbb{Z}$ is contained in finitely many maximal ideal of $\mathbb{Z}$.

Theorem 70. *Let R be an integral domain and $X^1(R)$ the set of the height-one prime ideals of R. Then the following statements are equivalent:*

(1) R is a Krull domain.
(2) R is completely integrally closed and the ascending chain condition holds on divisorial ideals of R.

(3) *Each nonzero ideal of R is t-invertible.*
(4) $R = \bigcap_{P\in \mathrm{Max}^t(R)} R_P$ *such that R_P is a rank one DVR for each $P \in \mathrm{Max}^t(R)$, and each nonzero $x \in R$ lies in only a finite number of maximal t-ideals of R.*
(5) $R = \bigcap_{P\in X^1(R)} R_P$ *such that R_P is a rank one DVR for each $P \in X^1(R)$, and each nonzero $x \in R$ lies in only a finite number of prime ideals of $X^1(R)$.*

Proof. ▶ (1) ⇒ (2) Since R is a Krull domain, there exists a family $\{V_\alpha\}$ of rank one discrete valuation rings such that $R = \bigcap_\alpha V_\alpha$, and each nonzero element x of R is non-unit in only finitely many V_α. Let $x \in \tilde{R}$. Then there exists a fractional ideal I of R such that $xI \subseteq I$. Since for each α, V_α is a PID, $IV_\alpha = aV_\alpha$ for some $a \in I$. Hence, $xI \subseteq I$ implies that $xIV_\alpha \subseteq IV_\alpha$, and hence $xaV_\alpha \subseteq aV_\alpha$. Thus, $xV_\alpha \subseteq V_\alpha$ for each α, and hence $x \in \bigcap_\alpha V_\alpha = R$. Thus, R is completely integrally closed.

To see that the ascending chain condition holds on divisorial ideals of R, we first show that for each fractional ideal I of R,

$$(R :_K I) = \bigcap_\alpha (V_\alpha :_K IV_\alpha).$$

Let $x \in (R :_K I)$. Then $xI \subseteq R = \bigcap_\alpha V_\alpha$, and hence $xI \subseteq V_\alpha$ for each α. Thus, $xIV_\alpha \subseteq V_\alpha$, and so $\bigcap_\alpha (V_\alpha :_K IV_\alpha)$. For the reverse containment, let $x \in \bigcap_\alpha (V_\alpha :_K IV_\alpha)$. Then $x \in (V_\alpha :_K IV_\alpha)$ for each α. Thus, $xI \subseteq xIV_\alpha \subseteq V_\alpha$ for each α, and hence $x \in (R :_K I)$. Therefore, for each divisorial ideal I of R, we have

$$I = I_v = (R :_K (R :_K I)) = \bigcap_\alpha (V_\alpha :_K (R :_K I)V_\alpha).$$

Now, consider the following ascending chain of divisorial ideals of R:

$$0 \neq I_1 \subseteq I_2 \subseteq \dots.$$

For each α,

$$(R :_K I_1)V_\alpha \supseteq (R :_K I_2)V_\alpha \supseteq \dots.$$

Hence,

$$(V_\alpha :_K (R :_K I_1)V_\alpha) \subseteq (V_\alpha :_K (R :_K I_2)V_\alpha) \subseteq \dots$$

is an ascending chain of fractional ideals in V_α for each α. Note that $(R :_K I_1)V_\alpha = V_\alpha$ for almost all α. For other finite number of finite V_α, there exists an integer $n \geq 1$ such that for each $m \geq n$ and all α,

$$(V_\alpha :_K (R :_K I_n)V_\alpha) = (V_\alpha :_K (R :_K I_m)V_\alpha).$$

Hence, $I_n = I_m$ for each $m \geq n$.

