Valuation rings

Definition 1 ([AK2017, 23.1])**.** A *discrete valuation* on a field K is a surjective function

$$v : K^\times \to \mathbb{Z}$$

such that for every $x, y \in K^\times$,

(1) $v(xy) = v(x) + v(y)$,
(2) $v(x + y) \geq \min\{v(x), v(y)\}$ if $x \neq -y$.

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

is called the *discrete valuation ring* of v. A *discrete valuation ring*, or *DVR*, is a ring which is a valuation ring of a discrete valuation.

Example 2.

(1) The field $\mathbb{C}((t)) = \{\sum_{n=N}^{\infty} a_n t^n \mid N \in \mathbb{N}, a_n \in \mathbb{C}\}$ of Laurent series without an essential singularity at $t = 0$ is the protypical example of a discrete valution ring. The valuation $v : \mathbb{C}((t)) \to \mathbb{Z}$ sends a series $f(t) = \sum_{n=N}^{\infty} a_n t^n$ with $a_N \neq 0$ to N. That is, $v(f)$ is the order of the zero of f at $0 \in \mathbb{C}$ (or minus the order of the pole) when f is considered as a meromorphic function on some neighbourhood of $0 \in \mathbb{C}$. This can be generalised to any field k by defining

$$k((t)) = \{\sum_{n=N}^{\infty} a_n t^n \mid N \in \mathbb{N}, a_n \in k\}.$$

(2) Moreover, if A contains a field k in such a way that $k \to A/\langle\pi\rangle$ is an isomorphism for $\pi \in A$ with $v(\pi) = 1$, then one can show that there is an induced inclusion of fields $K \subset k((t))$, and the valuation of K is induced by that of $k((t))$. We do not always have such a subfield $k \subset A$, as we shall soon see. However, by defining $k = A/\langle\pi\rangle$ and choose a splitting of *sets* $\sigma : k \subset A$, we can construct an inclusion of *sets* $K \subset k((t))$ induced by v, σ, and π.

(3) Any irreducible polynomial $f(x_1, \ldots, x_n) \in \mathbb{C}[x_1, \ldots, x_n]$ defines a discrete valuation v_f on the field $\mathbb{C}(x_1, \ldots, x_n) = \operatorname{Frac} \mathbb{C}[x_1, \ldots, x_n]$ as follows. For a nonzero $g \in \mathbb{C}(x_1, \ldots, x_n)$ write $g = f^N \frac{g_0}{g_1}$ with $g_0, g_1 \in \mathbb{C}[x_1, \ldots, x_n]$ polynomials not divisible by f. Then the order of g is N. In other words, $v_f(g)$ is the order of the zero (or minus the order of the pole) of g along the subvariety $\{a \in \mathbb{C}^n \mid f(a) = 0\}$.

Exercise: Describe the valuation of $\mathbb{C}(t)$ associated to t.

(4) Every discrete valuation on $\mathbb{C}(t)$ is of the form v_{t-a} for some $a \in \mathbb{C}$ except one: $v_\infty(\frac{f_0}{f_1}) = \deg f_1 - \deg f_0$. Extending $\mathbb{C}$ to an analytic variety $\mathbb{CP}^1$ by adjoining a "point at infinity", every element of $\mathbb{C}(t)$ extends to a meromorphic function on $\mathbb{CP}^1$ and v_∞ measures the order of the zero (or minus the order of the pole) at infinity.

This is a general principle: For any field extension K of $\mathbb{C}$ of transcendence degree one there is a bijection between the discrete valuations v of K with $v(\mathbb{C}) = 0$, and the points of the corresponding Riemann surface.

