Discrete valuation rings

<u>Def</u> A discrete valuation ring (DVR) is a principal ideal domain R that has only one non-zero prime ideal m.

Note: R DVR $\Rightarrow$ $\operatorname{Spec} R = \{(0), m\}$, m is maximal. If $x \in R \setminus m$ then x is invertible (otherwise x would be contained in the maximal ideal m)

So $R^\times = R \setminus m$.

Since R is PID, $m = (u)$ for some $u \in R$, u is called <u>uniformizer</u>

If u' is another uniformizer, then $u' = u \cdot a$, $a \in R^\times$.

The field R/m is called <u>residue field</u> of the DVR R.

<u>Lemma 13.5</u> If R is a DVR, then

$$\bigcap_{n \geq 0} m^n = (0).$$

Proof let $I = \bigcap_{n\geq 0} m^n = (x)$ since R is PID. But $m \cdot I = \bigcap_{n\geq 1} m^n = I$ because $R \supset m \supset m^2 \supset \dots$

hence $x \in m \cdot I = (u \cdot x)$ where u is a uniformizer $\Rightarrow x = uxa$ for some $a \in R \Rightarrow x(1-ua) = 0$

$\Rightarrow x = 0$ becaus $ua \neq 1$ (u is not invertible) $\square$

From this lemma $\Rightarrow \forall 0 \neq x \in R$ $\exists n \geq 0$ s.t. $x \in m^n \setminus m^{n+1}$, then

$x = u^n \cdot a$ where $a \notin m$, i.e. $a \in R^*$

Cor. In a DVR R any $0 \neq x \in R$ can be written as $x = u^n a$ for some $n \geq 0$, $a \in R^\times$, where u is a uniformizer. The exponent n does not depend on the choice of a uniformizer

Denote $n = \nu(x)$

Let F be the fraction field of R

Then the elements of F are of the form

$$\frac{x}{y} = \frac{u^{\nu(x)}\cdot a}{u^{\nu(y)}\cdot b} = u^{\nu(x)-\nu(y)} a b^{-1}$$

So $F^{\times} = \{u^n a \mid n \in \mathbb{Z},\ a \in R^{\times}\}$

ν extend to a group homomorphism

$\nu : F^{\times} \longrightarrow \mathbb{Z}$, s.t.

1) ν is surjective (because $\nu(u)=1$)

2) $\forall x,y \in F^{\times}$ s.t. $x+y \neq 0$ we have

$$\nu(x+y) \geq \min\{\nu(x), \nu(y)\}$$

<u>Proof of 2)</u>: $x = u^{\nu(x)}\cdot a$, $y = u^{\nu(y)} b$

let for example $\nu(x) \leq \nu(y)$, then

$$x+y = u^{\nu(x)}\left(a + u^{\nu(y)-\nu(x)} b\right)$$

Then $c = a + u^{\nu(y)-\nu(x)} b \in R$, $c \neq 0$, so

we have $c = u^{\nu(c)}\cdot d$, $d \in R^{\times}$, $\nu(c) \geq 0$

Then $x+y = u^{\nu(x)+\nu(c)} d$

$$\nu(x+y) = \nu(x) + \nu(c) \geq \nu(x) \qquad \square$$

<u>Def</u> The function ν is called the <u>valuation</u> of the DVR R.

Rem 1) it is convenient to extend ν to F by defining formally $\nu(0)=+\infty$. Then the condition 2) above is simply

$$\forall x,y\in F \qquad \nu(x+y)\geq \min\{\nu(x),\nu(y)\}$$

2) If F is a field with a function ν satisfying the properties 1) and 2) above, then

$$R=\{x\in F \mid \nu(x)\geq 0\} \text{ is a DVR}$$

(exercise)

Example $\mathbb{Z}_{(p)}=R$ is a DVR

$\mathfrak{m}=(p)$

Any $x\in\mathbb{Q}$ can be written as

$x=p^n\frac{a}{b}$ with $a,b\in\mathbb{Z}$ not divisible by p.

then $\nu(x)=n$

This is called p-adic valuation.

Prop 13.6 1) If R is a DVR then R is a Dedekind domain.

