Commutative Algebra

lecture 19: discrete valuation rings (2)

Misha Verbitsky

http://verbit.ru/IMPA/CA-2022/

IMPA, sala 2

February 17, 2022

Discrete valuations

DEFINITION: Let K be a field. A **discrete valuation** on K is a surjective map $\nu : (K\backslash 0) \longrightarrow \mathbb{Z}$ such that $\nu(xy) = \nu(x) + \nu(y)$ and $\nu(x+y) \geqslant \min(\nu(x), \nu(y))$. The **valuation ring** of ν is $\{x \in K \mid \nu(x) \geqslant 0\}$.

EXAMPLE: Let R be a factorial ring, and $p \in R$ a prime. Given $x \in k(R)$, write the prime decomposition $x = \prod_i p_i^{\alpha_i}$ (here $\alpha_i \in \mathbb{Z}$ and **can be negative,** because x belongs to the field of fractions). Take $\nu_{p_1}(x) := \alpha_1$. This function is called **p-adic valuation**. The corresponding valuation ring is all fractions $\frac{a}{b}$ where a and $b \in R$ are coprime and b is not divisible by p.

DEFINITION: A ring R without zero divisors is a **discrete valuation ring (DVR)** if $k(R)$ admits a discrete valuation such that R is its valuation ring.

REMARK: Local ring of Krull dimension 1 and without zero divisors **has only two prime ideals.** Conversely, a ring which has only two prime ideals $0 \subsetneq \mathfrak{m}$ has Krull dimension 1. A DVR **has only two prime ideals, 0 and $\mathfrak{m} := \nu^{-1}(\mathbb{Z}^{>0})$,** hence it is local and has Krull dimension 1.

Discrete valuation rings and principal ideals

Claim 1: Let R be a Noetherian local ring without zero divisors, and $\mathfrak{m}$ its maximal ideal. **Then $\mathfrak{m}$ is principal if and only if R is a discrete valuation ring.**

Proof: Let R be a DVR. Consider an element p with $\nu(p) = 1$. For any $x \in R$ with $\nu(x) = k$, one has $x = up^k$, where u is invertible, hence all ideals of R are principal.

Conversely, if $\mathfrak{m}$ is generated by p, **any element $x \in R$ which is not divisible by p is invertible,** hence $x = up^k$, where u is invertible. Then R is the DVR for the p-adic valuation. ■

Corollary 1: A discrete valuation ring is local, Noetherian, integrally closed, all its ideals are principal, and the Krull dimension of R is 1. ■

Many ways to characterise a discrete valuation ring

THEOREM: Let R be a Noetherian local ring without zero divisors, $\mathfrak{m}$ its maximal ideal, and $k := R/\mathfrak{m}$ its residue field. Assume that R has Krull dimension 1. **Then the following are equivalent.**
(i) R is a discrete valuation ring.
(ii) R is integrally closed.
(iii) $\mathfrak{m}$ is a principal ideal.
(iv) $\dim_k \frac{\mathfrak{m}}{\mathfrak{m}^2} = 1$.
(v) Every non-zero ideal of R is a power of $\mathfrak{m}$.
(vi) There exists $p \in R$ such that every non-zero ideal of R is generated by p^k, for some $k \in \mathbb{Z}^{>0}$.

Proof: Later today.

Projective R-modules

DEFINITION: An R-module M is called **free** if M is a direct sum of several copies of R (possibly infinitely many copies). It is called **projective** if it is a direct summand of a free R-module.

PROPOSITION: An R-module P is projective if for every surjective homomorphism $\varphi: \ A \longrightarrow B$ of R-modules and every homomorphism $\psi: \ P \longrightarrow B$, **the map ψ can be factorized through φ** making the following diagram commutative:

$$\begin{tikzcd} & A \arrow[d, "\varphi"] \\ P \arrow[ur, dashed, "\mu"] \arrow[r, "\psi"] & B \end{tikzcd}$$

Proof: Let $\varphi: \ F \longrightarrow P$ be a surjective map from a free module to P and $\psi = \varphi$. The map ψ **can be factorized through φ if and only if ψ admits a section μ,** which gives a decomposition $F = \ker \psi \oplus \operatorname{im} \mu$.