▶ (2) ⇒ (3) Let I be a nonzero ideal of R such that I is not t-invertible. Then $II^{-1} \subseteq P$ for some maximal t-ideal P of R. Thus,

$$(R : P) \subseteq (R : II^{-1}) = ((R : I) : (R : I)) = R,$$

where the last equality holds because R is completely integrally closed. It follows that $P_v = R$. Since the acc holds on divisorial ideals of R, $P_v = J_v = J_t$ for some finitely generated ideal J with $J \subseteq P$. Thus, $R = P_v = J_t \subseteq P_t = P \subseteq R$, and hence $P = R$; a contradiction

▶ (3) ⇒ (2) Let I be a nonzero ideal of R. Then $(II^{-1})_t = R$, and hence $I_t = J_t$ for some finitely generated subideal J of I. Then $I_v = J_v$ which implies that the acc holds on dicisorial ideals of R. On the other hand, let $x \in \tilde{R}$. Then $x \in (I : I)$ for some fractional ideal I of R. By (3), $(II^{-1})_t = R$ implies that $(II^{-1})_v = R$. Hence, $(I_v : I_v) = R$ because $(I_v : I_v) = (R : II^{-1}) = (R : (II^{-1})_v) = (R : R)$. Thus, $x \in (I : I) \subseteq (I_v : I_v) = R$.

▶ (2) ⇒ (4) Let P be a maximal t-ideal of R. Then $P_v = J_v$ for some finitely generated subideal J of P. If $P \subset P_v \subseteq R$, then $P_v = R$ because $P_v = (P_v)_t$. Hence, $R = P_v = J_v = J_t \subseteq P$; a contradiction. Thus, each maximal t-ideal of R is divisorial. Since R is a completely integrally closed and P is a divisorial ideal of R, R_P is a DVR by Theorem 62.

Since the acc holds for divisorial ideals of R, the result follows from Theorem 67. Note that $X^1(R) = \text{Max}^t(R)$.

∵ Let P be a maximal t-ideal of R. By (2) ⇒ (3), P is t-invertible, and hence PR_P is a principal ideal. Assume that $\text{ht}P \geq 2$. Thus, there is a prime ideal P_1 such that $(0) \subset P_1 \subset P$. Since P_1 is t-invertible, $P_1R_{P_1}$ is principal. Thus, $P_1R_P = PR_P$, which implies that $P_1 = P$; a contradiction. For the converse, let $P \in X^1(R)$. Then $\text{ht}(PR_P) = 1$ and PR_P is minimal over a principal ideal $\frac{a}{s}R_P$ of R_P because R_P is a PID. It implies that P is minimal over aR. Since aR is a t-ideal, P is a t-ideal. If $P \notin \text{Max}^t(R)$, then $P \subset M$ for some maximal t-ideal M of R. It implies that $\text{ht}P \geq 2$; a contradiction.

▶ (4) ⇒ (5) Let $P \in X^1(R)$. Then P is minimal over a principal ideal xR of R. Since xR is a t-ideal, P is a t-ideal. If $P \notin \text{Max}^t(R)$, then $P \subset M$ for some maximal t-ideal M of R. It implies that $\text{ht}P \geq 2$; a contradiction. Hence, P is a maximal t-ideal so that the result follows.

▶ (5) ⇒ (1) It is clear. □

Corollary 71. *Every Krull domain does satisfy the PIT.*

Proof. Let P be a minimal prime ideal of a principal ideal (a) of R. Then PR_P is a minimal prime ideal of aR_P, and hence $\text{ht}(PR_P) \leq 1$ because R_P is Noetherian. Thus, $\text{ht}(P) \leq 1$. □

Theorem 72. *Let R be a Krull domain and I a nonzero divisorial ideal of R. Then $I = (P_1^{e_1} \cdots P_n^{e_n})_t$ where $P_1, \ldots, P_n \in X^1(R)$ and $e_1, \ldots, e_n$ are positive integers.*

