

# SOME NOTES ON ALGEBRAIC GEOMETRY

LIANG TONGTONG

ABSTRACT.

## CONTENTS

1. Divisor on curves	1
2. Going-up and Going-down	3
3. Dimension theory	7
4. Geometric viewpoint of primary decomposition	8
5. Regularity and DVRs	9
6. Decomposition and Dedekind domain	12
7. Derived Geometry	14
References	14

## 1. DIVISOR ON CURVES

**Definition 1.1.** Let  $f: X \rightarrow Y$  be a finite morphism between smooth curves. We define

$$f^*: \text{Weil}Y \rightarrow \text{Weil}X$$

as follows, for any closed point  $Q \in Y$ , let  $t$  be a local parameter of  $Q$  i.e. a generator of the prime ideal in the DVR  $\mathcal{O}_Q$ , then define

$$f^*Q = \sum_{f(P)=Q} v_P(f^*(t))[P]$$

where  $P$  are closed points and note that  $f$  induces a morphism at stalk-level  $\mathcal{O}_P \rightarrow \mathcal{O}_Q$ .

We can extend this definition from prime divisors to any divisor freely.

*Remark 1.2.*  $f^*Q$  is independent of the choice of local parameter  $t$  because two local parameters is in difference of a unit in the local ring.

Since  $f$  is a finite morphism, then  $f^{-1}(Q)$  is a finite set, hence it is well defined.

For a principal divisor  $\text{div}(f)$  in  $Y$ ,  $f^*(\text{div}(g)) = \text{div}(g \circ f)$  (we may identify  $g \circ f$  as the image of  $g$  via the morphism induced by  $f$  at the sheaf-level. Hence, we actually have a morphism

$$f^*: \text{Cl}(Y) \rightarrow \text{Cl}(X)$$

---

Received by the editors June 3, 2021.

1991 *Mathematics Subject Classification.* Primary.

**Proposition 1.1.** *Let  $f: X \rightarrow Y$  be a finite morphism between smooth curves, the degree of field extension  $K(Y) \hookrightarrow K(X)$  induced by  $f$  is called **the degree of  $f$** , denoted by  $\deg f$ . Then for any divisor  $D \in \text{Weil}(X)$ , we have*

$$\deg(f^*D) = \deg(f) * \deg(D)$$

**Corollary 1.1.** *For a principle divisor  $\text{div}(h)$  on  $X$ ,  $\deg(h) = 0$ . Hence there is a surjective homomorphism*

$$\deg: \text{Cl}(X) \rightarrow \mathbb{Z}$$

However, in general,  $\deg$  is not injective. Next we will show the necessary and sufficient condition that  $\deg$  is injective.

**Example 1.3.** Let  $X$  be a projective and smooth curve, then if there exists a pair of distinct closed points  $P, Q \in X$  such that  $P - Q = \text{div}(h)$  for some  $h \in K(X)$ , then  $X \simeq \mathbb{P}^1$  i.e  $X$  is birational equivalent to a projective line. Hence  $\text{cl}(X) \cong \mathbb{Z}$  if and only if  $X \simeq \mathbb{P}^1$ .

First,  $\text{div}(h) = P - Q$  means for a rational function  $h$  on  $X$ ,  $h$  has a simple zero at  $P$  and a simple pole at  $Q$ .

Fact, there is a rational map  $\varphi: X \rightarrow \mathbb{P}^1$  corresponds to the field extension  $K(t) \rightarrow K(X)$  by sending  $t \mapsto h$  i.e. on the level of closed points, we have

$$(1) \quad \varphi(\alpha) = \begin{cases} [1 : h(\alpha)] & h(\alpha) \neq 0 \\ [0 : 1] & h(\alpha) = 0 \end{cases}$$

Hence  $\varphi^*([1 : 0]) = P$  while  $\varphi^*([0 : 1]) = Q$ . Recall Proposition 1.1, we have

$$1 = \deg(\varphi^*([1 : 0])) = \deg \phi * 1$$

thus  $\deg \varphi = 1$  and then  $K(X) = K(t)$ ,  $X, \mathbb{P}^1$  are birational.

**Example 1.4.** Elliptic curves are smooth cubic curves (degree 3) in  $\mathbb{P}_k^2$ . For simplicity, assume  $\text{char } k \neq 2$ , then it can be described by

$$y^2 = 4x^3 + g_2x + g_3$$

(it can be homogenized by replace  $x, y$  by  $x/z, y/z$ ). This form is called **Weierstrass form**. Now to describe the group structure on the set of closed points of elliptic curve  $E$ . Let  $\text{Cl}^0(E)$  be the kernel of  $\deg: \text{Cl}(E) \rightarrow \mathbb{Z}$  and we will show there is an 1-1 correspondence between  $E$  and  $\text{Cl}^0(E)$ . (Here we abuse of notation:  $E$  means the set of closed points in  $E$ , when we want to take it as a group).

We just consider the special case of elliptic curves

$$y^2z - x^3 + xz^2 = 0$$

then let  $P_0 = [0 : 1 : 0] \in E$  and  $\div(z) = 3P_0$  on  $E$  due to the following equations

$$\begin{cases} y^2z - x^3 + xz^2 = 0 \\ z = 0 \end{cases}$$

have 3 zeros at  $z = 0, x = 0$ .

Then let  $L \subset \mathbb{P}^2$  be a line  $ax + by + cz = 0$  and let  $l = ax + by + cz$  and  $L = \div(l)$  on  $\mathbb{P}^2$ . According to Bezout's theorem and a line is of degree 1,  $L \cap E$  has 3 points (including multiplicities, then we have

$$\div\left(\frac{l}{z}\right) = P + Q + R - 3P_0$$

which means that

$$[P + Q + R] \sim 3[P_0]$$

on  $E$ . Note that  $\deg(P - P_0) = 0$  for any point  $P$ , hence  $P - P_0 \in \text{Cl}^1(E)$ , then we give a map  $\alpha: E \rightarrow \text{Cl}^0(E)$  by

$$P \mapsto [P - P_0]$$

Now claim that it is injective: if  $P - P_0 \sim Q - P_0$ , then  $P - Q \sim \div(f)$  for some rational function  $f$ , if  $P \neq Q$ , then  $E \simeq \mathbb{P}^1$  by  $F: E \rightarrow \text{Cl}^0(E)$

$$x \mapsto [1 : f(x)]$$

when  $x \neq Q$  and  $Q \mapsto [0 : 1]$  and note that  $F * ([1 : 0]) = P$ , thus  $\deg F = 0$ . However, an elliptic curve is not rational, which leads to contradiction. Therefore, we must have  $P = Q$ .

Next to show it is surjective: For any  $D = \sum n_i P_i \in \text{Cl}^0(E)$  with  $\sum n_i = 0$ , then

$$\sum n_i P_i = \sum n_i (P_i - P_0)$$

let  $L$  be a line in  $\mathbb{P}^2$  determined by  $P_0$  and  $P_i$ , and let  $P_0, P_i, R_i$  be  $L \cap E$  and

$$(2) \quad P_0 + P_i + R_i \sim 3P_0$$

Hence  $P_i - P_0 \sim -(R_i - P_0)$ .

Then if  $n_i < 0$ , we may replace  $P_i - P_0$  by  $-(R_i - P_0)$  so that we may assume  $n_i \geq 0$ . In particular,  $\sum n_i \geq 0$ . If  $\sum n_i = 1$  with all  $n_i \geq 0$ , then  $D = P_i - P_0$ , which is in the image. Now we argue by induction on  $\sum n_i$ .