Conversely, if P is a direct summand of $F = P \oplus P_1$, we can extend ψ from P to a free R-module $F = P \oplus P_1$. Then **the map μ can be defined on the generators of F and restricted to $P \subset F$.** ■

Dual basis theorem

THEOREM: (Dual basis theorem) Let M be an R-module. Consider a natural map $\Psi:\ \operatorname{Hom}_R(M,R)\otimes_R M \longrightarrow \operatorname{Hom}_R(M,M)$. **Then the following are equivalent.**

(i) Ψ is an isomorphism.

(ii) $\operatorname{Id}_M \in \operatorname{im}(\Psi)$.

(iii) M is projective and finitely generated.

Proof: Clearly, Ψ is an isomorphism for any free finitely generated R-module M, hence for any direct sum component of a free finitely generated R-module. **Therefore, (iii) $\Rightarrow$ (i) $\Rightarrow$ (ii).**

The condition (ii) is equivalent to the following. There exists a finite collection of maps $f_i:\ M \longrightarrow R$, $i = 1,...,n$ and a finite set $m_i \in M$, $i = 1,...,n$ such that for any $m \in M$ one has $\sum_{i=1}^n f_i(m)m_i = m$. In particular, **(ii) implies that M is finitely generated.**

Let $F = \langle m_i \rangle$ be a free module generated by $\{m_i\}$, and $f(m) := \sum_{i=1}^n f_i(m)m_i$. Then f is a section of the natural projection $F \longrightarrow M$, hence M is projective. **This gives (ii) $\Rightarrow$ (iii).** ■

Projective modules in local rings

PROPOSITION: Let P be a finitely generated projective module over a local ring R. **Then P is a free R-module.**

Proof: Denote by $\mathfrak{m}$ the maximal ideal of R. Let $e_1, ..., e_n$ be a set of elements of $P \backslash \mathfrak{m}P$ generating $\frac{P}{\mathfrak{m}P}$. We chose e_i in such a way that their images in $\frac{P}{mP}$ are linearly independent over the field $R/\mathfrak{m}$. By Nakayama's lemma, $\{e_i\}$ generate P. Since P is projective, the projection from the free module $F := \langle e_1, ..., e_m \rangle \longrightarrow P$ has a section $\psi : P \longrightarrow \langle e_1, ..., e_m \rangle$. **Since $\operatorname{im} \psi$ modulo $\mathfrak{m}F$ generates $\frac{F}{\mathfrak{m}F}$, we have $F = \operatorname{im} \psi$, and P is a free R-module.** ■

Fractional ideals (reminder)

DEFINITION: Let R be a ring without zero divisors, and $k(R)$ its fraction field. A non-zero R-submodule $I \subset k(R)$ is called **a fractional ideal** of R if for some $a \in R$, one has $aI \subset R$.

CLAIM: Let R be a Noetherian ring, and $I \subset k(R)$ an R-submodule. Then I **is a fractional ideal if and only if I is finitely generated.**

DEFINITION: Let I_1, I_2 be fractional ideals. Then the **set $I_1 I_2$** of products of elemens in I_1, I_2 is a fractional ideal.

CLAIM: For any two fractional ideals I_1, I_2, **the intersection $I_1 \cap I_2$ is non-empty,** hence **$I_1 \cap I_2$ is also a fractional ideal.**

CLAIM: Let $I \subset R$ be a fractional ideal. Then the sets $I^{-1} := \{x \in R \mid xI \subset R\}$ and $R(I) := \{x \in k(R) \mid xI \subset R\}$ are fractional ideals. Moreover, for any fractional ideal I_1, I_2, **the R-module $J := \{x \in k(R) \mid xI_1 \subset I_2\}$ is a fractional ideal.**

CLAIM: For any fractional ideal I, **one has $R(I) \supset R \supset II^{-1}$. If, in addition, $I \subset R$, then $I^{-1} \supset R$.**

Invertible fractional ideals

DEFINITION: A fractional ideal $I \subset k(R)$ is called **invertible** if $II^{-1} = R$.

THEOREM: A fractional ideal is invertible if and only if it is projective, and it is then finitely generated.

