Discrete valuation rings

Definition. Let K be a field. A **discrete valuation** on K is a surjective function $v\colon K \to \mathbb{Z} \cup \{\infty\}$ satisfying properties

(1) For all $x, y \in K \setminus \{0\}$, we have $v(xy) = v(x) + v(y)$.
(2) For all $x, y \in K \setminus \{0\}$ such that $x+y \neq 0$, we have $v(x+y) \geq \min(v(x), v(y))$.
(3) $v(x) = \infty \Leftrightarrow x = 0$.

Remark. The element ∞ is a symbol such that for every $n \in \mathbb{Z}$ we have $n \leq \infty$ and $n + \infty = \infty$. By axiom (3), a valuation v is specified by giving its value for all $x \neq 0$.

Example. Let p be a prime. The field $\mathbb{Q}$ admits an valuation v_p defined as follows. Every rational number $x \neq 0$ can be written as $x = p^a \frac{q}{r}$, where $q, r \in \mathbb{Z}$ are not divisible by p. We then define $v_p(x) = a$. It is easy to see that this is well-defined and that $v_p(xy) = v_p(x) + v_p(y)$. Given $x = p^a \frac{q}{r}$ and $y = p^{a'} \frac{q'}{r'}$, we may assume WLOG that $a \leq a'$. We then have

$$x + y = p^a \left(\frac{q}{r} + \frac{p^{a'-a} q'}{r'} \right) = p^a \frac{r'q + p^{a'-a} q'}{rr'}.$$

Writing $r'q + p^{a'-a} q' = p^b q''$ with q'' not divisible by p, we have

$$v_p(x + y) = v_p \left(p^{a+b} \frac{q''}{rr'} \right) = a + b \geq a = \min(v_p(x), v_p(y)).$$

Example. Let k be a field. For every $\alpha \in k$, the field $k(x)$ admits a valuation v_α defined by the "order of vanishing at α".

Every $h \in k(x)$ can be written as $h = (x - \alpha)^n \frac{f}{g}$, where f and g are polynomials such that $f(a), g(a) \neq 0$, and $n \in \mathbb{Z}$. We then define $v_\alpha(h) = n$, and check similarly to the case of $\mathbb{Z}$ that this is a valuation.

If $k = \mathbb{C}$, we may interpret an $h \in \mathbb{C}(x)$ as an analytic function with singularities on $\mathbb{C}$, and then

$$v_\alpha(h) = \begin{cases} \text{the order of vanishing of } h \text{ if } h \text{ defined at } \alpha \\ -\text{the order of the polo of } h \text{ otherwise .} \end{cases}$$

Lemma. *If v is a valuation on K and $x \in K \setminus \{0\}$, then*

(1) $v(1) = v(-1) = 0$
(2) $v(-x) = v(x)$.
(3) $v(x^{-1}) = -v(x)$.
(4) *The set*

$$A = \{x \in K \mid v(x) \geq 0\}$$

is a subring of K.

Proof. (1): We have

$$v(1) = v(1^2) = v(1) + v(1),$$

which implies $v(1) = 0$. Then

$$0 = v(1) = v((-1)^2) = v(-1) + v(-1)$$

gives $v(-1) = 0$.

(2): We have $v(-x) = v((-1)x) = v(-1) + v(x) = v(x)$.

(3): We have $0 = v(1) = v(xx^{-1}) = v(x) + v(x^{-1})$, giving $v(x-1) = -v(x)$.
(4): We have $v(0) = \infty \geq 0$ and $v(1) = 0 \geq 0$, so $0, 1 \in A$. If $x, y \in A$, then

$$v(xy) = v(x) + v(y) \geq 0 + 0 = 0,$$

so $xy \in A$. We also have

$$v(x + y) \geq \min(v(x), v(y)) \geq \min(0, 0) = 0,$$

so $x + y \in A$. Finally if $x \in A$, then $v(-x) = v(x) \geq 0$, so $-x \in A$, which proves that A is a subring of K. □

Definition. Let A be an integral domain, with fraction field K. We say that A is a **discrete valuation ring** (or **DVR**), if there exists some valuation v on K such that for $x \in K$ we have

$$x \in A \Leftrightarrow v(x) \geq 0.$$

Remark. If v is a valuation on a field K, then the set $\{x \in K \mid v(x) \geq 0\}$ is easily seen to be a subring of K. In other words, every field equipped with a valuation contains a DVR determined by the valuation.