Observe that  $P_1 - P_0 + P_2 - P_0 \sim P_0 - R$  for some  $R$  (recall the relation 2, we get such  $R$  be consider the intersection between  $E$  and a line determined by  $P_1, P_2$ ) Then there is a point  $T$  such that  $T - P_0 \sim P_0 - R$  by consider the intersection between the  $E$  and the line given by  $T, P_0$ . Then we can use this observation to proceed the induction.

## 2. GOING-UP AND GOING-DOWN

**Theorem 2.1.** *Suppose  $f: A \hookrightarrow B$  is an integral extension, then the induced scheme morphism  $f^*: \text{Spec } B \rightarrow \text{Spec } A$  is surjective.*

**Theorem 2.2** (Going-up). *Let  $A, B$  be two integral domain and  $f: A \hookrightarrow B$  be an integral extension. For any two prime ideals  $\mathfrak{p}_1 \subset \mathfrak{p}_2$  in  $A$  and a prime ideal  $\mathfrak{q}_1$  in  $B$  such that  $\mathfrak{q}_1 \cap A = \mathfrak{p}_1$ , then there exists  $\mathfrak{q}_2$  in  $B$  such that  $\mathfrak{q}_2 \cap A = \mathfrak{p}_2$ .*

Going-down property: Let  $A \hookrightarrow B$  be an integral extension,  $\mathfrak{p}_2 \subset \mathfrak{p}_1 \subset A$  and  $\mathfrak{q}_1 \subset B$  be prime ideals such that  $\mathfrak{p}_1 \cap A = \mathfrak{p}_1$ , then there exists  $\mathfrak{q}_2 \in \text{Spec } B$  such that  $\mathfrak{q}_2 \cap A = \mathfrak{p}_2$ .

**Theorem 2.3** (Going-down). *When  $A \subset B$  are rings and  $A$  is integrally closed, then the going-down property holds and the induced morphism  $f^*: \text{Spec } B \rightarrow \text{Spec } A$  is an open map.*

To prove this theorem, we need several lemmas.

**Lemma 2.4** (Heuristic). *Let  $A \subset B$  be rings such that  $B$  is integral over  $B$ , then for any prime ideal  $\mathfrak{p} \subset B$  there exists a prime ideal  $\mathfrak{P}$  in  $B$  such that  $\mathfrak{P} \cap A = \mathfrak{p}$ .*

*Proof.* First, we do localization with respect to  $\mathfrak{p}$  and  $A_{\mathfrak{p}} \rightarrow B_{\mathfrak{p}}$  is still an integral extension. If there exists a prime ideal  $\mathfrak{P}B_{\mathfrak{p}}$  in  $B_{\mathfrak{p}}$  over  $\mathfrak{p}A_{\mathfrak{p}}$ , then  $\mathfrak{P} = \mathfrak{P}B_{\mathfrak{p}} \cap B$  satisfies that  $\mathfrak{P} \cap A = \mathfrak{p}$ .

Hence the problem is reduced to local case that we may assume  $A$  is a local ring with maximal ideal  $\mathfrak{m}$ . Next we just need to find a prime ideal  $\mathfrak{n}$  in  $B$  such that  $\mathfrak{n} \cap A = \mathfrak{m}$ . A good candidate for such  $\mathfrak{n}$  is the maximal ideal in  $B$  that contains  $\mathfrak{m}B$ , but we still need to show that  $\mathfrak{m}B$  is a proper ideal in  $B$ .

Argue by contradiction to show that  $\mathfrak{m}B$  is a proper ideal in  $B$ . If  $\mathfrak{m}B = B$ , then there exists  $b_1, \dots, b_n \in B$  and  $m_1, \dots, m_n \in \mathfrak{m}$  such that

$$\sum m_i b_i = 1$$

Then we have a subring  $A[b_1, \dots, b_n]$ . Note that all  $b_i$  is integral over  $A$ , then  $M = A[b_1, \dots, b_n]$  is a finitely generated  $A$ -module and by previous assumption,  $M \subset \mathfrak{m}M$ . By Nakayama's lemma,  $M = 0$ , contradiction.

Hence there exists a maximal ideal  $\mathfrak{n} \subset B$  such that  $\mathfrak{n}$  is over  $\mathfrak{m}$ . Claim that  $\mathfrak{n} \cap A$  is a maximal ideal in  $A$ , because  $B/\mathfrak{n}$  is a field integral over  $A/(\mathfrak{n} \cap A)$ , for any non-zero element  $x \in A/(\mathfrak{n} \cap A)$ ,  $x^{-1} \in B$  and  $x^{-1}$  is integral over  $A/(\mathfrak{n} \cap A)$  i.e there exists a monic polynomial with  $A/(\mathfrak{n} \cap A)$  such that

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

Then we have

$$x^{-1} = -(a_n x^{n-1} + \dots + a_1)$$

which shows that  $A/(\mathfrak{n} \cap A)$  is a field. Here we finish the proof.  $\square$

**Lemma 2.5.** *Let  $A \subset B$  be integral domains, for given  $\mathfrak{q}_1$  in  $\text{Spec } B$  and  $\mathfrak{p}_1$  in  $\text{Spec } A$ , then there exists a minimal prime ideal  $\mathfrak{q}$  of  $\text{Spec } B$  such that  $\mathfrak{q} \cap A$  is a minimal prime ideal in  $\text{Spec } A$ .*

This is a straight result from Heuristic lemma. Hence we may assume  $A, B$  are integral domains. **However, the key problem is that we have guaranteed that such  $\mathfrak{q} \subset \mathfrak{q}_1$  yet and that we will do next.**

Next we show that the condition that  $A$  is integrally closed is essential.

**Example 2.6.** Let  $k = \mathbb{C}$ ,  $B = k[x, y]$  and  $A = \{f \in B \mid f(0, 0) = f(0, 1)\}$ . The picture of  $\text{Spec } B$  is the plane  $k^2$  and we get  $\text{Spec } A$  by gluing  $P_1 = (0, 0)$  and  $P_2 = (0, 1)$  in  $k^2$  to be one point  $P$  and the induced map  $\text{Spec } B \rightarrow \text{Spec } A$  is the quotient map. Let  $C$  be the  $x$ -axis in  $k^2$  and  $\overline{C}$  be the image of  $x$ -axis in  $\text{Spec } A$ . However, the we have  $P \in \overline{C}$  and  $P_2$  over  $P$ , but we can find an irreducible closed subset in  $\text{Spec } B$  such that it contains  $P_2$  and its image is  $\overline{C}$ , because the preimage of  $\overline{C}$  is  $C$  and  $P_2 \notin C$ . Here the going-down property fails.

(The question is: How to show  $B$  is integral over  $A$  and  $A$  is not integrally closed?)

$B$  is integral over  $A$ :  $x \in A$ , we just need to show for any  $f(y) \in B$ ,  $f(y)$  is integral over  $A$ : consider  $(f(y) - f(0))(f(y) - f(1)) \in A$ , then  $f^2(y) - (f(0) + f(1))f(y) + f(0)f(1) - (f(y) - f(0))(f(y) - f(1)) = 0$  clearly.