Proof. Since R is a Krull domain, the t-operation and the v-operation coincide, $X^1(R) = \text{Max}^t(R)$ and $R = \bigcap_{P \in X^1(R)} R_P$ such that R_P is a rank one DVR for each $P \in X^1(R)$, and each nonzero $x \in R$ lies in only a finite number of prime ideals of $X^1(R)$. Hence, I is contained at most in finitely many height-one primes $P_1, \ldots, P_n$. Since R_{P_i} is a DVR, $IR_{P_i} = P_i^{e_i}R_{P_i}$. Hence,

$$I = \bigcap_{P \in X^1(R)} IR_P = \bigcap_{i=1}^{n} P_i^{e_i}R_{P_i} \cap \bigcap_{P \in X^1(R) \setminus \{P_1, \ldots, P_n\}} R_P = (P_1^{e_1} \cdots P_n^{e_n})_t.$$

□

Krull-Akizuki Theorem.

Remark 73. Let R be a commutative ring and M a unitary R-module.

(1) If I is a subideal of $\text{Ann}_R(M)$, then M is an R/I-module, and M is a Noetherian R-module if and only if M is a Noetherian R/I-module.
(2) If $M_1, \ldots, M_n$ are maximal ideals of R such that $M_1 \cdots M_n M = 0$, then M is a Noetherian R-module if and only if M is an Artinian R-module.

(3) If R is a Noetherian ring such that each prime ideal is maximal , then R is an Artinian ring with finitely many maximal ideals.
(4) R is an Artinian ring if and only R is a zero-dimensional Noetherian ring.
(5) If R/I is a Noetherian ring, then R is a Noetherian ring.
(6) If R is a Noetherian ring and M is a finitely generated R-module, then M is a Noetherian module.

Definition 74. Let R be an integral domain with quotient field K and $\mathrm{Max}(R)$ the set of all maximal ideals of R. The *global transform* of R, denoted by R^g, is defined as

$$R^g := \{x \in K \mid xM_1 \cdots M_n \subseteq R \text{ for some } M_i \in \mathrm{Max}(R)\}.$$

Note that M_is are not necessarily disjoint. It is clear that R^g is a ring containing R.

Theorem 75. *Let R be a Noetherian domain of dimension one with quotient filed K. Then $R^g = K$.*

Proof. Let $x \in K$, and set $I = (R :_R x)$. Since $\dim R = 1$ and R is a Noetherian domain, there are only finitely many maximal ideals, say $M_1, \dots, M_k$ of R containing I, and so $\sqrt{I} = M_1 \cap \ldots \cap M_k = M_1 \cdots M_k$. Note that $M_1 \cdots M_k$ is finitely generated; so there is an integer $n \geqslant 1$ such that $(M_1 \cdots M_k)^n \subseteq I$, and thus $x(M_1 \cdots M_k)^n \subseteq R$. Thus, $x \in R^g$. Since $R^g \subseteq K$, we have $R^g = K$. □

Theorem 76. *Let R be a Noetherian domain with quotient filed K and T a ring between R and K such that $T \subseteq R^g$. Then T/xT is finitely generated R-module for each nonzero element x of R.*

Proof. Let

$$I_m := (x^m T \cap R, xR)$$

for all integers $m \geq 1$. Since R is a Noetherian domain and $x \in I_m$ for each $m \geq 1$, $\{I_m\}_{m\geq 1}$ is a descending chain of finitely generated ideals of R. Then

$$I_1 = (xr_1, \dots, xr_l)$$

with $r_i \in T \subseteq R^g$. Thus, there exists a finite product of maximal ideals of R, say I, such that $Ir_i \subseteq R$ for $i = 1, \dots, l$. Hence, I_1/xR is a finitely generated R/I-module and I_1/xR is an Artinian R/I-module. Thus, there exists an integer $n \geq 1$ such that

$$I_n/xR = I_{n+j}/xR,$$

and hence

$$I_n = I_{n+j}$$

for all integers $j \geq 0$.

