Chapter 3

Valuation Rings

The results of this chapter come into play when analyzing the behavior of a rational function defined in the neighborhood of a point on an algebraic curve.

3.1 Extension Theorems

In Theorem 2.2.4, we generalized a result about field extensions to rings. Here is another variation.

3.1.1 Theorem

Let R be a subring of the field K, and $h : R \to C$ a ring homomorphism from R into an algebraically closed field C. If α is a nonzero element of K, then either h can be extended to a ring homomorphism $\overline{h} : R[\alpha] \to C$, or h can be extended to a ring homomorphism $\overline{h} : R[\alpha^{-1}] \to C$.

Proof. Without loss of generality, we may assume that R is a local ring and $F = h(R)$ is a subfield of C. To see this, let P be the kernel of h. Then P is a prime ideal, and we can extend h to $g : R_P \to C$ via $g(a/b) = h(a)/h(b),\ h(b) \neq 0$. The kernel of g is PR_P, so by the first isomorphism theorem, $g(R_P) \cong R_P/PR_P$, a field (because PR_P is a maximal ideal). Thus we may replace (R, h) by (R_P, g).

Our first step is to extend h to a homomorphism of polynomial rings. If $f \in R[x]$ with $f(x) = \sum a_i x^i$, we take $h(f) = \sum h(a_i)x^i \in F[x]$. Let $I = \{f \in R[x] : f(\alpha) = 0\}$. Then $J = h(I)$ is an ideal of $F[x]$, necessarily principal. Say $J = (j(x))$. If j is nonconstant, it must have a root β in the algebraically closed field C. We can then extend h to $\overline{h} : R[\alpha] \to C$ via $\overline{h}(\alpha) = \beta$, as desired. To verify that $\overline{h}$ is well-defined, suppose $f \in I$, so that $f(\alpha) = 0$. Then $h(f) \in J$, hence $h(f)$ is a multiple of j, and therefore $h(f)(\beta) = 0$. Thus we may assume that j is constant. If the constant is zero, then we may extend h exactly as above, with β arbitrary. So we can assume that $j \neq 0$, and it follows that $1 \in J$. Consequently, there exists $f \in I$ such that $h(f) = 1$.

This gives a relation of the form

$$\sum_{i=0}^{r} a_i \alpha^i = 0 \text{ with } a_i \in R \text{ and } \overline{a}_i = h(a_i) = \begin{cases} 1, & i = 0 \\ 0, & i > 0 \end{cases} \tag{1}$$

Choose r as small as possible. We then carry out the same analysis with α replaced by α^{-1}. Assuming that h has no extension to $R[\alpha^{-1}]$, we have

$$\sum_{i=0}^{s} b_i \alpha^{-i} = 0 \text{ with } b_i \in R \text{ and } \overline{b}_i = h(b_i) = \begin{cases} 1, & i = 0 \\ 0, & i > 0 \end{cases} \tag{2}$$

Take s minimal, and assume (without loss of generality) that $r \geq s$. Since $h(b_0) = 1 = h(1)$, it follows that $b_0 - 1 \in \ker h \subseteq \mathcal{M}$, the unique maximal ideal of the local ring R. Thus $b_0 \notin \mathcal{M}$ (else $1 \in \mathcal{M}$), so b_0 is a unit. It is therefore legal to multiply (2) by $b_0^{-1}\alpha^s$ to get

$$\alpha^s + b_0^{-1} b_1 \alpha^{s-1} + \cdots + b_0^{-1} b_s = 0 \tag{3}$$

Finally, we multiply (3) by $a_r \alpha^{r-s}$ and subtract the result from (1) to contradict the minimality of r. (The result of multiplying (3) by $a_r \alpha^{r-s}$ cannot be a copy of (1). If so, $r = s$ (hence $\alpha^{r-s} = 1$)and $a_0 = a_r b_0^{-1} b_s$. But $h(a_0) = 1$ and $h(a_r b_0^{-1} b_s) = 0$.) ♣

It is natural to try to extend h to a larger domain, and this is where valuation rings enter the picture.

3.1.2 Definition

A subring R of a field K is a *valuation ring* of K if for every nonzero $\alpha \in K$, either α or α^{-1} belongs to R.

3.1.3 Examples

The field K is a valuation ring of K, but there are more interesting examples.