$A$  is not integrally closed: Consider

$$\frac{(x + y - \frac{1}{2})^2 - (y - \frac{1}{2})^2}{x} = 2y - 1$$

which is in  $K(A)$  but not in  $A$ . However,  $(2y - 1)^2$  is in  $A$ , then  $2y - 1$  is a zero for a monic polynomial over  $A$  with variable  $T$ :

$$T^2 - (2y - 1)^2$$

Now suppose  $A \subset B$  are integral domains and  $A$  is integrally closed.

Observation 1: We may assume  $B$  is the integral closure of  $A$  in  $L$ .

Let  $L$  be the fraction field of  $B$  and  $K$  be the fraction field of  $A$ , then  $L/K$  is an algebraic field extension clearly. Let  $\bar{A}$  be the integral closure of  $A$  in  $L$ , if the going-down property holds for  $\bar{A}$ , then it holds for  $B$  because  $A \subset B \subset \bar{A}$ .

Observation 2: If for finite field extension  $L/K$ , the going-down properties holds, then for infinite algebraic field extensions, it still holds.

Suppose it is true for finite field extension, then for an algebraic field extension  $L/K$ , we have a filtration:

$$K = L_0 \subset L_1 \subset L_2 \subset \cdots \subset L_n \subset \cdots \subset L$$

where  $L_n/L_{n-1}$  is a finite field extension. Let  $\bar{A}_i$  be the integral closure of  $A$  in  $L_i$ , and  $\bar{A} = \bigcup_{i=1}^{\infty} \bar{A}_i$ . For given prime ideals  $\mathfrak{q} \subset \mathfrak{p}$  in  $A$  and  $\mathfrak{Q}$  in  $\bar{A}$  such that  $\mathfrak{P} \cap A = \mathfrak{p}$ . Let  $\mathfrak{P}_n = \mathfrak{P} \cap L_n$ , and apply the going-down property for the finite field extension  $L_n/K$  to get  $\mathfrak{Q}_n \subset \mathfrak{P}_n$  in  $\bar{A}_n$  such that  $\mathfrak{Q}_n \cap A = \mathfrak{q}$ . Clearly,  $\bigcup_i \mathfrak{Q}_i \subset \bar{A}$  is a prime ideal and is what we need.

Observation 3: We may assume  $L/K$  is a normal finite extension.

We just take the normal closure of  $L$  then restrict the prime ideals.

Observation 4: For a finite normal extension  $L/K$ , we consider  $K \subset K^s \subset L$ , where  $K/K^s$  is separable and  $L/K^s$  is purely inseparable. Hence we just need to check two cases: finite Galois extension (normal and separable) and finite normal purely separable extension.

**Lemma 2.7.** *Suppose  $L/K$  is a finite Galois extension with Galois group  $G$ ,  $A$  is integrally closed in  $K$ , then for any prime ideal  $\mathfrak{p}$ ,  $G$  acts transitively on the set of prime ideals of  $B$  lying over  $\mathfrak{p}$ .*

*Proof.* Suppose  $\mathfrak{q}$  and  $\mathfrak{q}'$  are two prime ideals of  $B$  lying over  $\mathfrak{p}$ . We need to show there is  $\sigma \in G$  such that  $\sigma(\mathfrak{q}) = \mathfrak{q}'$ .

Claim:  $\mathfrak{q}' \subset \bigcup_{\sigma \in G} \sigma(\mathfrak{q})$ . For any  $x \in \mathfrak{q}'$  and  $y = \prod_{\sigma' \in G} \sigma'(x) \in K \in \mathfrak{q}'$ , hence  $y \in \mathfrak{q}' \cap K$ . Since  $A$  is integrally closed,  $y \in A$ , hence  $y \in \mathfrak{p}$  actually. So  $y \in \sigma(\mathfrak{q})$  for any  $\sigma \in G$ . Because  $\sigma(\mathfrak{q})$  is a prime ideal, there exists  $\sigma'(x) \in \sigma(\mathfrak{q})$ , then  $x \in \sigma'^{-1}\sigma(\mathfrak{q})$ . Thus  $\mathfrak{q} \subset \bigcup_{\sigma \in G} \sigma(\mathfrak{q})$ .

By prime avoidance, there exists a  $\sigma(\mathfrak{q})$  such that  $\mathfrak{q} \subset \sigma(\mathfrak{q})$ . However,  $\mathfrak{q}' \cap A = \sigma(\mathfrak{q}) \cap A = \mathfrak{p}$ , so  $\mathfrak{q}' = \sigma(\mathfrak{q})$ , because for integral domains,  $(0)$  is unique prime ideal lying over  $(0)$ .  $\square$

Note that if  $L/K$  is a finite normal and purely-inseparable field extension, then  $\text{Aut}(L/K) = \{\text{id}\}$  and we may assume the characteristic is  $p$ . For  $x \in L$ , there is some integer  $v$  such that  $x^{p^v} = \alpha \in K$  and  $x^{p^v} - \alpha$  is the minimal polynomial.

Recall a lemma in field theory:

**Lemma 2.8.** *Suppose  $K$  is of characteristic  $p$ , if  $f(x) \in K[x]$  is irreducible, then there exists a non-negative integer  $v$  and an irreducible separable polynomial  $g(x) \in K[x]$  such that  $f(x) = g(x^{p^v})$ .*

*Sketch proof.* We argue it by induction and notice that if  $f$  is not separable, then the formal derivation  $f' = 0$ , which means that for each non constant item  $x^m$ ,  $m$

is a multiple of  $p$ . Hence there is a polynomial  $f_1$  such that  $f(x) = f_1(x^p)$ . We proceed this procedure until we have a separable polynomial.  $\square$

**Lemma 2.9.** *Let  $A \subset B$  be integral domains and  $A$  is integrally closed. If  $x \in B$  is integral over an ideal  $A$ , then the minimal polynomial of  $x$  over  $K(A)$  is of the form*

$$x^n + \sum_{i=1}^n c_i x^{n-i}$$

where  $c_i \in A$ .

A proof for more general case is in P63 Proposition 5.15 in [Ati69].

*Proof.* Clearly,  $x$  is algebraic over  $K(A)$ , suppose the minimal polynomial is

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

and we let  $L$  be the splitting field of this irreducible polynomial, so all the conjugates  $x_1, \dots, x_n$  are in  $L$  and  $a_i$  is given by symmetric polynomials in  $x_i$ . Note  $x_i$  is integral over  $A$  as  $x$ , then the coefficients  $a_i$  are integral over  $A$ . Since  $A$  is integrally closed,  $a_i \in A$  for each  $i$ .  $\square$

**Lemma 2.10.** *Suppose  $L/K$  is a finite normal and purely inseparable extension, for any prime ideal  $\mathfrak{p} \in \text{Spec } A$ , the fiber over  $\mathfrak{p}$  consists of exactly one element.*

*Proof.* Suppose there are two prime ideals,  $\mathfrak{q}, \mathfrak{q}'$  of  $B$  lying over  $\mathfrak{p}$ . We need to show  $\mathfrak{q} = \mathfrak{q}'$ . Suppose  $x \in \mathfrak{q}$ , then  $x^{p^v} = \alpha \in A$  (due to previous lemma) for some integer  $v \in \mathbb{N}$ , so  $\alpha \in \mathfrak{q} \cap A = \mathfrak{p}$ , then  $x^{p^v} \in \mathfrak{q}'$  and  $x \in \mathfrak{p}'$ . Thus  $\mathfrak{q} \subset \mathfrak{q}'$ . Similarly, we have  $\mathfrak{q}' \subset \mathfrak{q}$ . Finally,  $\mathfrak{q} = \mathfrak{q}'$ .