Proof. Step 1: $I^{-1}I \ni 1$ implies $\mathrm{Id}_I \in \mathrm{Hom}_R(I,R) \otimes_R I$, which implies projectivity by the Dual Basis Theorem.

Step 2: Consider an R-linear map $\varphi: I_1 \longrightarrow I_2$ If we tensor φ it with $k(R)$, we obtain a $k(R)$-linear map $I_1 \otimes_R k(R) \longrightarrow I_2 \otimes_R k(R)$, with $I_i \otimes_R k(R) = k(R)$. Clearly, $\mathrm{Hom}_{k(R)}(k(R), k(R)) = k(R)$. **Therefore, φ it is expressed as $v \longrightarrow \alpha v$, for some $\alpha \in k(R)$.** This gives $I^{-1} = \mathrm{Hom}_R(I,R)$.

Step 3: If I is projective, then $\mathrm{Id}_I \in \mathrm{Hom}_R(I,R) \otimes_R I$, hence $I^{-1}I \ni 1$, and $I^{-1}I = R$. ■

REMARK: The multiplication of fractional ideals is associative, and this multiplication **induces the structure of an abelian group on the set of invertible fractional ideals in R.**

Radical ideals in local rings of Krull dimension 1

Recall that **the radical** $\sqrt{I}$ of an ideal $I \subset R$ is the set of all $x \in R$ such that $x^n \in I$ for some $n > 0$. An ideal I is called **radical** if $I = \sqrt{I}$.

CLAIM: Let R be a local ring of Krull dimension 1. **Then any non-zero radical ideal of R is its maximal ideal.**

Proof: Let $I \subset R$ be a non-zero radical ideal. Then 0 in R/I is an intersection of all prime ideals in R/I. In other words, I is an intersection of prime ideals containing I. Since R is a local ring of Krull dimension 1 and without zero divisors, it has only two prime ideals. Since I is non-zero, there exists only one prime ideal $\mathfrak{m} \subset R$ containing I, hence $I = \mathfrak{m}$. ■

Corollary 2: Let R be a Noetherian local ring of Krull dimension 1, and $\mathfrak{m}$ its maximal ideal. **Then for any $t \in \mathfrak{m}$ there exists n such that $\mathfrak{m}^n \subset (t)$.**

Proof: The radical of (t) is $\mathfrak{m}$, by the previous claim. ■

Local rings of Krull dimension 1 with projective maximal ideal

PROPOSITION: Let R be a be a Noetherian local ring, and $\mathfrak{m}$ its maximal ideal. **Assume that $\mathfrak{m}$ is projective as an R-module. Then R is DVR.**

Proof: Sunce R is Noetherian and local, $\mathfrak{m}$ is free. Choose the elements $p_1, p_2, ..., p_n$ freely generating $\mathfrak{m}$. Then $\mathfrak{m} = \bigoplus_i (p_i)$, which is impossible, unless $n = 1$, because $p_1 p_2 \in (p_1) \cap (p_2)$. **Therefore, $\mathfrak{m}$ is a principal ideal,** and R is DVR by Corollary 1. ■

Corollary 3: Let R be a Noetherian local ring, and $\mathfrak{m}$ its maximal ideal. **Assume that $\mathfrak{m}$ is invertible as a fractional ideal. Then R is DVR.**

Proof: Invertible fractional ideals are projective. ■

Integrally closed local rings of Krull dimension 1

Proposition 2: Let R be an integrally closed Noetherian local ring of Krull dimension 1. **Then R is a discrete valuation ring.**

REMARK: The converse statement is implied by Corollary 1.

Proof. Step 1: Let $I \subset k(R)$ be a fractional ideal, and $R(I) \subset k(R)$ the ring of all $x \in k(R)$ such that $xI \subset I$. **Since $R(I) \subset \operatorname{Hom}_R(I, I)$, it is finitely generated as R-module, hence $R(I) = R$.**

Step 2: Let $\mathfrak{m}$ be the maximal ideal of R. Then $R \subset \mathfrak{m}\mathfrak{m}^{-1} \subset \mathfrak{m}$. Since any element of $R \backslash \mathfrak{m}$ is invertible, we have either $\mathfrak{m}\mathfrak{m}^{-1} = R$ or $\mathfrak{m}\mathfrak{m}^{-1} = \mathfrak{m}$. **In the second case, $\mathfrak{m}^{-1} = R$** by Step 1, because in this case $\mathfrak{m}^{-1} \subset R(\mathfrak{m})$. **In the first case, the fractional ideal $\mathfrak{m}$ is invertible.**