1. Let $K = \mathbb{Q}$, with p a fixed prime. Take R to be the set of all rationals of the form $p^r m/n$, where $r \geq 0$ and p divides neither m nor n.

2. Let $K = k(x)$, where k is any field. Take R to be the set of all rational functions $p^r m/n$, where $r \geq 0$, p is a fixed polynomial that is irreducible over k and m and n are arbitrary polynomials in $k[x]$ not divisible by p. This is essentially the same as the previous example.

3. Let $K = k(x)$, and let R be the set of all rational functions $f/g \in k(x)$ such that $\deg f \leq \deg g$.

4. Let K be the field of formal *Laurent series* over k. Thus a nonzero element of K looks like $f = \sum_{i=r}^{\infty} a_i x^i$ with $a_i \in k$, $r \in \mathbb{Z}$, and $a_r \neq 0$. We may write $f = a_r x^r g$, where g belongs to the ring $R = k[[x]]$ of formal power series over k. Moreover, the constant term of g is 1, and therefore g, hence f, can be inverted (by long division). Thus R is a valuation ring of K.

We now return to the extension problem.

3.1.4 Theorem

Let R be a subring of the field K, and $h : R \to C$ a ring homomorphism from R into an algebraically closed field C. Then h has a maximal extension $(V, \overline{h})$. In other words, V is a subring of K containing R, $\overline{h}$ is an extension of h, and there is no extension to a strictly larger subring. In addition, for any maximal extension, V is a valuation ring of K.

Proof. Let $\mathcal{S}$ be the set of all (R_i, h_i), where R_i is a subring of K containing R and h_i is an extension of h to R_i. Partially order $\mathcal{S}$ by $(R_i, h_i) \leq (R_j, h_j)$ if and only if R_i is a subring of R_j and h_j restricted to R_i coincides with h_i. A standard application of Zorn's lemma produces a maximal extension $(V, \overline{h})$. If α is a nonzero element of K, then by (3.1.1), $\overline{h}$ has an extension to either $V[\alpha]$ or $V[\alpha^{-1}]$. By maximality, either $V[\alpha] = V$ or $V[\alpha^{-1}] = V$. Therefore $\alpha \in V$ or $\alpha^{-1} \in V$. ♣

3.2 Properties of Valuation Rings

We have a long list of properties to verify, and the statement of each property will be followed immediately by its proof. The end of proof symbol will only appear at the very end. Throughout, V is a valuation ring of the field K.

1. The fraction field of V is K.

This follows because a nonzero element α of K can be written as $\alpha/1$ or as $1/\alpha^{-1}$.

2. Any subring of K containing V is a valuation ring of K.

This follows from the definition of a valuation ring.

3. V is a local ring.

We will show that the set $\mathcal{M}$ of nonunits of V is an ideal. If a and b are nonzero nonunits, then either a/b or b/a belongs to V. If $a/b \in V$, then $a + b = b(1 + a/b) \in \mathcal{M}$ (because if $b(1 + a/b)$ were a unit, then b would be a unit as well). Similarly, if $b/a \in V$, then $a + b \in \mathcal{M}$. If $r \in V$ and $a \in \mathcal{M}$, then $ra \in \mathcal{M}$, else a would be a unit. Thus $\mathcal{M}$ is an ideal.

4. V is integrally closed.

Let α be a nonzero element of K, with α integral over V. Then there is an equation of the form

$$\alpha^n + c_{n-1}\alpha^{n-1} + \cdots + c_1\alpha + c_0 = 0$$

with the c_i in V. We must show that $\alpha \in V$. If not, then $\alpha^{-1} \in V$, and if we multiply the above equation of integral dependence by $\alpha^{-(n-1)}$, we get

$$\alpha = -c_{n-1} - c_{n-2}\alpha^{-1} - \cdots - c_1\alpha^{-(n-2)} - c_0\alpha^{-(n-1)} \in V.$$

5. If I and J are ideals of V, then either $I \subseteq J$ or $J \subseteq I$. Thus the ideals of V are totally ordered by inclusion.

Suppose that I is not contained in J, and pick $a \in I \setminus J$ (hence $a \neq 0$). If $b \in J$, we must show that $b \in I$. If $b = 0$ we are finished, so assume $b \neq 0$. We have $b/a \in V$ (else $a/b \in V$, so $a = (a/b)b \in J$, a contradiction). Therefore $b = (b/a)a \in I$.

