Valuation rings

Theorem 1. Let R be a commutative domain with quotient field K. Then the following conditions on R are equivalent:

(1) For any $q \in K$ either $q \in R$ or $q^{-1} \in R$.
(2) Let $a, b \in R$ be non-zero elements. Then either $a|b$ or $b|a$ (in R).
(3) The set of ideals of R are linearly ordered.

EXERCISE 1 - Prove Theorem 1.

Definition Any ring satisfying the above conditions is called a *valuation ring*.

Theorem 2. A valuation ring is integrally closed.

Proof. Let V be a valuation ring. We will use condition 1 of Theorem 1. Let $K = \mathrm{Frac}(V)$ and let $u \in K$ be integral over V. Then

$$u^n + a_{n-1}u^{n-1} + \ldots + a_0 = 0 \qquad *$$

for some $a_i \in V$. We may as well assume that $u \notin V$. Thus by condition 1 of Theorem 1, we have that $u^{-1} \in V$ and it is not a unit of V. Thus $u^{-1} \in M$ the unique maximal ideal of V. Multiply $*$ by u^{-n} and we get

$$1 + a_{n-1}u^{-1} + \ldots + a_0u^{-n} = 0$$

Since $u^{-1} \in M$, by rearranging terms, we see that $1 \in M$, a contradiction. Thus $u \in V$. Done $\square$

Finding valuation rings

Let G be an abelian group under addition which is totally ordered by $\leq$. It is called an *ordered group* if the axiom

$$x \geq y,\ z \geq t \Rightarrow x + z \geq y + t$$

is satisfied. This axiom implies
(1) $x > 0,\ y \geq 0 \Rightarrow x + y > 0$ and
(2) $x \geq y \Rightarrow -y \geq -x$

Examples of ordered groups:

(1) $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ under addition with the usual ordering.

(2) the product $\mathbb{Z}^n$ of n copies of $\mathbb{Z}$ with lexicographic ordering, that is

$$(a_1, a_2, \ldots, a_n) < (b_1, b_2, \ldots, b_n) \Leftrightarrow$$

for some $i, b_1 = a_1, b_2 = a_2, \ldots, b_i = a_i$ and $b_{i+1} > a_{i+1}$

(3) Let $G_1, G_2, \ldots, G_n$ be any set of ordered groups. Then using the lexicographic ordering as above makes $G_1 \times G_2 \times \cdots \times G_n$ into an ordered group.

We make $G \cup \{\infty\}$ into an ordered set by declaring ∞ to be bigger than any element of G. We also make the convention that $g + \infty = \infty$ for all $g \in G \cup \{\infty\}$. The *positive elements* of G, are those $g \in G$, such that $g > 0$.

Definition. Let K be a field. A map $\upsilon : K \to G \cup \{\infty\}$ is called a *valuation* if it satisfies the following conditions for all $x, y \in K$.

(1) $\upsilon(xy) = \upsilon(x) + \upsilon(y)$
(2) $\upsilon(x + y) \geq \min\{\upsilon(x), \upsilon(y)\}$
(3) $\upsilon(x) = \infty \Leftrightarrow x = 0$

Note: The following statements follow from the definition of a valuation. Let υ and K be as above, Then

(1) $\upsilon(1) = 0$
(2) $\upsilon(x^{-1}) = -\upsilon(x)$, for all $x \in K$.

If we let K^* denote the non-zero elements of K, then by (1) υ defines a group homomorphism $K^* \to G$. The image of this map is an ordered subgroup of G called the value group of υ.

Theorem 3. Let K and υ be as above. Let $R_\upsilon = \{x \in K | \upsilon(x) \geq 0\}$ and $M_\upsilon = \{x \in K | \upsilon(x) > 0\}$. Then the following statements hold:

(1) R_υ is a ring, in fact a valuation ring.
(2) M_υ is an ideal of R_υ, in fact the maximal ideal of R_υ.
(3) The set $U = \{x \in K | \upsilon(x) = 0\}$ is precisely the set of units of R_υ.

EXERCISE 2 - Prove Theorem 3.

Example 1: Fix $p \in \mathbb{Z}$ a prime number. For $a \in \mathbb{Z}$ let $n_p(a)$ be the highest power of p that divides a. Let $\mathbb{Q}$ be the field of rational numbers and define $\upsilon_p : \mathbb{Q} \to \mathbb{Z} \cup \{\infty\}$ via $\upsilon_p(a/b) = n_p(a) - n_p(b)$. Then n_p is a valuation on $\mathbb{Q}$.

EXERCISE 3 - Describe the ring R_{υ_p}.

