Lecture 20 Discrete valuation rings

Def Let K be a field. A discrete valuation on K is a surjective function $v : K \to \mathbb{Z} \cup \{\infty\}$ s.t.

1) $\forall\, x, y \in K \setminus 0 \quad v(xy) = v(x) + v(y)$

2) $\forall\, x, y \in K \setminus 0$ s.t. $v(x+y) \geq \min(v(x), v(y))$

3) $v(x) = \infty \iff x = 0$.

Example k field $K = k(x)$ rational functions. "order of vanishing at $\alpha \in k$" is a valuation. Fix $\alpha \in k$

$$h = (x-\alpha)^n \frac{f(x)}{g(x)} \qquad f(\alpha), g(\alpha) \neq 0.$$

define $v_\alpha(h) = n$. $v_\alpha(0) := \infty$.

Check 1) $h_1, h_2 \in k(x)$

$$h_1 h_2 = (x-\alpha)^{n_1+n_2} \cdot \frac{f_1(x) f_2(x)}{g_1(x) g_2(x)}.$$

$$\nu(h_1 h_2) = n_1 + n_2 = \nu(h_1) + \nu(h_2).$$

2) Suppose $n_1 \leq n_2$

$$h_1 + h_2 = (x-\alpha)^{n_1} \left(\frac{f_1(x)}{g_1(x)} + (x-\alpha)^{n_2-n_1} \frac{f_2(x)}{g_2(x)} \right)$$

if $n_2 > n_1$ the brackets don't vanish.

if $n_2 = n_1$ we might have $\frac{f_1(\alpha)}{g_1(\alpha)} - \frac{f_2(\alpha)}{g_2(\alpha)} = 0$.

$$\Rightarrow \nu(h_1+h_2) \geq n_1 = \min(\nu(h_1), \nu(h_2)).$$

3) set $\nu(0) = \infty$. every $h \neq 0$ has some "order of vanishing".

Expanding $h(x)$ as a Laurent series at α we obtain:

$$h(x) = \sum_{k=\nu(h)}^{\infty} a_k (x-\alpha)^k \qquad a_{\nu(h)} \neq 0.$$

Example 2 Let p be prime. $K = \mathbb{Q}$.

$\forall\ x \neq 0$ can be written $x = p^a \frac{q}{r}$ $q, r \in \mathbb{Z}$ and $p \nmid q, r$.

Define $\nu_p(x) = a$. $\nu_p(0) = \infty$.

$x = p^a \frac{q}{r}$ $\quad y = p^b \frac{t}{s}$ $\quad p \nmid q, r, t, s$.

then $\nu_p(xy) = a + b = \nu_p(x) + \nu_p(y)$.

Suppose $\min(a, b) = a$

$$\nu_p(x+y) = p^a \left(\frac{q}{r} + p^{b-a} \frac{t}{s} \right) = p^a \left(\frac{sq + p^{b-a} rt}{rs} \right)$$

$p \nmid rs$ but we may have $p \mid sq + p^{b-a} rt$

So $v_p(x+y) \geq \min\{v_p(x), v_p(y)\}$.

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) $R = \{x \in K \mid v(x) \geq 0\}$ is a subring.

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

$\Rightarrow v(-1) = v(1) = 0$.

2) $v(-x) = v(-1) + v(x) = v(x)$.

3) $0 = v(1) = v(x x^{-1}) = v(x) + v(-x)$
$\Rightarrow v(x) = -v(x^{-1})$

4) $v(0) = \infty \geq 0$ and $v(1) = 0 \geq 0$
So $0, 1 \in R$

If $x, y \in R$ then

$$v(x+y) \geq \min\{v(x), v(y)\} \geq 0.$$

So $x+y \in R$

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

Also $v(-x) = v(x)$ so $-x \in R$.

We have a subring. □

Definition Let R be an integral domain and K its field of fractions.

R is a DVR (discrete valuation ring) if $\exists\ v : K \to \mathbb{Z} \cup \{\infty\}$ valuation s.t. $R = \{x \in K \mid v(x) \geq 0\}$.

Examples 1) $K = k(x)$ and $v_\alpha : K \to \mathbb{Z} \cup \{\infty\}$

The DVR is

$$\{ f \mid v_\alpha(f) \geq 0 \} = k[x]_{(x-\alpha)}.$$

where $m_\alpha = (x-\alpha)$ max ideal.

2) $K = \mathbb{Q}$ $\quad v_p : \mathbb{Q} \to \mathbb{Z} \cup \{\infty\}$.

$$\{ \underset{\| }{x} \mid v_p(x) \geq 0 \} = \mathbb{Z}_{(p)}$$ localisation at (p).

$p^a \frac{n}{s}$ $\quad a \geq 0$. prime

3) $k((t))$ the field of formal power series

$f = \sum_{i \geq k} a_i t^i$. $\quad a_n \neq 0$ $\quad$ let $v(f) = k$

Remark $\quad \frac{k\{\{t\}\}}{k((t))} \Rightarrow f = \sum_{i \geq k} a_i t^{i/n}$ Puiseux series.

k alg. closed $\mathrm{char}(k) = 0$.

Lemma R be a DVR with fraction field K and discrete valuation v. Let $x, y \in R$ then

1) $v(x) \geq v(y) \iff (x) \subseteq (y)$
2) $v(x) = v(y) \iff (x) = (y)$.

Proof Enough to show 1).

If $x, y = 0$ then $v = \infty$ and easy to show.