The existence is given by Heuristic approach.  $\square$

**Theorem 2.11.** *Suppose  $f : A \rightarrow B$  is an integral extension between integral domains and  $A$  is integrally closed, then  $f^* : \text{Spec } B \rightarrow \text{Spec } A$  is an open map.*

*Proof.* Since Zariski topology is generated by distinguished open set  $D_x = \{\mathfrak{q} \in \text{Spec } B \mid x \notin \mathfrak{q}\}, x \in B$ , we just need to show  $f^*(D_x)$  is open.

Let the minimal polynomial of  $x$  over  $K = K(A)$  be

$$(3) \quad x^n + a_1 x^{n-1} + \cdots + a_n$$

where  $a_i \in A$  by Lemma 2.9, then we claim that  $f^*(D_x) = \bigcup_{i=1}^n D_{a_i}$ .

By previous lemmas, we first assume  $L/K$  is a Galois extension and  $B$  is the integral closure of  $A$  in  $L$  and let  $G$  be the Galois group. Note that for any prime ideal  $\mathfrak{q} \in \text{Spec } B$ ,  $f^*(\mathfrak{q}) = f^*(\sigma(\mathfrak{q}))$ . Then we have

$$\begin{aligned} f^*(D(x)) &= \bigcup_{\sigma \in G} f^*(\sigma(D_x)) \\ &= \bigcup_{\sigma \in G} f^*(D_{\sigma(x)}) \\ (4) \quad &= f^*\left(\bigcup_{\sigma \in G} D_{\sigma(x)}\right) \\ &= f^*(V(\{\sigma(x) \mid \sigma \in G\})^c) \end{aligned}$$

Note that  $a_i$  acts on  $B$  via the extension  $f$ , let  $a'_i = f(a_i)$  and we rewrite equation 3 to be

$$(5) \quad x^n + a'_1 x^{n-1} + \cdots + a'_n = 0$$

and if  $\mathfrak{q} \in V(\{\sigma(x) \mid \sigma \in G\})$ , then  $\mathfrak{q} \in V(a'_1, \dots, a'_n)$  because  $a'_i$  is given by polynomial in  $\sigma(x)$ . Conversely, if  $\mathfrak{q} \in V(a'_1, \dots, a'_n)$ , then consider  $B/\mathfrak{q}$ ,  $\bar{x}^n = 0$  in  $B/\mathfrak{q}$ , hence  $x \in \mathfrak{q}$ , moreover,  $\sigma(x) \in \mathfrak{q}$  for all  $\sigma \in G$ . Hence we have

$$V(\{\sigma(x) \mid \sigma \in G\}) = V(a'_1, \dots, a'_n)$$

Back to equation 4, we have

$$f^*(D_x) = f^*(V(a'_1, \dots, a'_n)^c) = f^*\left(\bigcup_{i=1}^n D_{a'_i}\right) = \bigcup_{i=1}^n f^*(D_{a'_i}) = \bigcup_{i=1}^n D_{a_i}$$

Then we may assume  $L/K$  is a finite normal and purely inseparable extension, then by Lemma 2.10,  $f^*$  is injective. For any  $x \in B$ , there is a natural number  $v$  such that  $x^{p^v} \in A$ , then  $f^*D_x = D_{x^{p^v}}$  clearly.  $f^*$  is an open map clearly.  $\square$

**Theorem 2.12.** *Following the condition in previous theorem,  $f: A \rightarrow B$  has the going-down property.*

*Proof.* We just follows Lemma 2.5 to show we have such minimal prime ideal that is contained in  $\mathfrak{q}_1$ . First, we can find  $\mathfrak{q}'$  such that  $\mathfrak{q}' \cap A$  is a minimal prime ideal contained in  $\mathfrak{p}_1$ . Then consider the induced map  $A/(\mathfrak{q}' \cap A) \rightarrow B/\mathfrak{q}'$  and we have  $\overline{\mathfrak{q}'_1}$  in  $B/\mathfrak{q}'$  such that  $\mathfrak{q}'_1 \cap A = \mathfrak{p}_1$ . Since the Galois group acts transitively on the fiber of  $\mathfrak{p}$ , then we can find  $\sigma$  in the Galois group such that  $\sigma(\mathfrak{q}'_1) = \mathfrak{q}_1$ , then  $\mathfrak{q} = \sigma(\mathfrak{q}')$  is what we need, because  $\sigma(\mathfrak{q}') \cap A = \mathfrak{p}$  and  $\mathfrak{q} \subset \mathfrak{q}_1$ .  $\square$

The trick of Galois group action( group action):

**Proposition 2.1.** *Let  $G$  be a finite group of automorphisms of a ring  $A$ ,  $\mathfrak{p}$  be a prime ideal of  $A^G$  ( $G$ -fixed points of  $A$ ) and  $X$  be a set of prime ideals  $\mathfrak{P}$  in  $A$  such that  $\mathfrak{P} \cap A^G = \mathfrak{p}$ , then  $G$  acts transitively on  $X$ .*

*Proof.* Let  $\mathfrak{P}$  and  $\mathfrak{P}'$  be two elements in  $X$ , we now claim that  $\mathfrak{P}' \subset \bigcup_{\sigma \in G} \sigma(\mathfrak{P})$ . If the claim is true, then by prime avoidance, there exists some  $\sigma' \in G$  such that  $\mathfrak{P}' \subset \sigma'(\mathfrak{P})$ . Since  $\mathfrak{P}' \cap A^G = \sigma'(\mathfrak{P}) \cap A^G = \mathfrak{p}$ , then  $\mathfrak{P}' = \sigma'(\mathfrak{P})$ .

Now we prove the claim: for any  $x \in \mathfrak{P}'$ , consider  $\prod_{\sigma \in G} \sigma(x) \in A^G \cap \mathfrak{P}' = \mathfrak{p}$ , then  $\prod_{\sigma \in G} \sigma(x) \in \mathfrak{P}$ . Hence there exists  $\sigma \in G$  such that  $\sigma(x) \in \mathfrak{P}$ , which is equivalent to say that  $x \in \sigma^{-1}\mathfrak{P}$ , then  $x \in \prod_{\sigma \in G} \sigma(x)$ .  $\square$

### 3. DIMENSION THEORY

**Definition 3.1.** Let  $A$  be a Noetherian semilocal ring and  $\mathfrak{m}$  be the Jacobson radical of  $A$ , for an ideal  $I$  in  $A$  satisfying  $\mathfrak{m}^v \subset I \subset \mathfrak{m}$  for some positive integer  $v$ , then we define the **associated graded ring**  $G_I(A)$  to be

$$G_I(A) = \bigoplus_{n=0}^{\infty} I^n / I^{n+1}$$

If  $M$  is a finitely generated  $A$ -module, then the **associated graded module** is defined as

$$G_I(M) = \bigoplus_{n=0}^{\infty} I^n M / I^{n+1} M.$$

*Remark 3.2.* Note that  $A/I$  is an Artin ring, we just need to show  $A/I$  is of dimension 0 i.e. every prime ideal in  $A$  that contains  $I$  is a maximal ideal. Let  $\mathfrak{p}$  be a prime ideal in  $A$  that contains  $I$ , then  $\mathfrak{m}^v \subset \mathfrak{p}$  and  $\mathfrak{m} \subset \mathfrak{p}$  so that the product of all maximal ideals in  $A$  is contained in  $\mathfrak{p}$ , hence  $\mathfrak{p}$  is one of maximal ideals.