We see that any ring derived from a valuation on a field as above is a valuation ring. Next we show the converse, namely every valuation ring is derived from a valuation on its quotient field.

Theorem 4. Let R satisfy the equivalent conditions of Theorem 1. Then $R = R_v$ for some valuation v on the quotient field of R.

Proof. Let K denote the quotient field of R. We first need an ordered group to serve as the value group. Consider the set G of cyclic R-submodules of K (i.e., submodules of K of the form qR for some $q \in K$). Let $x, y \in K$. We define a (multiplicative) binary operation on this set on this set via $(xR) * (yR) = xyR$. This makes G into an abelian group with identity element R; the inverse of xR is $x^{-1}R$). We put an ordering on G by taking the *reverse ordering* under inclusion! Thus we define $xR \leq yR$ if and only if $yR \subseteq xR$. Since R satisfies the equivalent conditions of Theorem 3, this puts a total ordering on the elements of G (any two cyclic submodules are comparable, since either x/y or y/x is in R. Thus either $(x/y)R \subseteq R$ or $(y/x)R \subseteq R$). It is not difficult to check that this satisfies the axiom needed to make G an ordered group. That is if $xR \geq yR$, $zR \geq tR$, then $(xR)(zR) \geq (yR)(tR)$). Since ordering is determined by containment, this is easy. The valuation mapping v from K to $G \cup \{\infty\}$ is the obvious one, namely $v(x) = xR$, for $x \neq 0$, while $v(0) = \infty$. It is straightforward to show that this mapping satisfies the three conditions. □

EXERCISE 5 - Show that $R = R_v$.

A dimension 2 example

Let k be any field and let K be the quotient field of $k[x, y]$. Let $G = \mathbb{Z}^2$ with the lexicographic ordering. We will define a valuation on K as follows. First define v on the monomials of K by sending $y^i x^j \mapsto (i, j)$ (note $x \mapsto (0, 1)$, the minimal positive element of G). Extend this to all polynomials in x, y by sending $f \mapsto \min\{v(Z)\}$ where Z runs through all monomials in the terms of f (remember, the image of v is the ordered group G). Finally, we extend v to all of K by defining $v(f/g) = v(f) - v(g)$, for polynomials f and g. Then v is a valuation on K. The ring R_v is difficult to describe precisely. However, we can say the following:

Theorem 5. The ring R_v above has exactly two non-zero prime ideals which are:

(1) $M_v = \{h = f/g \in K : v(h) = v(f) - v(g) \geq (0, 1)\}$. Furthermore $M_v = (x)$; and
(2) $P = \{h = f/g \in R_v : v(h) = v(f) - v(g) \geq (0, n)$, for all integers $n\}$. This ideal is infinitely generated.

Note $(1, m) > (0, n)$ for any integers (positive or negative) m and n.

Proof. (1) Since $(0, 1)$ is the minimal positive element, M_v is as described. (Note, if G does not have a minimal positive element, for example if $G = \mathbb{Q}$, then M_v is not principal.) To see that M_v is generated by x, let $h \in M_v$. Thus $v(h) > 0$, and so $v(h) \geq (0, 1)$. Hence $v(h/x) \geq 0$. Hence $h/x \in R_v$. Thus $h = x(h/x) \in (x)$. Since the reverse inclusion is clear, we have that $M_v = (x)$.

(2) First we show that P is a prime ideal. Suppose that $f, g \in R_v$ and that neither f nor g is in P. Then by definition, there exists integers n, m such that $v(f) < (0, n)$ and $v(g) < (0, m)$. We may assume that $n \geq m$. Thus $v(fg) = v(f) + v(g) < (0, 2n)$. Hence $fg \notin P$, which proves that P is prime.

Before we show that P is not finitely generated, we make the observation that if $g \in R_v$ is in the ideal generated by the elements $g_1, \ldots, g_n$, then from the definition of a valuation, $v(g) \geq \inf\{v(g_1), \ldots v(g_n)\}$. Now suppose that P is generated by the elements $\{g_1, \ldots, g_n\}$. Without loss of generality we may assume that $v(g_1) = \inf\{v(g_1), \ldots, v(g_n)\}$. Since $v(g_1) > (0, n)$ all integers n, we have that $v(g_1/x) > (0, n)$ for all integers n. Thus $g_1/x \in P$. However, $v(g_1/x) < v(g_1)$. Therefore, by our choice of g_1 it is clear from our observation that $g_1/x \notin (g_1, \ldots, g_n)$ - a contradiction. Thus P is infinitely generated. □

Clearly the ring R_v above is not Noetherian. In fact one can show that a valuation ring R is Noetherian if and only if the value group of R is $\mathbb{Z}$. In which case the ring is a local PID.