(5) Any subring of the valuation ring $\mathbb{C}[[t]]$ of $\mathbb{C}((t))$ not contained in $\mathbb{C}[[t]]^\times$ inherits a discrete valuation. For example, if $\gamma(t) \in \mathbb{C}[[t]]$ is any power

series which does not satisfy an algebraic equation in $\mathbb{C}[t](X)$ (for example $\gamma(t) = e^t - 1 = \sum_{n=1}^{\infty} \frac{t^n}{n!}$), then $x \mapsto t, y \mapsto \gamma(t)$ defines a monomorphism $\mathbb{C}(x,y) \subset \mathbb{C}((t))$, and we get an induced discrete valuation on $\mathbb{C}(x,y)$. Heuristically, this measures the order of the zero (or minus the order of the pole) of an element of $\mathbb{C}(x,y)$ along the graph $\{(a, \gamma(a)) \in \mathbb{C}^2 \mid a \in \mathbb{C}\}$ of $\gamma(t)$.

(6) Here is an arithmetic analogue of the example (2). Let $p \in \mathbb{Z}$ be a prime. Given $x \in \mathbb{Q}$, write $x = p^N \frac{a}{b}$ with a, b prime to p. Then define $v_p(x) = N$. Then v_p is a discrete valuation whose valuation ring is the localisation $\mathbb{Z}_{(p)}$ of $\mathbb{Z}$ at p.

(7) More generally, if $K \subset \mathbb{C}$ is a finite algebraic extension of $\mathbb{Q}$, and $\mathcal{O}_K$ is the normalisation of $\mathbb{Z}$ in K, then every local ring of $\mathcal{O}_K$ (except K) is a discrete valuation ring.

(8) Here is an arithmetic analoque of example (1). Let $p \in \mathbb{Z}$ be a prime. The p-adic numbers $\mathbb{Q}_p$ admit a unique discrete valuation. Its valuation ring is the ring of p-adic integers.

(9) More generally, if $K/\mathbb{Q}_p$ is a finite algebraic extension, then there is a unique extension of the discrete valuation $v_{\mathbb{Q}_p}$ of $\mathbb{Q}_p$ to a valuation v_K on K. Note that we may have $v_K \circ \iota = e \cdot v_{\mathbb{Q}_p}$ for some $e \in \mathbb{N}$ where $\iota : \mathbb{Q}_p \to K$ is the inclusion. In this case we say K is ramified.

Definition 3. An integral domain A is called a *valuation ring* if for every element $a \in (\operatorname{Frac} A)^\times$, we have $a \in A$ or $a^{-1} \in A$.

Example 4. Consider $\mathbb{C}(x) = \operatorname{Frac} \mathbb{C}[x]$. For $f \in \mathbb{C}[x]$ define

$$v_x(f) = \max\{i \text{ such that } x^i | f\}$$

and for $f/g \in \mathbb{C}(x)$ define $v_x(f/g) = v_x(f) - v_x(g)$.

Consider $\mathbb{C}(x,y) = \operatorname{Frac} \mathbb{C}[x,y]$. For $f \in \mathbb{C}[x,y]$ define

$$v_y(f) = \max\{i \text{ such that } y^i | f\}$$

and for $f/g \in \mathbb{C}(x,y)$ define $v_y(f/g) = v_y(f) - v_y(g)$.

Next, for any $f \in \mathbb{C}(x,y)$, note that $y^{-v(f)} f \in \mathbb{C}[x,y]_{(y)}$ and so $y^{-v(f)} f$ has a well defined image in $\mathbb{C}(x) \cong \mathbb{C}[x,y]_{(y)}/y\mathbb{C}[x,y]_{(y)}$. Define

$$v'_x(f) = v_x(y^{-v(f)} f).$$

Finally, consider

$$A = \left\{ f \in \mathbb{C}(x,y) \;\middle|\; \begin{array}{l} v_y(f) > 0, \text{ or} \\ v_y(f) = 0 \text{ and } v'_x(f) \geq 0 \end{array} \right\}$$

This is a valuation ring such that $\mathbb{C}(x,y)^\times / A^\times \cong \mathbb{Z} \times \mathbb{Z}$. One integer measures the order of the zero along $V(y) = \mathbb{C} \times \{0\} \subset \mathbb{C}^2$ (or minus the order of the pole), and the other integer measures the order of the zero (or minus the order of the pole) of the residue at $(0,0) \in \mathbb{C}^2$ (i.e., after the zero or pole along $V(y)$ has been removed by multiplying with y^n for some n). Note, if we give $\mathbb{Z} \times \mathbb{Z}$ the lexicographical order, then it becomes a totally ordered set, and $(A - \{0\})/A^\times$ is the preimage of the elements greater than zero.