**Proposition 3.1.** *Let  $A$  be a Noetherian semilocal ring and  $I$  is such a ideal in the previous definition, then*

$$\dim A = \dim G_I(A)$$

*Proof.* □

Application of dimension theory:

**Theorem 3.3** (Zariski lemma). *Suppose  $A$  is a finitely generated  $k$ -algebra and  $\mathfrak{m}$  is a maximal ideal of  $A$ , then  $A/\mathfrak{m}$  is a finite algebraic extension of  $k$ .*

*Proof.* Note that the dimension of  $A/\mathfrak{m}$  is 0, then the transcendental degree of  $A/\mathfrak{m}$  is 0, hence  $A/\mathfrak{m}$  is a algebraic extension of  $k$ . Since  $A/\mathfrak{m}$  is finitely generated,  $A/\mathfrak{m}$  is a finite  $k$  extension. □

#### 4. GEOMETRIC VIEWPOINT OF PRIMARY DECOMPOSITION

Given a spectrum  $\text{Spec } A$ , the associated points are the generic points of irreducible components of support of some global section i.e. for some  $s \in A$ ,

$$\text{Supp}(s) = \{\mathfrak{p} \in \text{Spec } A \mid \frac{s}{1} \neq 0 \in A_{\mathfrak{p}}\}$$

namely if  $\mathfrak{p} \in \text{Supp}(s)$ , then  $\text{Ann}(s) \subset \mathfrak{p}$ , which means that

$$\text{Supp}(s) = V(\text{Ann}(s))$$

For any  $A$ -module, we just take the global section of the quasicohherent sheaf  $\tilde{M}$  so that we can define associated point of  $A$ -modules.

The **isolated points** is the generic points of irreducible components of  $\text{Spec } A$  i.e. the support of the function 1, while the other associated points are called **embedded points**. (The ideal is to replace the category of  $A$ -modules by the category quasicohherent sheaves over  $\text{Spec } A$ , then think it geometrically.)

**Proposition 4.1.** *Suppose  $A$  is a reduced ring, then  $\text{Spec } A$  has no embedded points.*

*Proof.* If  $A$  is integral, for any non-zero  $a \in A$ ,  $\text{Ann}(a) = (0)$ , hence the support is  $\text{Spec } A$ . Since  $\text{Spec } A$  is irreducible, the unique associated point is the generic point of  $\text{Spec } A$  i.e.  $[(0)]$ .

For general case, if  $f \in A$  is a function on a reduced affine scheme  $\text{Spec } A$ , then claim that  $\text{Supp}(f) = \overline{D(f)}$ : first, clearly  $D(f) \subset \text{Supp}(f)$  and  $\text{Supp}(f)$  is a closed subset, we just need to show  $\text{Supp}(f)$  is the smallest closed set to contain  $D(f)$ . Suppose  $V(I) \supset D(f)$  for ideal  $I$ , then

$$I \subset \bigcap_{\mathfrak{p} \in D(f)} \mathfrak{p}$$



since  $A$  is reduced, so is  $A_f$ , hence  $I = 0$  in  $A_f$ , i.e. for any  $s \in I$ , there is a positive integer  $n$  such that  $sf^n = 0$  in  $A$ . Thus we have  $s^n f^n = 0$  and  $sf = 0$ , due to the reducedness. Then  $I \subseteq \text{Ann}(f)$ .

Now we conclude that, for any  $s \in I$ ,  $V(\text{Ann}(f)) \subset V(s)$ , then  $\text{Supp}(f) \subset V(I)$ .

Next to show  $\overline{D(f)}$  is the union of irreducible components that meets  $D(f)$ . Suppose  $V(\mathfrak{p})$  is an irreducible component of  $\text{Spec } A$  i.e.  $\mathfrak{p}$  is a minimal prime ideal in  $A$  and  $V(\mathfrak{p}) \cap D(f) \neq \emptyset$ , then there is a prime ideal  $\mathfrak{p}'$  such that  $\mathfrak{p} \subset \mathfrak{p}'$  and  $f \notin \mathfrak{p}'$  i.e.  $f \notin \mathfrak{p}$ , then  $\mathfrak{p} \in D(f)$ . Hence  $V(\mathfrak{p}) = \{\mathfrak{p}\} \subset \overline{D(f)}$ .

Therefore  $\text{Supp}(f)$  is a union of irreducible components and each irreducible component  $V(\mathfrak{p})$  has no embedded point (because  $A/\mathfrak{p}$  is an integral domain).  $\square$

An important property of associated points: The natural map

$$M \rightarrow \prod_{\text{associated primes } \mathfrak{p}} M_{\mathfrak{p}}$$

is injective. The elements in the kernel of this map vanishes at each associated points, which means that their support are empty, hence their zero functions on  $\text{Spec } A$  i.e. 0 in  $M$ .

## 5. REGULARITY AND DVRs

**Theorem 5.1.** *Suppose  $(A, \mathfrak{m}, k)$  is a Noetherian local ring, then  $\dim A \leq \dim_k \mathfrak{m}/\mathfrak{m}^2$ .*

*Proof.* Since  $A$  is a Noetherian,  $\mathfrak{m}$  is a finitely generated  $A$ -module. Then by Nakayama's lemma, we may assume  $\mathfrak{m} = (x_1, \dots, x_n)$  such that  $\{\overline{x_i}\}_{i=1}^n$  is a  $k$ -basis of vector space  $\mathfrak{m}/\mathfrak{m}^2$ . Then by Krull's height theorem,  $\mathfrak{m}$  is the minimal prime ideal that over  $(x_1, \dots, x_n)$ , then the height of  $\mathfrak{m}$  is not bigger than  $n$  i.e.  $\dim A \leq \dim_k \mathfrak{m}/\mathfrak{m}^2$ .  $\square$

**Definition 5.2.**  $(A, \mathfrak{m}, k)$  is a regular local ring, if  $A$  is a Noetherian ring and  $\dim A = \dim_k \mathfrak{m}/\mathfrak{m}^2$ . If a Noetherian ring  $A$  is said to be regular, then it is regular at all its prime ideal.

**Proposition 5.1.** *A dimension 0 Noetherian local ring is regular if and only if it is a field.*

*Proof.* The proof is straightforward, Since it is of dimension 0 and regular, then its maximal ideal is 0.  $\square$

**Lemma 5.3.** *A surjection between to integral domains of the same dimension is an isomorphism.*

*Proof.* Let  $A, B$  be two integral domain of the same dimension and  $f: A \rightarrow B$  be a surjective ring homomorphism. The kernel  $\ker f$  must be a prime ideal  $\mathfrak{p}$  with  $A/\mathfrak{p} \cong B$ . Since  $A/\mathfrak{p}$  and  $A$  have the same dimension,  $\mathfrak{p}$  must be a minimal prime ideal of  $A$ . Because  $A$  is an integral domain,  $\mathfrak{p} = 0$ , then  $f$  is an isomorphism.  $\square$

**Theorem 5.4.** *Suppose  $(A, \mathfrak{m}, k)$  is a regular local ring of dimension  $n$ , then  $A$  is an integral domain.*

*Proof.* We prove it by induction on  $n$ . When  $n = 0$ , it is clearly true by previous proposition. Suppose it is true for dimension less than  $n$ .