2) If R is a Dedekind domain with exactly one maximal ideal, then R is a DVR

Proof 1) R is a DVR $\Rightarrow$ R is Noetherian (because it is a PID), the only non-zero prime ideal in R is maximal. It remains to check tha R is int. closed in its field of fractions.

Assume $x = \frac{a}{u^n}$, $a \in R^\times$, $n > 0$ is integral / R. Then

$$x^k + b_1 x^{k-1} + \ldots + b_k = 0 \quad , b_i \in R$$

$$\Rightarrow \frac{a^k}{u^{nk}} + \frac{b_1 a^{k-1}}{u^{n(k-1)}} + \ldots + b_k = 0$$

$$\Rightarrow a^k = -\left(b_k u^{nk} + \ldots + b_1 a^{k-1} u^n\right) \in \mathfrak{m}$$

but $a^k \in R^\times$ - contradiction.

Hence x is not int / R

$\Rightarrow$ all element integral /R are of the form $u^n a$, $n \geq 0$, so they are contained in R.

2) Assume R is Dedekind domain with unique non-zero prime ideal $\mathfrak{m}$. It remains to check that R is PID

We have unique factorization of ideals in Dedekind domains; this implies $\mathfrak{m} \neq \mathfrak{m}^2$, hence $\exists\, x \in \mathfrak{m} \setminus \mathfrak{m}^2$

Then $(x) = \mathfrak{m}^k$ for some $k \geq 1$ (again by unique factorization)

But $x \notin \mathfrak{m}^2 \Rightarrow k = 1$

$\Rightarrow \mathfrak{m} = (x)$

Any ideal $(0) \neq I \subset R$

$I = \mathfrak{m}^k = (x^k) \Rightarrow$ all ideals are principal. $\square$

<u>Cor.</u> $\mathcal{O}_K$ = ring of integers in a numb. field K, and $\mathfrak{p} \subset \mathcal{O}_K$ prime ideal then $\mathcal{O}_{K,\mathfrak{p}}$ = localization of $\mathcal{O}_K$ at $\mathfrak{p}$ is a DVR

<u>Proof:</u> $\mathcal{O}_{K,\mathfrak{p}}$ is a Dedekind dom. (exercise)

Cor. from. Prop. 13.4 $\Rightarrow \mathcal{O}_{K,\mathfrak{p}}$ has unique max. ideal $\mathfrak{p} \cdot \mathcal{O}_{K,\mathfrak{p}}$ $\square$

<u>Rem</u> By Lemma 13.2, the residue field of $\mathcal{O}_{K,\mathfrak{p}}$ $\quad \mathcal{O}_{K,\mathfrak{p}} / \mathfrak{p} \cdot \mathcal{O}_{K,\mathfrak{p}} \simeq \mathcal{O}_K / \mathfrak{p}$

Assume that $K \subset L$ are two number fields. We have $\mathcal{O}_K \subset \mathcal{O}_L$. Let $\mathfrak{p} \in \operatorname{Spec}(\mathcal{O}_K)$, $S = \mathcal{O}_K \setminus \mathfrak{p}$. S is mult closed subset of $\mathcal{O}_K$, but also of $\mathcal{O}_L$. We can localize w.r.t. S both $\mathcal{O}_K$ and $\mathcal{O}_L$, and we get

$$\mathcal{O}_{K,\mathfrak{p}} = S^{-1}\mathcal{O}_K \hookrightarrow S^{-1}\mathcal{O}_L$$

denote: $\quad A \qquad\qquad B$

<u>Observe</u>: 1) if $\mathfrak{p}\cdot\mathcal{O}_L = \prod_{i=1}^{k} \mathfrak{p}_i^{e_i}$, then $\mathfrak{p}_i$ are exactly those primes of $\mathcal{O}_L$, for which $\mathfrak{p}_i \cap \mathcal{O}_K = \mathfrak{p}$

$$\Leftrightarrow \mathfrak{p}_i \cap S = \emptyset$$

This means that the non-zero prime ideals of B are exactly $S^{-1}\mathfrak{p}_i$ (this follows from Prop. 13.4.)

