Commutative Algebra

lecture 18: discrete valuation rings

Misha Verbitsky

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

IMPA, sala 232

February 14, 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.

Discrete valuation rings

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

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

Proof. Step 1: Clearly, all $x \in A$ which satisfy $\nu(x) = 0$ are invertible. Therefore, the ideal $\mathfrak{p} := \{x \in A \mid \nu(x) > 0\}$ is maximal. Since **all elements which don't belong to $\mathfrak{p}$ are invertible,** A is local.

Step 2: Let $p \in A$ be an element which satisfies $\nu(p) = 1$. Then for any $x \in A$ such that $k = \nu(x)$, the element $x_1 := xp^{-k}$ belongs to A and is invertible. Then, $x = p^k x_1$. We obtain that any ideal which contains p^k contains all elements $x \in A$ with $\nu(x) \geqslant k$.

Step 3: Let $I \subset A$ be an ideal, and $k := \min_{x \in I} \nu(x)$. By Step 2, $I = (p^k)$, hence I is a principal ideal. The only chain of ideals which exists in A is $(p^{k_1}) \subsetneq (p^{k_2}) \subsetneq (p^{k_3}) \subsetneq ...$ with $k_1 > k_2 > k_3 > ....$ and it terminates, because all k_i are positive integers. Therefore, A is Noetherian. It is integrally closed because it is factorial. ■

Many ways to characterize a discrete valuation ring

THEOREM: Let A be a Noetherian local ring without zero divisors, $\mathfrak{m}$ its maximal ideal, and $k := A/\mathfrak{m}$ its residue field. Assume that A has Krull dimension 1. **Then the following are equivalent.**

(i) A is a discrete valuation ring.

(ii) A 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 A is a power of $\mathfrak{m}$.

(vi) There exists $p \in A$ such that every non-zero ideal of A is generated by p^k, for some $k \in \mathbb{Z}^{>0}$.

I will prove this theorem later today.

Fractional ideals: basic properties

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.**

Proof: Let I be finitely generated by the collection $\{\frac{a_i}{b_i} \in k(R)\}$, with $a_i, b_i \in R$. Then $\prod_i b_i I \subset R$. Conversely, if $aI \subset R$, then aI is finitely generated, because aI is an ideal in a Noetherian ring. ■

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.**

Proof: Since $aI_i \subset R$, the intersection $I_i \cap R$ is non-empty. Let $a_i \in I_i \cap R$. Then $a_1 a_2 \in RI_i = I_i$, hence $a_1 a_2 \in I_1 \cap I_2$. ■

Fractional ideals: I^{-1} and $R(I)$

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.**

Proof. Step 1: Let $a, b \in R \backslash 0$ be elements such that $aI_1 \subset R$ and $b \in I_2 \cap R$. Then $abI_1 \subset bR \subset I_2$, hence J is non-empty.

Step 2: For any non-zero elements $c, d \in R$ such that $c \in I_1$, $dI_2 \subset R$, and any $x \in J$, we have $cdx = d(xc) \subset dI_2 \subset R$, hence $cdx \in R$. ■

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

Proof: $R(I) \supset R$ because I is R-module and $R \supset II^{-1}$ because $aI \subset R$ for any $a \in I^{-1}$. Finally, $I \subset R$ implies that any $x \in R$ satisfies $xI \subset R$, hence $x \in I^{-1}$.
■

Integrally closed local rings of Krull dimension 1

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

REMARK: The converse statement follows from Proposition 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: Since all ideals of R are contained in $\mathfrak{m}$ and contain 0 and $\dim R = 1$, the only maximal chain of prime ideals in R is $0 \subsetneq \mathfrak{m}$. Therefore, **$R$ has only two prime ideals, $\mathfrak{m}$ and 0.**

Step 3: Let $\mathfrak{m}$ be the maximal ideal of R. We are going to show that the fractional ideal $\mathfrak{m}^{-1} \supset R$ is not equal to R. Consider the set $\mathfrak{S}$ of all ideals $I \subset R$ such that $I^{-1} \supsetneq R$; this set includes all principal ideals, hence it is non-empty. An increasing chain of ideals in R terminates. Let $J \in \mathfrak{S}$ be the maximal (in the sense of inclusion) ideal which satisfies $J^{-1} \supsetneq R$. By Step 2, **to show that $\mathfrak{m}^{-1} \neq R$, it suffices to prove that J is prime.**

Integrally closed local rings of Krull dimension 1 (2)

Step 4: By absurd, assume that $x, y \in R\backslash J$, and $xy \in J$. Take $z \in J^{-1}\backslash R$. Then $zy(xR + J) \subset R$, because $z(xyR) \in zJ \subset R$ and $yzJ \ni yR \subset R$. Since the ideal $J_1 := xR + J \notin \mathfrak{S}$, $zyJ_1 \subset R$ implies $zy \in R$. Then $z(yR + J) \subset R$, giving $(yR + J)^{-1} \neq R$, a contradiction. **We proved that $\mathfrak{m}^{-1} \supsetneq R$.**

Step 5: Claim 1 implies that $R \supset \mathfrak{m}\mathfrak{m}^{-1} \supset \mathfrak{m}R = \mathfrak{m}$. However, $\mathfrak{m}\mathfrak{m}^{-1} = \mathfrak{m}$ implies $\mathfrak{m}^{-1} \subset R(\mathfrak{m}) = R$ (Step 1), **hence $\mathfrak{m}\mathfrak{m}^{-1} = R$.**

Step 6: By Krull lemma, $\bigcap_i \mathfrak{m}^i = 0$. Then $\mathfrak{m} \neq \mathfrak{m}^2$. Choose $p \in \mathfrak{m}\backslash\mathfrak{m}^2$. Then $p\mathfrak{m}^{-1} \subset R$. Since $p \notin \mathfrak{m}^2$ and $\mathfrak{m}^{-1}\mathfrak{m}^2 = \mathfrak{m}$, this implies $p\mathfrak{m}^{-1} \not\subset \mathfrak{m}$. Then $p\mathfrak{m}^{-1} \subset R$ **is a submodule not contained in $\mathfrak{m}$, hence $p\mathfrak{m}^{-1} = R$ and $pR = \mathfrak{m}$.**

Step 7: Since $\bigcap_i \mathfrak{m}^i = 0$, any $x \in R$ belongs to $\mathfrak{m}^d\backslash\mathfrak{m}^{d+1}$ for some d. Then $p^{-d}x \in R\backslash m$ is invertible, hence R is factorial, and every element of $k(R)$ is represented as $x = p^d u$, where $u \in R$ is invertible. Define $\nu : k(R) \longrightarrow \mathbb{Z}$ by $\nu(x) = d$. **Then $R = \nu^{-1}(0)$, and R is discrete valuation ring.** ■

Residue fields of discrete valuation rings

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. (ii) implies (i) by Proposition 2. (i) implies (iv) by Claim 2.

Step 2: Assume (iii), and let $(p) = \mathfrak{m}$. Then $\mathfrak{m}^{-1} = p^{-1}R$ and $\mathfrak{m}\mathfrak{m}^{-1} = R$, hence for any $x \in \mathfrak{m}^k \backslash \mathfrak{m}^{k+1}$, the element $p^{-k}x \in R \backslash \mathfrak{m}$ is invertible. This implies that R is factorial, hence integrally closed. We proved that (iii) implies (ii) and (i). Also, (v) implies (vi) which implies that R is factorial. We proved that all (i)-(vi) are equivalent, except (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. ■