Example. For the valuation v_p on $\mathbb{Q}$, the associated discrete valuation ring consists of fractions of the form $p^a \frac{q}{r}$ where $a \geq 0$ and p divides neither q nor r. Equivalently, setting $m' = p^a m$, we see that it consists of all fractions m'/n such that p does not divide n, which is precisely the ring $\mathbb{Z}_{(p)} \subset \mathbb{Q}$.

Example. For the valuation $v(x^n f/g) = n$, the associated DVR is $k[x]_{(x)} \subset k(x)$.

Example. Let k be a field, and let $k((x))$ be the ring of formal Laurent series, i.e. whose elements are formal sums

$$\sum_{i \geq n} a_i x^i,$$

where $n \in \mathbb{Z}$ (so finitely many terms $a_i x^i$ with $i < 0$ are allowed). One can check that this is a field. Setting $v(f) = i$, where i is the smallest integer such that $a_i \neq 0$, we get a discrete valuation on $k((x))$, with associated DVR the ring of formal power series $k[[x]] \subset k((x))$.

Lemma. *Let A be a discrete valuation ring with fraction field K and discrete valuation v. Let $x, y \in A$. Then*

$$v(x) \geq v(y) \Leftrightarrow (x) \subseteq (y)$$

and

$$v(x) = v(y) \Leftrightarrow (x) = (y)$$

Proof. The case where x or y is 0 is easy, so assume $x, y \neq 0$. If $v(x) \geq v(y)$, then $v(xy^{-1}) = v(x) + v(y^{-1}) = v(x) - v(y) \geq 0$, so $xy^{-1} \in A$. It follows that $x = (xy^{-1})y$, so $x \in (y)$ and hence $(x) \subseteq (y)$. Conversely, if $(x) \subseteq (y)$, then $x \in (y)$, so there is some $a \in A$ such that $x = ay$. We get $v(x) = v(ay) = v(a) + v(y) \geq 0 + v(y) = v(y)$.

The second equivalence of the lemma follows easily from the first. □

Theorem. *Let A be a discrete valuation ring with fraction field K and discrete valuation v. Then*

(1) *The ring A is local, with maximal ideal*

$$\mathfrak{m} = \{x \in A \mid v(x) > 0\}.$$

(2) *There is an element $x \in A$ such that $v(x) = 1$, and for any such x, we have $\mathfrak{m} = (x)$.*
(3) *With x as in the previous point, the ideals of A are (0) and (x^k) for $k \geq 0$.*
(4) *A has dimension 1.*
(5) *A is integrally closed.*

Proof. (1) Let $x \in A$. Then x is a unit if and only if $(x) = (1)$, which is if and only if $v(x) = v(1) = 0$. Thus the set of non-units is precisely

$$\mathfrak{m} = \{x \in A \mid v(x) > 0\}.$$

It is easy to check that $\mathfrak{m}$ is an ideal, and hence that A is local with maximal ideal $\mathfrak{m}$.

(2) Since v is assumed surjective, there is some $x \in K$ with $v(x) = 1$. By definition of A, we have $x \in A$. By definition of $\mathfrak{m}$, we have $x \in \mathfrak{m}$ and so $(x) \in \mathfrak{m}$. If $y \in \mathfrak{m}$, then $v(y) \geq 1 = v(x)$, so $y \in (x)$. Hence $\mathfrak{m} \subseteq (x)$, so $\mathfrak{m} = (x)$.

(3) Let $\mathfrak{a} \subseteq A$ be an ideal. If $\mathfrak{a} \neq (0)$, let $k = \min_{y \in \mathfrak{a}} v(y)$. For any $y \in \mathfrak{a}$, we have $v(y) \geq k = v(x^k)$, so $y \in (x^k)$, and hence $\mathfrak{a} \subseteq (x^k)$. There is some $y \in \mathfrak{a}$, with $v(y) = k = v(x^k)$, hence $(y) = (x^k)$. Since

$$(y) \subseteq \mathfrak{a} \subseteq (x^k),$$

we must then have $(x^k) = \mathfrak{a}$.

(4) By the previous two points, we have that the ideals of A are $(1), (x), (x^2), \cdots$ and (0). If $k \geq 2$, then

$$1 = v(x) < v(x^k) = k,$$

so $x \notin (x^k)$. Since $x^k \in (x^k)$, the ideal (x^k) is not prime. Hence (x) and (0) are the only prime ideals of A, so A has dimension 1.