6. Conversely, let V be an integral domain with fraction field K. If the ideals of V are totally ordered by inclusion, then V is a valuation ring of K.

If α is a nonzero element of K, then $\alpha = a/b$ with a and b nonzero elements of V. By hypothesis, either $(a) \subseteq (b)$, in which case $a/b \in V$, or $(b) \subseteq (a)$, in which case $b/a \in V$.

7. If P is a prime ideal of the valuation ring V, then V_P and V/P are valuation rings.

First note that if K is the fraction field of V, it is also the fraction field of V_P. Also, V/P is an integral domain, hence has a fraction field. Now by Property 5, the ideals of V are totally ordered by inclusion, so the same is true of V_P and V/P. The result follows from Property 6.

8. If V is a Noetherian valuation ring, then V is a PID. Moreover, for some prime $p \in V$, every ideal is of the form $(p^m),\ m \geq 0$. For any such p, $\cap_{m=1}^{\infty}(p^m) = 0$.

Since V is Noetherian, an ideal I of V is finitely generated, say by $a_1, \ldots, a_n$. By Property 5, we may renumber the a_i so that $(a_1) \subseteq (a_2) \cdots \subseteq (a_n)$. But then $I \subseteq (a_n) \subseteq I$, so $I = (a_n)$. In particular, the maximal ideal $\mathcal{M}$ of V is (p) for some p, and p is prime because $\mathcal{M}$ is a prime ideal. If (a) is an arbitrary ideal, then $(a) = V$ if a is a unit, so assume a is a nonunit, that is, $a \in \mathcal{M}$. But then p divides a, so $a = pb$. If b is a nonunit, then p divides b, and we get $a = p^2c$. Continuing inductively and using the fact that V is a PID, hence a UFD, we have $a = p^m u$ for some positive integer m and unit u. Thus $(a) = (p^m)$. Finally, if a belongs to (p^m) for every $m \geq 1$, then p^m divides a for all $m \geq 1$. Again using unique factorization, we must have $a = 0$. (Note that if a is a unit, so is p, a contradiction.)

9. Let R be a subring of the field K. The integral closure $\overline{R}$ of R in K is the intersection of all valuation rings V of K such that $V \supseteq R$.

If $a \in \overline{R}$, then a is integral over R, hence over any valuation ring $V \supseteq R$. But V is integrally closed by Property 4, so $a \in V$. Conversely, assume $a \notin \overline{R}$. Then a fails to belong to the ring $R' = R[a^{-1}]$. (If a is a polynomial in a^{-1}, multiply by a sufficiently high power of a to get a monic equation satisfied by a.) Thus a^{-1} cannot be a unit in R'. (If $ba^{-1} = 1$ with $b \in R'$, then $a = a1 = aa^{-1}b = b \in R'$, a contradiction.) It follows that a^{-1} belongs to a maximal ideal $\mathcal{M}'$ of R'. Let C be an algebraic closure of the field $k = R'/\mathcal{M}'$, and let h be the composition of the canonical map $R' \to R'/\mathcal{M}' = k$ and the inclusion $k \to C$. By (3.1.4), h has a maximal extension to $\overline{h} : V \to C$ for some valuation ring V of K containing $R' \supseteq R$. Now $\overline{h}(a^{-1}) = h(a^{-1})$ since $a^{-1} \in \mathcal{M}' \subseteq R'$, and $h(a^{-1}) = 0$ by definition of h. Consequently $a \notin V$, for if $a \in V$, then

$$1 = \overline{h}(1) = \overline{h}(aa^{-1}) = \overline{h}(a)\overline{h}(a^{-1}) = 0,$$

a contradiction. The result follows.

10. Let R be an integral domain with fraction field K. Then R is integrally closed if and only if $R = \cap_\alpha V_\alpha$, the intersection of some (not necessarily all) valuation rings of K.

The "only if" part follows from Property 9. For the "if" part, note that each V_α is integrally closed by Property 4, hence so is R. (If a is integral over R, then a is integral over each V_α, hence a belongs to each V_α, so $a \in R$.) ♣

3.3 Discrete Valuation Rings

3.3.1 Definitions and Comments

An *absolute value* on a field K is a mapping $x \to |x|$ from K to the real numbers, such that for every $x, y \in K$,
1. $|x| \geq 0$, with equality if and only if $x = 0$;
2. $|xy| = |x|\ |y|$;
3. $|x + y| \leq |x| + |y|$.