Take  $f \in \mathfrak{m}/\mathfrak{m}^2$ , then  $A/(f)$  is a Noetherian local ring. According to Krull's principal ideal theorem,  $\dim A/(f) \geq n - 1$ . Observe that the Zariski cotangent

space at  $A/(f)$  i.e.  $(\mathfrak{m}/(f))/(\mathfrak{m}/(f))^2 = (\mathfrak{m}/\mathfrak{m}^2)/(\bar{f})$  is of dimension  $n - 1$  clearly. By Theorem 5,  $A/(f)$  is a regular local ring of dimension  $n - 1$ . Apply the inductive hypothesis,  $A/(f)$  is an integral domain.

We just need to show that any minimal prime ideal in  $A$  is  $(0)$ . Let  $\mathfrak{p} \subset A$  be a minimal prime ideal, we claim that  $A/\mathfrak{p}$  is a regular local ring of dimension  $n$ . The Zariski cotangent space of  $A/\mathfrak{p}$  is a quotient of  $\mathfrak{m}/\mathfrak{m}^2$ , hence its dimension is at most  $n$ . Since  $\mathfrak{p}$  is a minimal prime ideal of  $A$ ,  $\dim A/\mathfrak{p} = \dim A = n$ , then by Theorem 5,  $A/\mathfrak{p}$  is a regular Noetherian local ring of dimension  $n$ . Now we replace  $A$  by  $A/\mathfrak{p}$  in the argument in the first paragraph, then  $A/(\mathfrak{p} + (f))$  is an integral domain. Note that the quotient morphism  $A/(f) \rightarrow A/(\mathfrak{p} + (f))$  is an isomorphism by Lemma 5.3.

Thus  $\mathfrak{p} = \mathfrak{p} + (f)$  i.e.  $\mathfrak{p} \subset fA$ . Every element in  $\mathfrak{p}$  is of the form  $fv$  for  $v \in A$ . Further, since  $f \notin \mathfrak{p}$ ,  $v \in \mathfrak{p}$ . We have  $\mathfrak{p} \subset f\mathfrak{p}$ , then  $\mathfrak{p} = f\mathfrak{p}$ . Then apply Nakayama's lemma (global version), we conclude that  $\mathfrak{p} = 0$ .  $\square$

Next we focus on the case of dimension 1.

**Theorem 5.5.** *Suppose  $(A, \mathfrak{m}, k)$  is a Noetherian local ring of dimension 1, then the following are equivalent:*

- (a)  $(A, \mathfrak{m})$  is regular.
- (b)  $\mathfrak{m}$  is principal
- (c) all the non-zero ideals are of the form  $\mathfrak{m}^n$ .
- (c)'  $A$  is a principal ideal domain.

*Proof.* (a)  $\implies$  (b): Since  $A$  is regular and  $\dim A = 1$ , then  $\dim_k \mathfrak{m}/\mathfrak{m}^2 = 1$ . Let  $u \in \mathfrak{m} \setminus \mathfrak{m}^2$  be a representative of a generator in  $\mathfrak{m}/\mathfrak{m}^2$ . By Nakayama's lemma,  $u$  generates  $\mathfrak{m}$ , hence  $\mathfrak{m}$  is a principal ideal.

(b)  $\implies$  (a): It is obvious. Since  $\mathfrak{m} = (t)$ , then  $\dim_k \mathfrak{m}/\mathfrak{m}^2 \leq 1$ , while  $1 = \dim A \leq \dim_k \mathfrak{m}/\mathfrak{m}^2$ . Thus  $\dim A = \dim_k \mathfrak{m}/\mathfrak{m}^2 = 1$  and  $A$  is regular.

(a)  $\implies$  (c): Let  $I \subset A$  be a non-zero ideal, then there exists  $n$  such that  $I \subset \mathfrak{m}^n$  and  $I \not\subset \mathfrak{m}^{n+1}$ . We take  $t \in I \setminus \mathfrak{m}^{n+1}$ . Note that  $\dim_k \mathfrak{m}^n/\mathfrak{m}^{n+1} = 1$  because  $\mathfrak{m}^n = (u^n)$  (recall previous argument), hence  $t$  generates  $\mathfrak{m}^n/\mathfrak{m}^{n+1}$  as a representative. By Nakayama's lemma,  $t$  generates  $\mathfrak{m}^n$ . Hence  $\mathfrak{m}^n = (t) \subset I \subset \mathfrak{m}^{n+1}$  and  $I = \mathfrak{m}^n$ . In total, all the non-zero ideals of  $A$  is of the form  $\mathfrak{m}^k$  for some positive integer  $k$ .

(c)  $\implies$  (a): Argue by contradiction. Suppose  $A$  is not regular, then  $\dim_k \mathfrak{m}/\mathfrak{m}^2$  is at least 2. Then there is an element  $x \in \mathfrak{m} \setminus \mathfrak{m}^2$ , such that  $\mathfrak{m}^2 \subsetneq (x, \mathfrak{m}^2) \subsetneq \mathfrak{m}$ , contradiction.

(c)' is equivalent to (c) clearly.  $\square$

**Definition 5.6.** Suppose  $K$  is a field, a **discrete valuation** on  $K$  is a function  $v: K^* \rightarrow \mathbb{Z}$  such that  $v(xy) = v(x) + v(y)$  and if  $x + y \neq 0$ ,

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

(we set  $v(0) = \infty$  for convenience). The **valuation ring**  $\mathcal{O}_v$  with respect to  $v$  is defined to be

$$\mathcal{O}_v = \{x \in K \mid v(x) \geq 0\}$$

We say a ring  $A$  is a **discrete valuation ring** or **DVR** if there is a discrete valuation  $v$  on the fraction field  $K = K(A)$  such that  $A$  is the valuation ring with respect to  $v$ .

**Proposition 5.2.**  $(A, \mathfrak{m})$  is a DVR if and only if it satisfies the one of the equivalent conditions in 5.5.

*Proof.* We first to show a DVR is a Noetherian local principal ideal domain. First, it is a local ring: let  $\mathfrak{m} = \{x \in A \mid v(x) > 0\}$ , it is an ideal clearly. For  $x \in A \setminus \mathfrak{m}$ , then  $v(x) = 0$  and  $v(x^{-1}x) = v(x^{-1}) + v(x) = v(1) = 0$ , then  $v(x^{-1}) = 0$  with  $x^{-1} \in A$ . Hence  $\mathfrak{m}$  is the unique maximal ideal in  $A$ . Next to show  $\mathfrak{m}$  is a principal ideal: take  $t \in \mathfrak{m}$  such that  $v(t) = 1$ , then for any  $x \in \mathfrak{m}$   $v(xt^{-1}) = v(x) - v(t) \geq 0$  hence  $xt^{-1} \in A$  and  $\mathfrak{m} = (t)$ . Let  $I_n = \{x \in A \mid v(x) \geq n\}$ , then we have a filtration

$$A = I_0 \supsetneq \mathfrak{m} = I_1 \supsetneq I_2 \supsetneq I_3 \supsetneq I_4 \cdots \supsetneq I_n \supsetneq \cdots$$

We claim that all the non-zero ideals are of the form  $I_n$ . Let  $I \subset A$  be an ideal, then take  $x \in I$  such that  $v(x) = n$  is the least one in  $I$ , then  $I \subset I_n$ . Conversely, for any  $y \in I$ ,  $v(x^{-1}y) = v(y) - v(x) \geq 0$ , then  $x^{-1}y \in A$ , hence  $I = (t)$ . Similarly,  $(t) = I_n$ . Now we have proven the claim. In particular, suppose  $\mathfrak{m} = (u)$ , all the non-zero ideals are of the form  $(u^n)$ . Then  $A$  is a principal ideal domain of dimension 1 (it is a domain because it is a subring of a field). Hence  $A$  satisfies the conditions in Theorem 5.5.