Suppose $x, y \neq 0$. If $v(x) \geq v(y)$ then $v(xy^{-1}) = v(x) + v(y^{-1}) = v(x) - v(y) \geq 0$ so $xy^{-1} \in R$ so $x = (xy^{-1})y$ and $x \in (y) \Rightarrow (x) \subseteq (y)$.

if $(x) \subseteq (y)$ then $x \in (y) \Rightarrow x = ry$ and so $v(x) = v(r) + v(y) \Rightarrow v(x) \geq v(y)$

Theorem Let R be a DVR with fraction field K and valuation v.

1) R is local and the maximal ideal is $\mathfrak{m} = \{x \in R \mid v(x) > 0\}$.

2) There is an element $x \in R$ s.t. $v(x) = 1$ and for any such x $\mathfrak{m} = (x)$.

3) The ideals of R are (0) and (x^k) $v(x) = 1$. ($\Leftrightarrow$ R is a P.I.D)

4) A has dimension 1

5) A is integrally closed

Proof 1) Suppose $x \in R$ is a unit $\Leftrightarrow$ $(x) = (1) \Leftrightarrow v(x) = v(1) = 0 \Leftrightarrow x \notin \mathfrak{m}$

$\mathfrak{m}$ consists of non-units

Show $\mathfrak{m}$ is an ideal

1) $0 \in \mathfrak{m}$ since $v(0) = \infty$

2) $x, y \in \mathfrak{m}$ then $v(x+y) \geq \min v(x), v(y)$
> 0

so $x+y \in \mathfrak{m}$

3) $r \in R$ $x \in \mathfrak{m}$ then $v(rx) = v(r) + v(x)$
≥ 0.

$rx \in \mathfrak{m}$.

Hence R is local with max ideal $\mathfrak{m}$,

2) we assume v is surjective so

$\exists\ x \in R$ s.t. $v(x) = 1$ and $x \in \mathfrak{m}$

so $(x) \subset \mathfrak{m}$. If $y \in \mathfrak{m}$ then $v(y) \geq v(x)$

so $(y) \subset (x)$ so $(x) = \mathfrak{m}$.

3) Let $I \subseteq R$ be an ideal. If $I \neq 0$

let $k = \min_{y \in I} v(y)$. Then for any

$y \in I \quad v(y) \geq k = v(x) \Rightarrow (y) \subseteq (x^k)$

$\Rightarrow I \subseteq (x^k)$. Moreover, there must exist some $y \in I$ with $v(y) = k$. and $v(x^k) = v(y) \iff (x^k) = (y)$.

Since $(y) \subseteq I \subseteq (x^k)$ we have $I = (x^k)$.

4) By previous the ideals are $(1)\ (x)\ (x^2) \ldots (0)$. If $k \geq 2$ then $1 = v(x) < v(x^k) = k$ so $x \in (x^k)$ hence (x^k) is not prime we have $(x) \geq (0)$ are the only prime ideals $\dim R = 1$.

5) Jules will discuss integral closure. on wednesday.

Corollary A DVR is Noetherian.

Proposition R is a local Noetherian integral domain of dimension 1

TFAE.

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

Proof We've already shown $1 \Rightarrow 2, 4$

We show $2 \Leftrightarrow 3$.

Suppose $\mathfrak{m} = (x)$ then $x \neq 0$ since $\dim = 1$

we have $(x^2) \subseteq (x)$. If $x \in (x^2)$ then $x = rx^2$ since R is an integral domain $\Rightarrow 1 = rx$ so x is a unit and $m = (1)$ $\Rightarrow\Leftarrow$ So $m/m^2 \neq 0$ so $\dim m/m^2 > 0$. As an R/m-module m/m^2 is generated by $x + m^2$ so $\dim_{R/m} m/m^2 \leq 1$. $\Rightarrow \dim = 1$.

$3 \Rightarrow 2$ If $\dim m/m^2 = 1$ there is an x s.t. $x + m^2$ generates m/m^2. But m is finitely generated since R is Noetherian so Nakayama's lemma says x generates m.

$2 \Rightarrow 4$ Suppose $\mathfrak{m} = (x)$ so every non-unit is rx for some $r \in R$.

Consider the set of ideals not of the form (x^k) and let I be the maximal (R Noetherian).

Then I is finitely generated and

$$I = (y_1, \ldots, y_n) = (a_1 x, \ldots, a_n x) = (a_1, \ldots a_n)(x)$$

Now $(a_1, \ldots a_n)(x) \subseteq (a_1, \ldots, a_n)$.

If equality then by Nakayama's lemma $I\mathfrak{m} = I \Rightarrow I = 0$.

Otherwise $I \subsetneq (a_1, \ldots a_n)$ and by maximality of I we have $(a_1, \ldots a_n) = (x^k)$

But then $I = (x^k)(x) = (x^{k+1})$.

4 ⇒ 1 For every $y \neq 0$ $y \in R$ we have $(y) = (x^k)$ for some k.

Define $v(y) = k$, and extend multiplicatively to the fraction field.

□.

Appendix Review of Nakayama's Lemma

M finitely generated module / R and $I \subseteq R$ ideal. If $IM \subseteq M$ then there exists $i \in I$ s.t. $im = m$ $\forall m \in M$.

"$IM = M \Longrightarrow \exists\ i$ s.t. $im = m$ $\forall m \in M$"

Local version If R is local with max ideal m and M finitely generated R mod. then $mM = M \Rightarrow M = 0$

Corollary R local and M finitely generated. If $m_i \in M$ are such that $\phi(m_i)$ are a basis of $M/\mathfrak{m}M$, then m_i generate M.