Lemma 5. *For any discrete valuation v on a field K with valuation ring A, we have*

$$A^\times = v^{-1}(0).$$

Consequently, v induces an isomorphism $K^\times/A^\times \cong \mathbb{Z}$ with $(A-\{0\})/A^\times \cong \mathbb{N}$. In particular, every DVR is a valuation ring.

Proof. An easy exercise using the fact $v(x^{-1}) = -v(x)$. □

The converse is true as well. So the valuation is actually unnecessary information. Everything is determined by the ring structure of A.

Lemma 6. *A valuation ring A with fraction field K is a discrete valuation ring if and only if the quotient group $K^\times/A^\times$ is isomorphic to $\mathbb{Z}$.*

Proof. We have already observed the "only if" so we prove the "if". Suppose that A is a valuation ring and $\phi : K^\times/A^\times \cong \mathbb{Z}$. Note $(A-\{0\})/A^\times$ is a submonoid, so either $\phi((A-\{0\})/A^\times) \subset \mathbb{N}$ or $\phi((A-\{0\})/A^\times) \subset -\mathbb{N}$. If the latter is the case, replace ϕ with $-\phi$. We claim that $\phi^{-1}(\mathbb{N}) = (A-\{0\})/A^\times$, and the composition $v : K^\times \to K^\times/A^\times \to \mathbb{Z}$ is a discrete valuation.

We clearly have $v(ab) = v(a)+v(b)$ for every $a, b \in K^\times$. In particular, $v(a^{-1}) = -v(a)$. Suppose that $a \in K^\times$ has $v(a) \in \mathbb{N}$. Either $a \in A$ or $a^{-1} \in A$. The latter would imply that $-n \in \mathbb{N}$ since $\phi((A-\{0\})/A^\times) \subset \mathbb{N}$, so we must have $a \in A$, and we have proven the claim that $\phi^{-1}(\mathbb{N}) = (A-\{0\})/A^\times$. In particular, we now know that $v(a) \geq 0$ if and only if $a \in A-\{0\}$. Consider $a, b \in K^\times$, and, without loss of generality, suppose that $\frac{a}{b} \in A$ (so $\min\{v(a), v(b)\} = v(b)$). Then also $\frac{a}{b}+1 = \frac{a+b}{b} \in A$, so $v(a+b) \geq v(b) = \min\{v(a), v(b)\}$. □

Definition 7. Recall that a domain A is said to be *normal* if given any $a \in \operatorname{Frac} A$, if $f(a) = 0$ for some monic $f(X) \in A[X]$, then $a \in A$.

Lemma 8. *Every valuation ring is normal. Every valuation ring is a local ring.*

Proof. Let A be the valuation ring and $K = \operatorname{Frac} A$.

A is normal: Let $f(X) = X^{d+1} + \sum_{0\leq i\leq d} a_i X^i$ be a monic in $A[X]$, and $b \in K$ an element such that $f(b) = 0$. If $b \in A$ we are done, so suppose $b^{-1} \in A$. But since $f(b) = 0$ the element $-\sum_{0\leq i\leq d} a_i b^i/b^d = b^{d+1}/b^d = b$ is also in A.

A is local: We will show that the set $A-A^\times$ of non-units is an ideal. If $a \in A-A^\times$ and $b \in A$, then clearly $ab \in A-A^\times$ since otherwise $a^{-1} = b(ab)^{-1} \in A$. Let $a, b \in A-A^\times$. Without loss of generality, suppose that $\frac{a}{b} \in A$. If $a+b \in A^\times$, then $(\frac{a}{b}+1)\frac{1}{a+b} = \frac{a+b}{b}\frac{1}{a+b} = \frac{1}{b} \in A$. A contradiction. □

Theorem 9. *Let A be a subring of a field K. The following are equivalent.*

1. *A is a valuation ring.*
2. *The set of principal ideals of A is totally ordered by inclusion.*
3. *The set of ideals of A is totally ordered by inclusion.*
4. *A is a local ring and every finitely generated ideal of A is principal.*

Proof.