We next show that $T \subseteq x^{-n}R + xT$. Let $r \in T$. Then $r \in R^g$, and hence there exists a finite product of maximal ideals of R, say J, such that $rJ \subseteq R$. Then $L := (R :_R rR)$ is an ideal of R containing J. Therefore, R/L is Artinian. Hence, there exists an integer $k \geq 1$ such that

$$(x^k) + L = (x^{k+1}) + L.$$

Therefore,

$$x^k = ax^{k+1} + l$$

for some $a \in R$ and $l \in L$. Hence,

$$rx^k = rax^{k+1} + rl.$$

Thus,

$$r = rax + rlx^{-k}.$$

Since $rl \in R$, we have

$$r \in x^{-k}R + xT.$$

Thus, $T \subseteq x^{-k}R + xT$.

Now, assume that $T \nsubseteq x^{-n}R + xT$, and choose $b \in T \setminus (x^{-n}R + xT)$. Since $T \subseteq x^{-k}R + xT$, we have that $k > n$ and $b \in x^{-k}R + xT$; so we may assume that k is the smallest integer with this property. Hence,

$$b = cx^{-k} + xr'$$

or

$$x^k b = c + x^{k+1}r'$$

with $c \in R$ and $r' \in T$. Therefore,

$$x^k(b - xr') = c \in I_k,$$

and since

$$I_k = I_{k+1}$$

by the previous paragraph,

$$x^k(b - xr') = x^{k+1}r'' + xc'$$

for some $r'' \in T$ and $c' \in R$. Hence,

$$b = x(r'' + r') + c'x^{-(k-1)} \in x^{-(k-1)}R + xT,$$

a contradiction.

Therefore,

$$T/xT \subseteq (x^{-n}R + xT)/xT \cong R/(x^{n+1}T \cap R)$$

as R-modules. Note that $R/x^{n+1}R$ is a Noetherian ring. Also, since

$$x^{n+1}R \subseteq \mathrm{Ann}_R(T/xT) \cap \mathrm{Ann}_R(R/(x^{n+1}T \cap R)),$$

both T/xT and $R/(x^{n+1}T \cap R)$ are $R/x^{n+1}R$-modules.
Clearly, $R/(x^{n+1}T \cap R)$ is generated by $1 + x^{n+1}T \cap R$ over $R/x^{n+1}R$. Hence, $R/(x^{n+1}T \cap R)$ is a Noetherian $R/x^{n+1}R$-module, and thus $R/(x^{n+1}T \cap R)$ is a Noetherian R-module. Therefore, T/xT is a Noetherian R-module.

Moreover, if N is an ideal of T containing x, then N/xT is an R-submodule of T/xT, and hence N/xT is a finitely generated R-module. Thus, N is finitely generated. $\square$

Corollary 77. *Let R be a Noetherian domain of dimension one with quotient filed K. Then each ring between R and K is again Noetherian.*

Proof. Assume that T is a ring between R and $K = R^g$ and J is a nonzero ideal of T. Since $JK = K$, and hence there exists a nonzero element $x \in R$ such that $x \in J$. Therefore, J is finitely generated by Theorem 76. Hence, T is a Noetherian ring.

Let Q be a prime ideal of T. Then $P := Q \cap R$ is a prime ideal of R. Since $\dim R = 1$, P is a maximal ideal of R, and hence R/P is a filed. Note that T/Q is a finitely generated R/P-module. Thus, T/Q is a field, and hence Q is a maximal ideal of T. Therefore, $\dim T \leq 1$. $\square$

Mori-Nagata Theorem.

Lemma 78. *Assume that R is a Noetherian integral domain with quotient field K and the integral closure $\bar{R}$. Let $a_1, \ldots, a_n \in \bar{R}$. Then*

$$(R :_K (R :_K \sum_{i=1}^{n} Ra_i)) \subseteq (\bar{R} :_K (\bar{R} :_K \sum_{i=1}^{n} \bar{R}a_i)).$$

Proof. Since $a_i \in \bar{R}$, there exists a nonzero finitely generated ideal I of R such that $a_i I \subseteq I$ for $i = 1, \ldots, n$. Thus, $\sum_{i=1}^{n} Ra_i I \subseteq I$. Since

$$(\sum_{i=1}^{n} Ra_i I)_v = ((\sum_{i=1}^{n} Ra_i)_v I_v)_v,$$

we have

$$(\sum_{i=1}^{n} Ra_i)_v I_v \subseteq (\sum_{i=1}^{n} Ra_i I)_v \subseteq I_v.$$