Conversely, suppose  $A$  is a regular Noetherian local and  $\mathfrak{m} = (u)$ , we define the valuation on  $K = K(A)$  by sending  $v(u) = 1$  and  $v(i) = 0$  if  $i$  is a unit in  $A$ . Claim that all non-zero element in  $K$  is of the form  $au^n$  with an integer  $n$ : for any  $x, y \in A$ , they are of the forms  $x = bu^n$  and  $y = cx^m$  for  $b, c \in A^*$  and non-negative integers  $n, m$ , then

$$\frac{x}{y} = bc^{-1}x^{n-m}$$

where  $bc^{-1}$  is still a unit in  $A$ . Hence we prove the claim and following the claim, the valuation is well-defined by extending  $v(ax^n) = n$ . Clearly, if  $v(x) \geq 0$ , then  $x \in A$ . Hence  $A$  is a DVR.  $\square$

**Theorem 5.7.** Suppose  $(A, \mathfrak{m})$  is a Noetherian local domain of dimension 1, then  $A$  is a DVR if and only if  $A$  is integrally closed.

*Proof.* When  $A$  is a DVR, it is a principal ideal domain, in particular, it is a UFD, hence it is integrally closed. Conversely, suppose  $A$  is integrally closed, we are going to show that  $\mathfrak{m}$  is a principal ideal. For any non-zero  $x \in \mathfrak{m}$ ,  $(x)$  is a  $\mathfrak{m}$ -primary (because  $\mathfrak{m}$  is of height 1 i.e. the unique non-zero prime ideal in  $A$ ). Then  $\sqrt{(x)} = \mathfrak{m}$  i.e. for any  $y \in \mathfrak{m}$ , there exists a positive integer  $n_y$  such that  $y^{n_y} \in (x)$ . Since  $\mathfrak{m}$  is finitely generated, there exists  $n$  such that  $\mathfrak{m}^n \subseteq (x)$  and  $\mathfrak{m}^{n-1} \not\subseteq (x)$ . Choose  $y \in \mathfrak{m}^{n-1}$  such that  $y \notin (x)$ , then  $\frac{y}{x}\mathfrak{m} \subseteq \frac{1}{x}\mathfrak{m}^n \subseteq A$ , hence  $\frac{y}{x}\mathfrak{m}$  is an ideal in  $A$  and either  $\frac{y}{x}\mathfrak{m} \subset \mathfrak{m}$  or  $\frac{y}{x}\mathfrak{m} = A$ . We want to show that  $\frac{y}{x}\mathfrak{m} = A$  then  $\mathfrak{m} = \frac{x}{y}A$  is a principal ideal.

It suffices to show that  $\frac{y}{x}\mathfrak{m} \not\subseteq \mathfrak{m}$  and we argue by contradiction. Suppose  $\frac{y}{x}\mathfrak{m} \subset \mathfrak{m}$ , then  $\frac{y}{x}$  determines an  $A$ -linear map from finitely generated  $A$ -module  $\mathfrak{m}$  to itself. Take a list of generators and we have an  $A$ -matrix  $T$ . Note that  $T - \frac{y}{x}I = 0$  and  $\det(T - \frac{y}{x}I) = 0$ , hence the monic polynomial with coefficients in  $A$  is  $\det(T - tI)$  in variable of  $t$ . Then  $\frac{y}{x}$  is integral over  $A$  and  $\frac{y}{x} \in A$  because  $A$  is integrally closed. Hence  $y \in (x)$ , which leads to contradiction.  $\square$

## 6. DECOMPOSITION AND DEDEKIND DOMAIN

We first do some observation: suppose  $A$  is a Noetherian domain and  $\mathfrak{a} \subseteq A$  is a non-zero ideal. We have known that the primary decomposition exists, hence

$$\mathfrak{a} = \bigcap_{\text{primary}} \mathfrak{q}$$

If  $A$  is of dimension 1, then every non-zero prime ideal is a maximal ideal and for a primary decomposition, there is no embedded prime in the set of associated prime ideals of  $\mathfrak{a}$ . Note that for two distinct primary ideals  $\mathfrak{q}$  and  $\mathfrak{q}'$  where  $\sqrt{\mathfrak{q}} = \mathfrak{m}$  and  $\sqrt{\mathfrak{q}'} = \mathfrak{m}'$  are two distinct maximal ideal, then claim that  $\mathfrak{q} + \mathfrak{q}' = 1$ . If  $\mathfrak{q} + \mathfrak{q}' \neq 1$ , then there exists a maximal ideal  $\mathfrak{m}''$  to contain  $\mathfrak{q} + \mathfrak{q}'$ , further  $\mathfrak{m}''$  contain  $\sqrt{\mathfrak{q}}$  and  $\sqrt{\mathfrak{q}'}$  i.e.  $\mathfrak{m}''$  contain  $\mathfrak{m} + \mathfrak{m}' = (1)$ , contradiction. Since all distinct primary ideals are coprime, we may write

$$\mathfrak{a} = \prod_{\text{primary}} \mathfrak{q}$$

Now the question is: **when would every  $\mathfrak{p}$ -primary ideal of  $A$  be a power of  $\mathfrak{p}$ ?** The answer is when  $A$  is integrally closed (necessary and sufficient condition). Now we move on to this answer.

Observation

- $\mathfrak{q}$  is  $\mathfrak{p}$ -primary in  $A$  if and only if  $\mathfrak{q}A_{\mathfrak{p}}$  is  $\mathfrak{p}A_{\mathfrak{p}}$ -primary.
- when  $\mathfrak{q}$  is  $\mathfrak{p}$ -primary, then  $\mathfrak{q} = \mathfrak{p}^n$  if and only  $\mathfrak{q}A_{\mathfrak{p}} = (\mathfrak{p}A_{\mathfrak{p}})^n$ .

Hence we may reduce the question to local case.

Now the question is: **For a Noetherian local domain  $(A, \mathfrak{m})$  of dimension 1, when would every  $\mathfrak{m}$ -primary ideal be a power of  $\mathfrak{m}$ ?**

Further observation:

- Every non-zero ideal in  $A$  is  $\mathfrak{m}$ -primary.
- $\mathfrak{q}$  is  $\mathfrak{m}$ -primary if and only if  $\sqrt{\mathfrak{q}} = \mathfrak{m}$ .

Thus, the local question becomes: **For a Noetherian local domain  $(A, \mathfrak{m})$  of dimension 1, when would every non-zero ideal be of the form  $\mathfrak{m}^n$ ,  $n \in \mathbb{N}$ ?**

Recall Theorem 5.5, we see that the answer is DVR!

**Theorem 6.1.** *Let  $A$  be a Noetherian domain of dimension 1, then every primary decomposition is a prime decomposition if and only if for each non-zero prime ideal  $\mathfrak{p}$ ,  $A_{\mathfrak{p}}$  is a DVR.*

Recall that  $A$  is integrally closed if and only if  $A_{\mathfrak{p}}$  is integrally closed for each prime ideal  $\mathfrak{p} \in \text{Spec } A$ . Then by Theorem 5.7, we have

**Theorem 6.2.** *Let  $A$  be a Noetherian domain of dimension 1, then every primary decomposition is a prime decomposition if and only if  $A$  is integrally closed.*

**Definition 6.3.**  $A$  is a Dedekind domain if  $A$  is an integrally closed Noetherian domain of dimension 1.

**Example 6.4.** Let  $K$  be a finite field extension of  $\mathbb{Q}$  and  $\mathcal{O}_K$  be the integral closure of  $\mathbb{Z}$  in  $K$  (we may also call it the ring of integers in  $K$ .) Now we claim that  $\mathcal{O}_K$  is a Dedekind domain.