(1) ⇒ (2) Recall that the set of principal ideals of a domain A is in canonical bijection with $A-\{0\}/A^\times$. Define a partial order on $K^\times/A^\times$ by $a \leq b$ if $b/a \in A-\{0\}/A^\times$. Then the definition of a valuation ring implies that this is a total order.

(2) ⇒ (3) Now suppose that $I, J \subset A$ are ideals with $I \not\subset J$. Choose some $a \in I$ which is not in J, and let b be any element of J. Since $a \notin J$, $a \notin (b)$, and so $(b) \subset (a) \subset I$. Since this is true for any $b \in J$, we see that $J \subset I$.

(3) $\Rightarrow$ (4) Since the ideals are totally ordered, the maximal ideal which exists by Zorn's Lemma is unique. By induction it suffices to show that ideals generated by two elements are principal. Suppose that $I = \langle f, g\rangle$ is such an ideal. Either $(f) \subset (g)$ or $(g) \subset (f)$, so $I = (f)$ or (g).

(4) $\Rightarrow$ (1) Let $a, b \in A - \{0\}$, and let $\mathfrak{m}$ be the maximal ideal. Since $I = \langle a, b\rangle$ is principal, $I/\mathfrak{m}I$ is a one dimensional $A/\mathfrak{m}$-vector space, so there are $c, d \in A$ with $ac = bd$ with at least one of c, d not in $\mathfrak{m}$, i.e., at least one of c, d is a unit (since A is local $A^\times = A - \mathfrak{m}$). Say c is the unit. Then $d/c = a/b \in A$. □

The totally ordered set $K^\times/A^\times$ we associated to a valuation ring in the previous proof ($a \leq b$ if $b/a \in (A - \{0\}/A^\times)$ contains even more information than we might expect.

Lemma 10. *Let A be a valuation ring. Then the map $v : A - \{0\} \to K^\times/A^\times$ induces a bijection between the ideals of A, and the "right-closed" proper subsets of $(A - \{0\})/A^\times$. I.e., those subsets S which satisfy $\gamma \in S, \gamma \leq \gamma' \implies \gamma' \in S$.*

To make the notation easier, define $\Gamma = K^\times/A^\times \cup \{\infty\}$ with $\gamma \leq \infty$ for all $\gamma \in K^\times/A^\times$ and extend v to $K/A^\times$ defining $v(0) = \infty$. The bijection is then given by:

$$I \mapsto v(I)$$
$$v^{-1}S \hookleftarrow S$$

Warning: this does not imply by any means that all ideals are principal. For example, we may have $K^\times/A^\times \cong \mathbb{Q}$ or $\mathbb{R}$ or indeed, any subgroup of $\mathbb{R}$.

Proof. For $\gamma \in \Gamma$, we will write $\Gamma_{\geq\gamma}$ for $\{\gamma \in \Gamma \mid \gamma \leq \gamma'\}$.

Let I be an ideal. Let us show that $v(I)$ is "right closed". Suppose $\gamma, \gamma' \in \Gamma$ are non-infinite elements with $\gamma \in v(I)$ and $\gamma' \geq \gamma$. Clearly, $v : A - \{0\} \to (A - \{0\})/A^\times = \Gamma_{\geq 0}$ is surjective. Choose $a, a' \in A$ such that $v(a) = \gamma$ and $v(a') = \gamma'$. Then $\gamma' \geq \gamma$ implies $a'/a \in A$, so $a' = \frac{a'}{a}a \in I$, and therefore $\gamma' = v(a') \in v(I)$. Now we show that $v^{-1}v(I) = I$. Choose $a, b \in A$ such that $a \in I$ and $v(a) = v(b)$. Then $b/a \in A$, so $b = a\frac{b}{a} \in I$.