Hence,

$$(\sum_{i=1}^{n} Ra_i)_v \subseteq (I_v : I_v).$$

Since $I_v \subseteq R$ and R is Noetherian, I_v is finitely generated, and hence

$$(\sum_{i=1}^{n} Ra_i)_v \subseteq (I_v : I_v) \subseteq \bar{R}.$$

Assume that $x \in (\bar{R} :_K \sum_{i=1}^{n} \bar{R}a_i)$. Then $xa_i\bar{R} \subseteq x\sum_{i=1}^{n} \bar{R}a_i \subseteq \bar{R}$. By a_i replaced by xa_i, we have

$$(\sum_{i=1}^{n} Rxa_i)_v \subseteq \bar{R}.$$

Thus,

$$(\bar{R} :_K \sum_{i=1}^{n} \bar{R}a_i)(\sum_{i=1}^{n} Ra_i)_v \subseteq \bar{R}$$

which implies that

$$(\sum_{i=1}^{n} Ra_i)_v \subseteq (\bar{R} :_K (\bar{R} :_K \sum_{i=1}^{n} \bar{R}a_i)).$$

$\square$

Corollary 79. *Assume that R is a Noetherian integral domain with quotient field K and the integral closure $\bar{R}$. If Q is a t-ideal of $\bar{R}$, then $Q \cap R$ is a t-ideal of R.*

Proof. Set $P := Q \cap R$, and let $x \in P_t \subseteq R$. Then $x \in J_v$ for some finitely generated subideal J of P. Let $J = (a_1, \ldots, a_n)$. Then $a_i \in \bar{R}$. Hence,

$$J_v = (R :_K (R :_K \sum_{i=1}^{n} Ra_i)) \subseteq (\bar{R} :_K (\bar{R} :_K \sum_{i=1}^{n} \bar{R}a_i)) = (J\bar{R})_v$$

by Lemma 78. Note that $J\bar{R} \subseteq P\bar{R} = (Q \cap R)\bar{R} \subseteq Q$, and hence $(J\bar{R})_t \subseteq Q$. Thus, $x \in J_v = J_t \subseteq (J\bar{R})_t \subseteq Q$, and hence $x \in Q \cap R = P$. $\square$

Theorem 80. *Let R be an integral domain. Then $R = \bigcap_{P\in Ass(R)} R_P$, where* $\mathrm{Ass}(R)$ *is the set of prime ideals P of R such that P is minimal over $(aR :_R bR)$ for some $a, b \in R$.*

Proof. It is clear that $R \subseteq \bigcap_{P\in \mathrm{Ass}(R)} R_P$. For the reverse containment, let $x \in \bigcap_{P\in \mathrm{Ass}(R)} R_P$. Then $x \in R_P$ for all $P \in \mathrm{Ass}(R)$. Let $P \in \mathrm{Ass}(R)$ and $x = \frac{a}{b}$ where $a \in R$ and $b \in R \setminus P$. Suppose on the contrary that $x \notin R$. Then $a \notin bR$, and hence $1 \notin (bR :_R aR)$. Thus, $(bR :_R aR)$ is a proper ideal of R. We know that every proper ideal of a ring has at least one minimal prime ideal. So let Q be a minimal prime ideal of $(bR :_R aR)$. Hence, $Q \in \mathrm{Ass}(R)$, and hence $\frac{a}{b} \in R_Q$. Thus, $aR_Q \subseteq bR_Q$, and hence $(bR_Q :_{R_Q} aR_Q) = R_Q$. So

$$R_Q = (bR_Q :_{R_Q} aR_Q) = (bR :_R aR)R_Q \subseteq QR_Q \subseteq R_Q.$$

It implies that $QR_Q = R_Q$; a contradiction. Thus, $x \in R$. □

Theorem 81. *Assume that R is a Noetherian integral domain with integral closure $\bar{R}$. Then* $\mathrm{Ass}(\bar{R}) = \mathrm{Min}(\bar{R})$.