Step 3: By Krull lemma, $\mathfrak{m} \supsetneq \mathfrak{m}^2 \supsetneq ... \supsetneq \mathfrak{m}^n$. Let $t \in \mathfrak{m} \backslash \mathfrak{m}^2$. By Corollary 2, $\mathfrak{m}^n \subset (t)$, for some $n > 0$; choose the minimal n with this property, and let $x \in \mathfrak{m}^{n-1} \backslash (t)$.

Let $y := \frac{x}{t}$. Since $x \notin (t)$, we have $y \notin R$.

Clearly, $x\mathfrak{m} \subset \mathfrak{m}^n \subset (t)$. This gives $y\mathfrak{m} \subset R$. Then Step 2 implies that $\mathfrak{m}^{-1}\mathfrak{m} = R$, and Corollary 3 implies that R is DVR. ■

Residue fields of discrete valuation rings (reminder)

Claim 2: Let R be a discrete valuation ring, and $\mathfrak{m}$ its maximal ideal, and $k := R/\mathfrak{m}$ its residue field. **Then $\mathfrak{m}^d/\mathfrak{m}^{d+1}$ is 1-dimensional as a k-vector space for all $d \in \mathbb{Z}^{\geqslant 0}$.**

Proof: Let p be the generator of $\mathfrak{m}$, and $L_{p^d}(x) := p^d x$. Then $L_{p^d}: R \mapsto \mathfrak{m}^d$ is an isomorphism which maps $\mathfrak{m}$ to $\mathfrak{m}^{d+1}$. ■

REMARK: For some discrete valuation rings, **the map $R \longrightarrow R/\mathfrak{m} = k$ has a section $k \longrightarrow R$.** This is true, for example, for the ring $\mathbb{C}[t]$ localized in (t); in this case, $k = \mathbb{C}$ **(prove this)**. For other rings, such section does not exist; for example, consider the ring $\mathbb{Z}$ localized in (p); in this case, the residue field in $\mathbb{Z}/p\mathbb{Z}$ **(prove this)**.

Many ways to characterise a discrete valuation ring

THEOREM: Let R be a Noetherian local ring without zero divisors, $\mathfrak{m}$ its maximal ideal, and $k := R/\mathfrak{m}$ its residue field. Assume that R has Krull dimension 1. **Then the following are equivalent.**
(i) R is a discrete valuation ring. (ii) R is integrally closed.
(iii) $\mathfrak{m}$ is a principal ideal. (iv) $\dim_k \frac{\mathfrak{m}}{\mathfrak{m}^2} = 1$.
(v) Every non-zero ideal of R is a power of $\mathfrak{m}$.
(vi) There exists $p \in R$ such that every non-zero ideal of R is generated by p^k, for some $k \in \mathbb{Z}^{>0}$.

Proof. Step 1: (i) implies (ii), (iii), (v) and (vi) as follows from Proposition 1. (i) implies (iv) by Claim 2. **Therefore, (i) implies (ii)-(vi).**

Step 2: (iii) $\Leftrightarrow$ (i) by Claim 1. (ii) implies (i) by Proposition 2. Also, (v) implies (vi) which implies that R is factorial which implies (ii). **We proved that all (i)-(vi) are equivalent, except maybe (iv).**

Step 3: Now we prove that (iv) implies (iii). Let p be a generator of $\mathfrak{m}$ modulo $\mathfrak{m}^2$. Then the natural map $\frac{(p)}{(p)\mathfrak{m}} \longrightarrow \frac{\mathfrak{m}}{\mathfrak{m}^2}$ is surjective. By Nakayama lemma, for any morphism $\varphi: M \longrightarrow N$ of finitely generated modules over a local ring, **surjectivity of the map $\varphi: \frac{M}{\mathfrak{m}M} \longrightarrow \frac{N}{\mathfrak{m}N}$ implies the surjectivity of φ,** hence $\mathfrak{m}$ is a principal ideal. ■