Let $S \subset \Gamma_{\geq 0}$ be a non-empty "right-closed" proper subset. We claim that $v^{-1}S$ is an ideal. Indeed, for any $a \in A$, $b \in v^{-1}S$, we have $v(ab) \geq v(b)$ since $\frac{ab}{b} \in A$, so $ab \in v^{-1}S$. Moreover, consider $a, b \in v^{-1}S$ and suppose that $v(a) \geq v(b)$. Then $a/b \in A$ so $a/b + 1 = \frac{a+b}{b} \in A$, so $v(a+b) \geq v(b)$, so $a + b \in v^{-1}S$ since S is "right-closed". The fact $v(v^{-1}(S)) = S$ follows directly from the fact that $A \to \Gamma_{\geq 0}$ is surjective. □

Corollary 11. *A DVR is a PID. More specficially, if $\mathfrak{m} = \langle\pi\rangle$, then all ideals of the DVR are of the form $\mathfrak{m}^n = \langle\pi^n\rangle$.*

Proof. We have seen above that if A is a DVR, then $A - \{0\}/A^\times$ is isomorphic to $\mathbb{N}$. Then we notice that the "right-closed" proper subsets of $\mathbb{N}$ are all of the form $\mathbb{N}_{\geq n}$, and therefore correspond to ideals $\langle a\rangle$ with $v(a) = n$. □

Lemma 12. *Let A be a ring. The following conditions are equivalent.*

(1) Every ascending chain of ideals stabilisers.
(2) Every ideal is finitely generated.

Proof. (1) $\Rightarrow$ (2). Let I be an ideal. Choose elements $a_0 \in I$, $a_1 \in I - \langle a_0 \rangle, a_2 \in I - \langle a_0, a_1 \rangle$, etc. Since the chain $\langle a_0 \rangle \subset \langle a_0, a_1 \rangle \subset \langle a_0, a_1, a_2 \rangle \subset \dots$ stabilises, we must have $I = \langle a_0, \dots, a_n \rangle$ for some n. That is I is finitely generated.

(2) $\Rightarrow$ (1). Let $I_0 \subset I_1 \subset I_2 \subset \dots$ be an ascending chain of ideals. The union is also an ideal, and finitely generated by assumption so $\cup_{n \geq 0} I_n = \langle f_1, \dots, f_m \rangle$ for some f_i. But then there must exist some I_i which contains all $f_1, \dots, f_m$. Hence, the chain stabilises. □

Definition 13. Recall that a ring is *noetherian* if it satisfies the equivalent conditions of Lemma 12.

Definition 14. Recall that the *dimension* of a ring is the length n of the longest chain $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_n$ of prime ideals. A local ring of dimension n is said to be *regular* if its maximal ideal $\mathfrak{m}$ can be generated by n elements.

In particular, a local domain has dimension 1 if and only if the set of prime ideals is $\{\langle 0 \rangle, \mathfrak{m}\}$, and a local domain of dimension 1 is regular if and only if $\mathfrak{m}$ is principal.

We will use the following.

Proposition 15 ([AK2017, Proposition 10.14])**.** *Let R be a ring, R' an R-algebra, and $x \in R'$, the following are equivalent.*

(1) x satisfies a monic in $R[X]$.
(2) There exists an $R[x]$-module M which is finitely generated over R, and has $\mathrm{Ann}_R(M) = 0$.

Theorem 16 ([Atiyah-Macdonald, Proposition 9.2], [AK2017, Theorem 23.6])**.** *The following are equivalent.*

(1) A is a DVR.
(2) A is a normal noetherian local ring of dimension 1.
(3) A is a regular noetherian local ring of dimension 1.

Proof.

(1) $\Rightarrow$ (2) We have seen above that every DVR is a valuation ring (Lemma 5) and therefore normal (Lemma 8). Moreover, we know all the ideals of a PID are of the form $\mathfrak{m}^n$ (Lemma 11), so the only two primes are $\mathfrak{m}$ and $\langle 0 \rangle$ (i.e., it has dimension 1), and the ascending chain condition is easily checked to hold.