The absolute value is *nonarchimedean* if the third condition is replaced by a stronger version:
$3'$. $|x + y| \leq \max(|x|, |y|)$.
As expected, *archimedean* means not nonarchimedean.

The familiar absolute values on the reals and the complex numbers are archimedean. However, our interest will be in nonarchimedean absolute values. Here is where most of them come from.

A *discrete valuation* on K is a surjective map $v : K \to \mathbb{Z} \cup \{\infty\}$, such that for every $x, y \in K$,
(a) $v(x) = \infty$ if and only if $x = 0$;
(b) $v(xy) = v(x) + v(y)$;
(c) $v(x + y) \geq \min(v(x), v(y))$.

A discrete valuation induces a nonarchimedean absolute value via $|x| = c^{v(x)}$, where c is a constant with $0 < c < 1$.

3.3.2 Examples

We can place a discrete valuation on all of the fields of Subsection 3.1.3. In Examples 1 and 2, we take $v(p^r m/n) = r$. In Example 3, $v(f/g) = \deg g - \deg f$. In Example 4, $v(\sum_{i=r}^{\infty} a_i x^i) = r$ (if $a_r \neq 0$).

3.3.3 Proposition

If v is a discrete valuation on the field K, then $V = \{a \in K : v(a) \geq 0\}$ is a valuation ring with maximal ideal $\mathcal{M} = \{a \in K : v(a) \geq 1\}$.

Proof. The defining properties (a), (b) and (c) of (3.3.1) show that V is a ring. If $a \notin V$, then $v(a) < 0$, so $v(a^{-1}) = v(1) - v(a) = 0 - v(a) > 0$, so $a^{-1} \in V$, proving that V is a valuation ring. Since a is a unit of V iff both a and a^{-1} belong to V iff $v(a) = 0$, $\mathcal{M}$ is the ideal of nonunits and is therefore the maximal ideal of the valuation ring V. ♣

3.3.4 Definitions and Comments

Discrete valuations do not determine all valuation rings. An arbitrary valuation ring corresponds to a generalized absolute value mapping into an ordered group rather than the real numbers. We will not consider the general situation, as discrete valuations will be entirely adequate for us. A valuation ring V arising from a discrete valuation v as

in (3.3.3) is said to be a *discrete valuation ring*, abbreviated DVR. An element $t \in V$ with $v(t) = 1$ is called a *uniformizer* or *prime element*. (Note that uniformizers exist by surjectivity of v.) A uniformizer tells us a lot about the DVR V and the field K.

3.3.5 Proposition

Let t be a uniformizer in the discrete valuation ring V. Then t generates the maximal ideal $\mathcal{M}$ of V, in particular, $\mathcal{M}$ is principal. Conversely, if t' is any generator of $\mathcal{M}$, then t' is a uniformizer.

Proof. Since $\mathcal{M}$ is the unique maximal ideal, $(t) \subseteq \mathcal{M}$. If $a \in \mathcal{M}$, then $v(a) \geq 1$, so $v(at^{-1}) = v(a) - v(t) \geq 1 - 1 = 0$, so $at^{-1} \in V$, and consequently $a \in (t)$. Now suppose $\mathcal{M} = (t')$. Since $t \in \mathcal{M}$, we have $t = ct'$ for some $c \in V$. Thus

$$1 = v(t) = v(c) + v(t') \geq 0 + 1 = 1,$$

which forces $v(t') = 1$. ♣

3.3.6 Proposition

If t is a uniformizer, then every nonzero element $a \in K$ can be expressed uniquely as $a = ut^n$ where u is a unit of V and $n \in \mathbb{Z}$. Also, $K = V_t$, that is, $K = S^{-1}V$ where $S = \{1, t, t^2, \dots\}$.

Proof. Let $n = v(a)$, so that $v(at^{-n}) = 0$ and therefore at^{-n} is a unit u. To prove uniqueness, note that if $a = ut^n$, then $v(a) = v(u) + nv(t) = 0 + n = n$, so that n, and hence u, is determined by a. The last statement follows by Property 1 of Section 3.2 and the observation that the elements of V are those with valuation $n \geq 0$. ♣

A similar result holds for ideals.

3.3.7 Proposition

Every nonzero proper ideal I of the DVR V is of the form $\mathcal{M}^n$, where $\mathcal{M}$ is the maximal ideal of V and n is a unique nonnegative integer. We write $v(I) = n$; by convention, $\mathcal{M}^0 = V$.