Proof. Let $Q \in \mathrm{Ass}(\bar{R})$, $P := Q \cap R$, and $S = R \setminus P$. Put

$$D := (R_P)^g \cap \bar{R}_S = (R_P)^g \cap \overline{R_P}.$$

Then

(1) $\bar{D} = \bar{R}_S$, hence $R_P \subseteq D \subseteq \bar{R}_S$ are integral extensions.
(2) D is a Noetherian domain because R_P is a Noetherian domain and $R_P \subseteq D \subseteq (R_P)^g$ (Theorem 76).

Since $Q \in \mathrm{Ass}(\bar{R})$, there exist $a, b \in \bar{R}$ such that $Q \in \mathrm{Min}(a\bar{R} : b\bar{R})$. Thus, $Q\bar{R}_S \in \mathrm{Min}(a\bar{R}_S : b\bar{R}_S)$, and hence $Q\bar{R}_S \in \mathrm{Ass}(\bar{R}_S)$. Put

$$M := Q\bar{R}_S \cap D.$$

Since $Q\bar{R}_S$ is a t-ideal of $\bar{R}_S$, M is a t-ideal of D by Corollary 79. Since $R_P \subseteq D$ and $\bar{R}_S = \bar{D}$, D is integral over R_P. Hence, M is a maximal ideal of D because

$$PR_P = Q\bar{R}_S \cap D \cap R_P = M \cap R_P.$$

$\because$ Let $\frac{a}{b} \in Q\bar{R}_S \cap R_P$ where $a \in Q \subseteq \bar{R}$ and $b \in S$. Then $\frac{a}{b} = \frac{c}{d}$ for some $c \in R$ and $d \in S$. Thus, there exists $s \in S$ such that $sbc = sad \in Q \cap R = P$. Hence, $c \in P$ which implies that $\frac{a}{b} = \frac{c}{d} \in PR_P$. The other containment is clear.
We claim that M is invertible. Suppose not. Since M is a maximal ideal of D and

$$M \subseteq MM^{-1} \subsetneq D,$$
$$M = MM^{-1}.$$

Then

$$M^{-1} \subseteq (M : M) \subseteq \bar{D} = \bar{R}_S$$

because M is finitely generated. On the other hand,

$$M^{-1} \subseteq ((R_P)^g : PR_P) = (R_P)^g.$$

$\because$ Let $x \in M^{-1}$. Then $xPR_P = x(M \cap R_P) \subseteq xM \subseteq D \subseteq (R_P)^g$.
Thus,

$$M^{-1} \subseteq \bar{R}_S \cap (R_P)^g = D,$$

and it implies that

$$M = M_t = M_v = D;$$

a contradiction. Therefore, M is an invertible ideal of D.

Now, if Q is not a minimal prime ideal of $\bar{R}$, there exists a prime ideal Q_0 of $\bar{R}$ such that $Q_0 \subsetneq Q$. Since $\bar{R}_S$ is integral over D,

$$Q_0\bar{R}_S \cap D \subsetneq Q\bar{R}_S \cap D = M.$$

Then $Q_0\bar{R}_S \cap D \subseteq M^n$ for all integers $n \geq 1$ because M is invertible. Let $x \in Q_0\bar{R}_S \cap D$. Then we have the following ascending chain of ideals of D

$$xD \subsetneq xM^{-1} \subsetneq xM^{-2} \subsetneq \dots.$$

This contradicts that D is a Noetherian domain. Therefore, $Q \in \mathrm{Min}(\bar{R})$. The converse is trivial.