2) B is integral over A: since $\mathcal{O}_L$ is integral over $\mathcal{O}_K$, if $x \in \mathcal{O}_L$ then $\exists\, a_i \in \mathcal{O}_K$:

$$x^n + a_1 x^{n-1} + \ldots + a_n = 0$$

But then $\forall t \in S$

$$\left(\frac{x}{t}\right)^n + \frac{a_1}{t}\left(\frac{x}{t}\right)^{n-1} + \dots + \frac{a_n}{t^n} = 0$$

$a_i/t^i \in S^{-1}\mathcal{O}_K = A$

$\Rightarrow x/t \in B$ is int/ A.

3) B is a finitely generated A-module:

since $\mathcal{O}_L$ is a fin. generated abelian group, we can find $e_1, \dots, e_n \in \mathcal{O}_L$, s.t. $\forall x \in \mathcal{O}_L \quad x = \sum \alpha_i e_i \quad \alpha_i \in \mathbb{Z}$

Then $S^{-1}\mathcal{O}_L = B$ is generated $/A$ by the images of e_i:

$$\frac{x}{t} \in B \Rightarrow \frac{x}{t} = \frac{\sum \alpha_i e_i}{t} = \sum \frac{\alpha_i}{t} \cdot e_i$$

and $\frac{\alpha_i}{t} \in \mathcal{O}_{K,p} = A$.

Since B is an A-submodule of a field L, B is torsion-free.

Since A is a PID, a torsion-free module is free $\Rightarrow B \simeq A^m$ for some $m \geq 1$

Thm 13.7 (Fundamental identity).

Let $K \subset L$ be number fields, $p \subset \mathcal{O}_K$ a prime ideal, $\mathcal{O}_K/p = \mathbb{F}_q$,

$$p \cdot \mathcal{O}_L = \prod_{i=1}^{k} p_i^{e_i}$$

with $\mathcal{O}_L/p_i = \mathbb{F}_{q^{f_i}}$ for some $f_i \geq 1$

Then: $$[L:K] = \sum_{i=1}^{k} e_i f_i$$

Proof We use the same notation as before.

We have $B \simeq A^m$ as A-module.

Localize A and B w.r.t. $S = A \setminus \{0\}$

$\Rightarrow S^{-1}B = L \simeq (S^{-1}A)^m$ as $S^{-1}A$-module

$S^{-1}A = K \Rightarrow m = [L:K]$

A has unique max ideal $m = p \cdot \mathcal{O}_K$

$$A/m = \mathcal{O}_K/p = \mathbb{F}_q$$

Then $B/mB \simeq (A/mA)^m = \mathbb{F}_q^{[L:K]}$

On the other hand, by CRT:

$$B/mB \simeq \prod_{i=1}^{k} B/q_i^{e_i},$$ where

$q_i = p_i \cdot B$. It remains to compute the dimensions of $B/q_i^{e_i}$ over $\mathbb{F}_q$

$B/\mathfrak{q}_i^{e_i}$ has a filtration

$$0 \subset \mathfrak{q}_i^{e_i-1}/\mathfrak{q}_i^{e_i} \subset \mathfrak{q}_i^{e_i-2}/\mathfrak{q}_i^{e_i} \subset \dots \subset B/\mathfrak{q}_i^{e_i}$$

the quotients are

$$\mathfrak{q}_i^j/\mathfrak{q}_i^{j+1} \simeq B/\mathfrak{q}_i \quad \left(\begin{array}{l}\text{see} \\ \text{Corollary } 9.4 \\ \text{in Lecture } 9\end{array}\right)$$

and $B/\mathfrak{q}_i \simeq \mathcal{O}_L/\mathfrak{p}_i = \mathbb{F}_{q^{f_i}}$

$$\Rightarrow \dim_{\mathbb{F}_q}\left(B/\mathfrak{q}_i^{e_i}\right) = e_i f_i$$

$$\Rightarrow \mathbb{F}_q^{[L:K]} \simeq \prod_{i=1}^{k} \mathbb{F}_q^{e_i f_i}$$

$$\Rightarrow [L:K] = \sum_{i=1}^{k} e_i f_i \qquad \square$$