Proof. Choose $a \in I$ such that $n = v(a)$ is as small as possible. By (3.3.6), $a = ut^n$, so $t^n = u^{-1}a \in I$. By (3.3.5), $\mathcal{M} = (t)$, and therefore $\mathcal{M}^n \subseteq I$. Conversely, let $b \in I$, with $v(b) = k \geq n$ by minimality of n. As in the proof of (3.3.6), bt^{-k} is a unit u', so $b = u't^k$. Since $k \geq n$ we have $b \in (t^n) = \mathcal{M}^n$, proving that $I \subseteq \mathcal{M}^n$. The uniqueness of n is a consequence of Nakayama's lemma. If $\mathcal{M}^r = \mathcal{M}^s$ with $r < s$, then $\mathcal{M}^r = \mathcal{M}^{r+1} = \mathcal{M}\mathcal{M}^r$. Thus $\mathcal{M}^r$, hence $\mathcal{M}$, is 0, contradicting the hypothesis that I is nonzero. ♣

We may interpret $v(I)$ as the length of a composition series.

3.3.8 Proposition

Let I be a nonzero proper ideal of the discrete valuation ring R. Then $v(I) = l_R(R/I)$, the composition length of the R-module R/I.

Proof. By (3.3.7), we have $R \supset \mathcal{M} \supset \mathcal{M}^2 \supset \cdots \supset \mathcal{M}^n = I$, hence

$$R/I \supset \mathcal{M}/I \supset \mathcal{M}^2/I \supset \cdots \supset \mathcal{M}^n/I = 0.$$

By basic properties of composition length, we have, with $l = l_R$,

$$l(R/I) = l(\frac{R/I}{\mathcal{M}/I}) + l(\mathcal{M}/I) = l(R/\mathcal{M}) + l(\frac{\mathcal{M}/I}{\mathcal{M}^2/I}) + l(\mathcal{M}^2/I).$$

Continuing in this fashion, we get

$$l(R/I) = \sum_{i=0}^{n-1} l(\mathcal{M}^i/\mathcal{M}^{i+1}).$$

Since $\mathcal{M}$ is generated by a uniformizer t, it follows that $t^i + \mathcal{M}^{i+1}$ generates $\mathcal{M}^i/\mathcal{M}^{i+1}$. Since $\mathcal{M}^i/\mathcal{M}^{i+1}$ is annihilated by $\mathcal{M}$, it is an $R/\mathcal{M}$-module, that is, a vector space, over the field $R/\mathcal{M}$. The vector space is one-dimensional because the $\mathcal{M}^i$, $i = 0, 1, \ldots, n$, are distinct [see the proof of (3.3.7)]. Consequently, $l(R/I) = n$. ♣

We are going to prove a characterization theorem for DVR's, and some preliminary results will be needed.

3.3.9 Proposition

Let I be an ideal of the Noetherian ring R. Then for some positive integer m, we have $(\sqrt{I})^m \subseteq I$. In particular (take $I = 0$), the nilradical of R is nilpotent.

Proof. Since R is Noetherian, $\sqrt{I}$ is finitely generated, say by $a_1, \ldots, a_t$, with $a_i^{n_i} \in I$. Then $(\sqrt{I})^m$ is generated by all products $a_1^{r_1} \cdots a_t^{r_t}$ with $\sum_{i=1}^t r_i = m$. Our choice of m is

$$m = 1 + \sum_{i=1}^{t} (n_i - 1).$$

We claim that $r_i \geq n_i$ for some i. If not, then $r_i \leq n_i - 1$ for all i, and

$$m = \sum_{i=1}^{t} r_i < 1 + \sum_{i=1}^{t} (n_i - 1) = m,$$

a contradiction. But then each product $a_1^{r_1} \cdots a_t^{r_t}$ is in I, hence $(\sqrt{I})^m \subseteq I$. ♣

3.3.10 Proposition

Let $\mathcal{M}$ be a maximal ideal of the Noetherian ring R, and let Q be any ideal of R. The following conditions are equivalent:

1. Q is $\mathcal{M}$-primary.
2. $\sqrt{Q} = \mathcal{M}$.
3. For some positive integer n, we have $\mathcal{M}^n \subseteq Q \subseteq \mathcal{M}$.