Notice. $M \in \mathrm{Min}(D)$, and hence D has finitely many maximal ideals. We note that $M = Q\bar{R}_S \cap D$ such that $Q \in \mathrm{Min}(\bar{R})$. Hence, $Q\bar{R}_S \in \mathrm{Min}(\bar{R}_S)$. Thus, $M\bar{R}_S = Q\bar{R}_S$. If there exists a prime ideal $Q' \subsetneq M$, then

$$Q'\bar{R}_S \subsetneq M\bar{R}_S = Q\bar{R}_S$$

since $\bar{R}_S$ is integral over D (INC property); a contradiction. □

Theorem 82. *Assume that R is a Noetherian integral domain with integral closure $\bar{R}$. If Q is a nonzero minimal prime ideal of $\bar{R}$, then $\bar{R}_Q$ is a DVR.*

Proof. Let $Q \in \mathrm{Min}(\bar{R})$. It is enough to show that $\bar{R}_Q$ is a Noetherian domain whose maximal ideal is principal. Put $P := Q \cap R$, $D := (R_P)^g \cap \bar{R}_S$ where $S = R \setminus P$, and $M := Q\bar{R}_S \cap D$. Then D is a Noetherian domain with $M \in \mathrm{Min}(D)$. Since $MD_M \in \mathrm{Max}(D_M)$, $\dim D_M = \mathrm{ht}M = 1$. Thus, $(D_M)^g = qf(D)$. Hence,

$$D_M \subseteq \bar{R}_{\bar{R}\setminus Q} \subseteq \bar{R}_{\bar{R}\setminus(0)} = qf(D) = (D_M)^g.$$

It implies that $\bar{R}_Q$ is a Noetherian domain, and hence $Q\bar{R}_Q$ is finitely generated. We claim that $Q\bar{R}_Q$ is invertible, and hence principal. Suppose not. Then

$$Q\bar{R}_Q.(Q\bar{R}_Q)^{-1} = Q\bar{R}_Q$$

by maximality of $Q\bar{R}_Q$. Thus,

$$(Q\bar{R}_Q)^{-1} \subseteq (Q\bar{R}_Q : Q\bar{R}_Q) \subseteq \bar{R}_Q$$

because $Q\bar{R}_Q$ is finitely generated. Thus, $(Q\bar{R}_Q)^{-1} = \bar{R}_Q$ which contradicts that $Q\bar{R}_Q$ is a t-ideal. This contradiction proves that $Q\bar{R}_Q$ is invertible. □

Lemma 83. *Assume that R is a Noetherian integral domain with integral closure $\bar{R}$. If $\{I_i\}$ is a descending chain of divisorial ideals of R such that $\cap I_i$ contains a nonzero element, then the chain is stationary.*

Proof. Let $x \in \cap I_i$ be a nonzero element. Then

$$xR \subseteq \cap I_i \subseteq \ldots \subseteq I_2 \subseteq I_1 \subseteq R.$$

Hence,

$$xR \subseteq xI_1^{-1} \subseteq xI_2^{-1} \subseteq \ldots \subseteq x(\cap I_i)^{-1} \subseteq R.$$

Since R is Noetherian, there exists an integer $n \geq 1$, such that $xI_n^{-1} = xI_{n+1}^{-1} = \ldots$. Hence, $I_n = I_{n+1} = \ldots$. □

Lemma 84. *Assume that R is a Noetherian integral domain with integral closure $\bar{R}$. For each nonzero prime ideal P of R, there are only finitely many nonzero minimal prime ideals of $\bar{R}$ lying over P.*

Proof. Assume that P is a prime ideal of R, and $Q \in \mathrm{Min}(\bar{R})$ such that $Q \cap R = P$. Let $D := (R_P)^g \cap \bar{R}_S$ where $S = R \setminus P$ and $M := Q\bar{R}_S \cap D$. Then M is a maximal ideal of D and $M \in \mathrm{Min}(D)$ and hence, $D^g_M = qf(D_M) = qf(D)$. Thus, any ring between D_M and its quotient field is Noetherian. In particular, $\bar{D}_M$ is Noetherian. Let $N = (D \setminus M) \cap \bar{R}$. Then N is a m.c.s. of $\bar{R}$ containing S, $\bar{D}_M = \bar{R}_N$, and