(5) Let $x \in K$, and assume that x is integral over A. We must show that $x \in A$.
Since x is integral over A, we can find a relation.

$$x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0, \qquad a_i \in A$$

so

$$x^n = -a_{n-1}x^{n-1} - \cdots - a_0.$$

If $v(x) = d$, we then get

$$\begin{aligned} v(x^n) = nv(x) = nd &= v(-a_{n-1}x^{n-1} - \cdots - a_0) \\ &\geq \min_i (v(-a_i x^i)) \end{aligned}$$

Thus there exists an $i \leq n-1$ such that

$$nd = v(x^d) \geq v(-a_i x^i) = v(-a_i) + v(x^i) \geq id,$$

This gives $(n-i)d \geq 0$, and so $d \geq 0$. Hence $x \in A$.

□

In fact, most of these properties characterise DVRs (among Noetherian local domains of dimension 1).

Proposition. *Let A be a Noetherian, local integral domain of dimension 1. The following are equivalent:*

(1) *A is a DVR.*
(2) *A is integrally closed.*
(3) *$\mathfrak{m}$ is principal.*
(4) *$\mathfrak{m}/\mathfrak{m}^2$ is a 1-dimensional $A/\mathfrak{m}$-module.*
(5) *There exists an $x \in A$ such that every ideal in A is of the form (x^k).*

Proof. We have already seen that (1) implies (2), (3), (5) and (6).

Let us prove do a few of the easier other implications.

(3) $\Rightarrow$ (4): Assume $\mathfrak{m} = (x)$. Then $x \neq 0$, since otherwise $\mathfrak{m} = (0)$, which means $\dim A = 0$.

We have $(x^2) \subseteq (x)$, and we claim this inclusion is strict. If not, we would have $x \in (x^2)$, which means $x = ax^2$ for some $a \in A$. Since A is an integral domain and $x \neq 0$, this implies that $1 = ax$, so x is a unit, which contradicts $x \in \mathfrak{m}$. Hence $\mathfrak{m}/\mathfrak{m}^2 = (x)/(x^2) \neq 0$, and so $\dim_{A/\mathfrak{m}} \mathfrak{m}/\mathfrak{m}^2$. On the other hand, $\mathfrak{m}/\mathfrak{m}^2$ is generated as an $A/\mathfrak{m}$-module by $x + \mathfrak{m}^2$, so $\dim_{A/\mathfrak{m}} \mathfrak{m}/\mathfrak{m}^2 \leq 1$ and so $\dim_{A/\mathfrak{m}} \mathfrak{m}/\mathfrak{m}^2 = 1$.

(4) $\Rightarrow$ (3): If $\mathfrak{m}/\mathfrak{m}^2$ is 1-dimensional, there is some $x \in \mathfrak{m}$ such that $x + \mathfrak{m}^2$ generates $\mathfrak{m}/\mathfrak{m}^2$. But $\mathfrak{m}$ is finitely generated, since A is Noetherian, and then Nakayama's lemma says that x generates $\mathfrak{m}$.

(3) $\Rightarrow$ (5): There is an x such that $\mathfrak{m} = (x)$, so that every non-unit in A is of the form ax for some $a \in A$. Assume for a contradiction that $\mathfrak{a}$ is an ideal which is not of the form (x^k), and let it be maximal among ideals with this property (there is such a maximal one since A is Noetherian). We have

$$\mathfrak{a} = (y_1, \ldots, y_n) = (a_1 x, \cdots, a_n x) = (a_1, \cdots, a_n)(x).$$

Now $\mathfrak{a} = (a_1, \ldots, a_n)(x) \subseteq (a_1, \ldots, a_n)$. If $\mathfrak{a} = (a_1, \ldots, a_n)$, we have $\mathfrak{a} = (x)\mathfrak{a}$, which by Nakayama's lemma implies $\mathfrak{a} = (0)$.

Otherwise $\mathfrak{a} \subsetneq (a_1, \ldots, a_n)$, which by the maximality property of $\mathfrak{a}$ implies that $(a_1, \ldots, a_n) = (x^k)$ for some k. But then $\mathfrak{a} = (x)(x^k) = (x^{k+1})$, contradicting the defining property of $\mathfrak{a}$.

(5) $\Rightarrow$ (1): For every $y \neq 0$, we have $\sqrt{(y)} = \mathfrak{m} = (x)$. It then follows that $y \in (x^k)$ for some k, and we take a minimal such. Then define $v(y) = k$, and extend this multiplicatively to the fraction field of A. $\square$

Note that the above proof is incomplete, in that we have omitted any implication from (2) to the other ones.