Proof. We have (1) implies (2) by definition of $\mathcal{M}$-primary; see (1.1.1). The implication (2) $\Rightarrow$ (1) follows from (1.1.2). To prove that (2) implies (3), apply (3.3.9) with $I = Q$ to get, for some positive integer n,

$$\mathcal{M}^n \subseteq Q \subseteq \sqrt{Q} = \mathcal{M}.$$

To prove that (3) implies (2), observe that by (1.1.1),

$$\mathcal{M} = \sqrt{\mathcal{M}^n} \subseteq \sqrt{Q} \subseteq \sqrt{\mathcal{M}} = \mathcal{M}. \ \clubsuit$$

Now we can characterize discrete valuation rings.

3.3.11 Theorem

Let R be a Noetherian local domain with fraction field K and unique maximal ideal $\mathcal{M} \neq 0$. (Thus R is not a field.) The following conditions are equivalent:
1. R is a discrete valuation ring.
2. R is a principal ideal domain.
3. $\mathcal{M}$ is principal.
4. R is integrally closed and every nonzero prime ideal is maximal.
5. Every nonzero ideal is a power of $\mathcal{M}$.
6. The dimension of $\mathcal{M}/\mathcal{M}^2$ as a vector space over $R/\mathcal{M}$ is 1.

Proof.

(1) $\Rightarrow$ (2): This follows from (3.3.7) and (3.3.5).
(2) $\Rightarrow$ (4): This holds because a PID is integrally closed, and a PID is a UFD in which every nonzero prime ideal is maximal.
(4) $\Rightarrow$ (3): Let t be a nonzero element of $\mathcal{M}$. By hypothesis, $\mathcal{M}$ is the only nonzero prime ideal, so the radical of (t), which is the intersection of all prime ideals containing t, coincides with $\mathcal{M}$. By (3.3.10), for some $n \geq 1$ we have $\mathcal{M}^n \subseteq (t) \subseteq \mathcal{M}$, and we may assume that $(t) \subset \mathcal{M}$, for otherwise we are finished. Thus for some $n \geq 2$ we have $\mathcal{M}^n \subseteq (t)$ but $\mathcal{M}^{n-1} \not\subseteq (t)$. Choose $a \in \mathcal{M}^{n-1}$ with $a \notin (t)$, and let $\beta = t/a \in K$. If $\beta^{-1} = a/t \in R$, then $a \in Rt = (t)$, contradicting the choice of a. Therefore $\beta^{-1} \notin R$. Since R is integrally closed, β^{-1} is not integral over R. But then $\beta^{-1}\mathcal{M} \not\subseteq \mathcal{M}$, for if $\beta^{-1}\mathcal{M} \subseteq \mathcal{M}$, then β^{-1} stabilizes a finitely generated R-module, and we conclude from the implication (4) $\Rightarrow$ (1) in (2.1.4) that β^{-1} is integral over R, a contradiction.

Now $\beta^{-1}\mathcal{M} \subseteq R$, because $\beta^{-1}\mathcal{M} = (a/t)\mathcal{M} \subseteq (1/t)\mathcal{M}^n \subseteq R$. (Note that $a \in \mathcal{M}^{n-1}$ and $\mathcal{M}^n \subseteq (t)$.) Thus $\beta^{-1}\mathcal{M}$ is an ideal of R, and if it were proper, it would be contained in $\mathcal{M}$, contradicting $\beta^{-1}\mathcal{M} \not\subseteq \mathcal{M}$. Consequently, $\beta^{-1}\mathcal{M} = R$, hence $\mathcal{M}$ is the principal ideal (β).
(3) $\Rightarrow$ (2): By hypothesis, $\mathcal{M}$ is a principal ideal (t), and we claim that $\cap_{n=0}^{\infty}\mathcal{M}^n = 0$. Suppose that a belongs to $\mathcal{M}^n$ for all n, with $a = b_n t^n$ for some $b_n \in R$. Then $b_n t^n = b_{n+1}t^{n+1}$, hence $b_n = b_{n+1}t$. Thus $(b_n) \subseteq (b_{n+1})$ for all n, and in fact $(b_n) = (b_{n+1})$ for sufficiently large n because R is Noetherian. Therefore $b_n = b_{n+1}t = ctb_n$ for some $c \in R$, so $(1 - ct)b_n = 0$. But $t \in \mathcal{M}$, so t is not a unit, and consequently $ct \neq 1$. Thus b_n must be 0, and we have $a = b_n t^n = 0$, proving the claim.