$$\mathrm{Max}(\bar{R}_N) = \{Q_\alpha \bar{R}_N \mid Q \in \mathrm{Spec}(\bar{R}); Q_\alpha \bar{R}_N \cap D = M\}$$

since $\bar{R}_S$ is integral over D. Since $\bar{R}_N$ is integral over D_M, a prime ideal of $\bar{R}_N$ is maximal if and only if it is minimal over $M\bar{R}_N$, and hence the number of maximal ideals of $\bar{R}_N$ is finite. Since D has finitely many maximal ideals,

$$\{M_\alpha \in \mathrm{Max}(\bar{R}_S) \mid M_\alpha \cap D = Q\bar{R}_S \cap D\}$$

must be finite. Since

$$\{Q_\alpha \bar{R}_S \mid Q_\alpha \in \mathrm{Min}(\bar{R}), Q_\alpha \cap R = P\} \subseteq \{M_\alpha \in \mathrm{Max}(\bar{R}_S) \mid M_\alpha \cap D = Q\bar{R}_S \cap D\},$$

the set

$$\{Q \in \mathrm{Min}(\bar{R}) \mid Q \cap R = P\}$$

must be finite. □

Theorem 85. *Assume that R is a Noetherian integral domain with integral closure $\bar{R}$. Then $\bar{R}$ is a Krull domain.*

Proof. Note that $\bar{R} = \bigcap_{Q \in \mathrm{Min}(\bar{R})} \bar{R}_Q$. Since each $\bar{R}_Q$ is a DVR by Theorem 82, it suffices to show that each nonzero element of $\bar{R}$ lies in only a finite number of minimal prime ideals of $\bar{R}$. Let x be a nonzero element of R, and

$$\Lambda = \{Q_\alpha \in \mathrm{Min}(\bar{R}) \mid x \in Q_\alpha\}$$

be infinite. Then

$$\Lambda_1 = \{Q_\alpha \cap R \mid Q_\alpha \in \Lambda\}$$

is infinite by Lemma 84.

$\because$ If $\Lambda_1 = \{P_1, \ldots, P_n\}$, then for each $Q \in \Lambda$, $Q \in \mathrm{Min}(\bar{R})$ and $Q \cap R = P_i$ for some $i = 1, \ldots, n$. Thus, Q is contained in the set of minimal prime ideals of $\bar{R}$ lying over P_i.

Since each ideal in Λ_1 is a divisorial ideal containing x, Λ_1 has a minimal element and only a finite number of minimal elements. Let $P_1 \in \Lambda_1$ be the minimal element of Λ_1. Then the set

$$\Lambda_2 = \{Q_\alpha \cap R \in \Lambda_1 \mid P_1 \subset Q_\alpha \cap R\}$$

which is infinite. Thus, there exists a minimal element $P_2 \in \Lambda_2$ such that the set

$$\Lambda_3 = \{Q_\alpha \cap R \in \Lambda_2 \mid P_2 \subset Q_\alpha \cap R\}$$

is infinite. Continuing this process, we have an infinite chain of prime ideals

$$P_1 \subset P_2 \subset \ldots$$

of R; a contradiction because R is a Noetherian domain. Therefore, Λ must be finite. □

Corollary 86. *Any Krull domain of dimension one is a Dedekind domain, i.e. Noetherian integrally closed domain of dimension one.*

References

1. Chang, G.W. and Kang, B.G., 2002. "Integral closure of a ring whose regular ideals are finitely generated". Journal of Algebra, 251(2), 529-537.
2. Fossum, R.M. 1973. "The divisor class group of a Krull domain". New York: Springer.
3. Gilmer, R. 1972. "Multiplicative ideal theory". New York: Marcel Dekker.
4. Rotman, J. 1979. "An Introduction to Homological Algebra". New York: Academic Press.

(Hamdi) School of Mathematics, Institute for Research in Fundamental Sciences (IPM), P.O. Box: 19395-5746, Tehran, Iran.

Email address: `h.hamdimoghadam@tabrizu.ac.ir`