(2) $\Rightarrow$ (3) To get from normal to regular, we want to find some $\frac{a}{b} \in K$ whose integrality implies that $\mathfrak{m}$ is principal. First we claim that there is $b, a \in A$ such that $b \in \mathfrak{m}$, and $a\mathfrak{m} \subset \langle b \rangle$. Indeed, if we can find such a, b, then $\frac{a}{b}\mathfrak{m} \subset A$. Our second claim is that normality implies this inclusion is in fact a bijection. That is, $1 \in \frac{a}{b}\mathfrak{m}$. This second claim implies that there is $t \in \mathfrak{m}$ such that $\frac{a}{b}t = 1$, and therefore $\mathfrak{m} = \langle t \rangle$, since any $c \in \mathfrak{m}$ can be written as $c\frac{a}{b}t$ and $c\frac{a}{b} \in A$.

Let us prove the first claim (this is usually an easy consequence of the theory of depth, or the theory of primary decomposition, but we do it by hand). Certainly, we can find a nonzero $b \in \mathfrak{m}$ because $\dim A > 0$. But then $A/\langle b \rangle$ has a single prime, say $\mathfrak{n}$, since the primes of $A/\langle b \rangle$ are in canonical bijection with the primes of A containing b. Let I be the largest ideal such that $I = \mathrm{Ann}(a')$ for some nonzero $a' \in A/\langle b \rangle$. But I is

prime, since given $c, d \in A/\langle b\rangle$ with $cd \in \mathrm{Ann}(a')$, $d \notin \mathrm{Ann}(a')$, we have $c \in \mathrm{Ann}(da') \supset \mathrm{Ann}(a')$, and this inclusion must be equality by maximality of $\mathrm{Ann}(a')$. Since $\mathfrak{n}$ is the only prime, we deduce that $\mathfrak{n} = \mathrm{Ann}(a')$. Then any lifting $a \in A$ of $a' \in A/\langle b\rangle$ satisfies $a\mathfrak{m} \subset \langle b\rangle$. Note $a' \neq 0$ so $a \notin \langle b\rangle$; this will come up soon.

Now we prove the second claim. If 1 is not in $\frac{a}{b}\mathfrak{m}$, then we have $\frac{a}{b}\mathfrak{m} \subset \mathfrak{m}$. But then the finitely generated A-module $\mathfrak{m}$ admits a $A[\frac{a}{b}]$-module structure. Since $\mathrm{Ann}_A(\mathfrak{m}) = 0$, Proposition 15 implies then that $\frac{a}{b}$ is in the integral closure of A. But A is normal, so this implies that $\frac{a}{b} \in A$, contradicting $a = b\frac{a}{b} \notin \langle b\rangle$.

(3) $\Rightarrow$ (1) First we claim that

$$(*) \qquad \bigcap_{n\in\mathbb{N}} \mathfrak{m}^n = 0.$$

Indeed, since A is noetherian, this intersection is a finitely generated ideal. So it is a finitely generated module M such that $\mathfrak{m}M = M$. Nakayama's Lemma then implies that it is zero.

Now let t be an element such that $\mathfrak{m} = \langle t\rangle$ (so $\mathfrak{m}^n = \langle t^n\rangle$). Since $\cap_{n\in\mathbb{N}}\mathfrak{m}^n = 0$, every nonzero element a of A can be written uniquely as $a = ut^n$ for some unit u. Explicitly, n is the largest integer such that $a \in \mathfrak{m}^n \setminus \mathfrak{m}^{n+1}$, and $u = \frac{a}{t^n}$ is in $A^\times$ because mutliplication by t^n induces an isomorphism of A-modules

$$A/\mathfrak{m} \xrightarrow{\sim} \mathfrak{m}^n/\mathfrak{m}^{n+1}$$

(or rather, multiplication by t^{-n} induces an isomorphism $\mathfrak{m}^n/\mathfrak{m}^{n+1} \xrightarrow{\sim} A/\mathfrak{m}$). Indeed, we can even say that every element of $K^\times$ can be written uniquely as ut^n for some $n \in \mathbb{Z}$ and $u \in A^\times$. Now one checks readily that for any $a \in K^\times$, we have $a \in A$ or $a^{-1} \in A$, and furthermore, $A/\langle t\rangle \cong \mathbb{Z}$. (Alternatively, we could have checked that $ut^n \mapsto n$ satisfies the axioms of a discrete valuation).

□