Now let I be any nonzero proper ideal of R. Then $I \subseteq \mathcal{M}$, but by the above claim we have $I \not\subseteq \cap_{n=0}^{\infty}\mathcal{M}^n$. Thus there exists $n \geq 0$ such that $I \subseteq \mathcal{M}^n$ and $I \not\subseteq \mathcal{M}^{n+1}$.

Choose $a \in I \setminus \mathcal{M}^{n+1}$; since $\mathcal{M}^n = (t)^n = (t^n)$, we have $a = ut^n$ with $u \notin \mathcal{M}$ (because $a \notin \mathcal{M}^{n+1}$). But then u is a unit, so $t^n = u^{-1}a \in I$. To summarize, $I \subseteq \mathcal{M}^n = (t^n) \subseteq I$, proving that I is principal.
(2) $\Rightarrow$ (1): By hypothesis, $\mathcal{M}$ is a principal ideal (t), and by the proof of (3) $\Rightarrow$ (2), $\cap_{n=0}^{\infty}\mathcal{M}^n = 0$. Let a be any nonzero element of R. Then $(a) \subseteq \mathcal{M}$, and since $\cap_{n=0}^{\infty}\mathcal{M}^n = 0$, we will have $a \in (t^n)$ but $a \notin (t^{n+1})$ for some n. Thus $a = ut^n$ with $u \notin \mathcal{M}$, in other words, u is a unit. For fixed a, both u and n are unique (because t, a member of $\mathcal{M}$, is a nonunit). It follows that if β is a nonzero element of the fraction field K, then $\beta = ut^m$ uniquely, where u is a unit of R and m is an integer, possibly negative. If we define $v(\beta) = m$, then v is a discrete valuation on K with valuation ring R.
(1) $\Rightarrow$ (5): This follows from (3.3.7).
(5) $\Rightarrow$ (3): As in the proof of (3.3.7), $\mathcal{M} \neq \mathcal{M}^2$. Choose $t \in \mathcal{M} \setminus \mathcal{M}^2$. By hypothesis, $(t) = \mathcal{M}^n$ for some $n \geq 0$. We cannot have $n = 0$ because $(t) \subseteq \mathcal{M} \subset R$, and we cannot have $n \geq 2$ by choice of t. The only possibility is $n = 1$, hence $\mathcal{M} = (t)$.
(1) $\Rightarrow$ (6): This follows from the proof of (3.3.8).
(6) $\Rightarrow$ (3): By hypothesis, $\mathcal{M} \neq \mathcal{M}^2$, so we may choose $t \in \mathcal{M} \setminus \mathcal{M}^2$. But then $t + \mathcal{M}^2$ is a generator of the vector space $\mathcal{M}/\mathcal{M}^2$ over the field $R/\mathcal{M}$. Thus $R(t+\mathcal{M}^2)/\mathcal{M}^2 = \mathcal{M}/\mathcal{M}^2$. By the correspondence theorem, $t + \mathcal{M}^2 = \mathcal{M}$. Now $\mathcal{M}(\mathcal{M}/(t)) = (\mathcal{M}^2 + (t))/(t) = \mathcal{M}/(t)$, so by NAK, $\mathcal{M}/(t) = 0$, that is, $\mathcal{M} = (t)$. ♣.

Note that surjectivity of a discrete valuation [see (3.3.1)] excludes the *trivial valuation* $v(a) = 0$ for every $a \neq 0$.

3.3.12 Corollary

The ring R is a discrete valuation ring if and only if R is a local PID that is not a field. In particular, since R is a PID, it is Noetherian.

Proof. The "if" part follows from (2) implies (1) in (3.3.11). For the "only if" part, note that a discrete valuation ring R is a PID by (1) implies (2) of (3.3.11); the Noetherian hypothesis is not used here. Moreover, R is a local ring by Property 3 of Section 3.2. If R is a field, then every nonzero element $a \in R$ is a unit, hence $v(a) = 0$. Thus the valuation v is trivial, a contradiction. ♣

3.3.13 Corollary

Let R be a DVR with maximal ideal $\mathcal{M}$. If $t \in \mathcal{M} \setminus \mathcal{M}^2$, then t is a uniformizer.

Proof. This follows from the proof of (5) implies (3) in (3.3.11). ♣