First,  $\mathcal{O}_K$  is integrally closed clearly. Second,  $\mathbb{Z} \hookrightarrow \mathcal{O}_K$  is an integral morphism, and  $\mathbb{Z}$  is a Dedekind domain clearly, hence by going-up and going-down,  $\dim \mathcal{O}_K = \dim \mathbb{Z} = 1$ . Finally, it remains to show  $\mathcal{O}_K$  is a Noetherian. We need the following lemma to show it.

**Lemma 6.5.** *Given a domain  $A$  and  $K = K(A)$  the fraction field with characteristic 0, let  $L/K$  be a finite separable extension of degree  $n$  and  $B$  be the integral closure of  $A$  in  $L$ . Then there exists a basis  $\{v_1, \dots, v_n\}$  in  $L$  such that*

$$B \subseteq Av_1 + \dots + Av_n$$

Thus, as a consequence, if  $A$  is Noetherian, so is  $B$ .

*Proof.* Observe that for any non-zero  $v \in L$ , there is an  $a \in A$  such that  $av \in B$  (there is an  $a$  such that  $av$  is integral over  $A$  because  $v$  is algebraic over  $K$ , the fraction field of  $A$ .)

Thus we may assume  $\{w_1, \dots, w_n\}$  is a basis of  $L$  over  $K$  with  $w_i \in B$ . Note that  $\langle v, v' \rangle = \text{Tr}(vv')$  is a non-degenerate bilinear form of  $L$  over  $K$  when it is separable. Let  $(v_1, \dots, v_n)$  be the dual basis of  $(w_1, \dots, w_n)$  namely  $\langle v_i, w_j \rangle = \delta_{ij}$  for each  $i, j$ .  $((v_1, \dots, v_n)$  is still a basis of  $L$  over  $K$  because they are linearly independent.)

Then  $\forall b \in B$ , write  $b = \sum_{i=1}^n \alpha_i v_i$  where  $\alpha_i \in K$ . Then

$$\langle b, w_j \rangle = \sum_{i=1}^n \alpha_i \langle v_i, w_j \rangle = \sum_{i=1}^n \alpha_i \delta_{ij} = \alpha_j$$

because  $bw_j \in B$ ,  $\text{Tr}(bw_j) \in B$  (the trace is the sum of all its Galois conjugate elements and all its Galois conjugate elements is integral over  $K$  clearly), then  $\text{Tr}(bw_j) = B \cap K = A$  i.e.  $\alpha_j \in A$ .  $\square$

In general, there is proposition:

**Theorem 6.6** (Krull-Akizuki). *Let  $A$  be a Noetherian domain of dimension 1 with fraction field  $K$ , if  $L/K$  is a finite extension and  $B \subset L$  is an arbitrary subring that contains  $A$ , then  $B$  is a Noetherian domain.*

We need to prove that for any ideal  $I$  in  $B$ ,  $I$  is a finitely generated  $B$ -module. Observe that  $I \otimes_A K$  is a  $K$ -vector space in  $L$ , hence  $I \otimes_A K$  is of finite dimension, namely we say that  $I$  is an  $A$ -module of finite rank. We need the following lemma to prove the theorem.

**Lemma 6.7.** *Let  $A$  and  $L$  be the ones in the assumption of the theorem and let  $M$  be a torsion-free  $A$ -module of finite rank  $r$ . Then for  $0 \neq a \in A$ , we have*

$$l(M/aM) \leq r * l(A/aA)$$

*Proof.* First, we assume  $M$  is finitely generated. Take  $x_1, \dots, x_r$  in  $M$  linearly independent over  $A$  and let  $E = \oplus_{i=1}^r Ax_i$ , then there exists  $t \in A$  such that for any  $y \in M$ ,  $ty \in E$  (We just find such  $t'$  for each generator of  $M$ , then multiply them together to get such  $t$ ). Let  $C = M/E$  and  $tC = 0$  i.e.  $C$  is totally an  $A$ -torsion module and is finitely generated obviously. Then there exists a filtration of  $C$ :

$$C = C_0 \supset C_1 \supset \dots \supset C_n = 0$$

such that  $C_i/C_{i+1} = A/\mathfrak{p}_i$  for some non-zero prime ideal  $\mathfrak{p}_i$  and actually, such prime ideals are maximal ideals (the existence of this filtration is in Professor Qiu's notes Proposition 4.11 P75 and since  $A$  is an integral domain of dimension 1, every non-zero prime ideal is a maximal ideal). Hence  $C$  is of finite length clearly. For any  $0 \neq a \in A$  and any positive integer  $n$ , we have an exact sequence

$$E/a^n E \longrightarrow M/a^n M \longrightarrow C/a^n C \longrightarrow 0$$

this gives

$$(6) \quad l(M/a^n M) \leq l(E/a^n E) + l(C)$$

Since  $M$  and  $E$  are torsion-free, we have  $a^i E/a^{i+1} E \cong E/aE$  and similar for  $M$ , then we may rewrite the equation 6 into

$$(7) \quad nl(M/aM) \leq nl(E/a^n E) + l(C)$$

for each  $n$ . Thus  $l(M/aM) \leq l(E/aE)$ . Note that  $E \cong A^r$ , hence  $l(E/aE) = rl(A/aA)$ . This completes the proof in the case finitely generated modules.

In general case, take any finitely generated submodule  $\overline{N}$  in  $M/aM$  and let  $N$  be the preimage of  $\overline{N}$  in  $M$ , which is finitely generated. Then

$$l(\overline{N}) = l(N/(N \cap aM)) \leq l(N/aN) \leq rl(A/aA)$$

Since this inequation is independence of the choice of finitely generated submodules in  $M/aM$ , so that  $\overline{M}$  is in fact finitely generated, otherwise we can find a finitely generated submodule in  $\overline{M}$  of arbitrarily length. Hence  $l(M/aM) \leq rl(A/aA)$ .  $\square$

*Remark 6.8.* We need  $C$  to be torsion, otherwise, consider  $C = \mathbb{Z}^2$  and  $A = \mathbb{Z}$ , which is not of finite length.

Now we prove the theorem.

*Proof of the theorem.* We may replace the field  $L$  by the fraction field of  $B$ . For any non-zero ideal  $I$  in  $B$ ,  $I$  is a finite rank  $A$ -module. Take  $0 \neq a \in I \cap A$ ,  $l(I/aI) \leq l(A/aA)$ . By Krull's principal ideal theorem,  $A/aA$  is of dimension 0, then  $A/aA$  is an Artinian ring (Noetherian and dimension 0), hence  $l(A/aA)$  is finite. Thus  $l(I/aI)$  is finite i.e.  $I/aI$  is a finite length  $A$ -module. Moreover,  $I$  is a finitely generated  $B$ -module.  $\square$

*Remark 6.9.* Actually, such  $B$  is of dimension at most 1. If  $P$  is a non-zero prime ideal in  $B$ ,  $B/P$  is a Noetherian domain of dimension 0 i.e. an Artinian ring, therefore  $B/P$  is a field, namely  $P$  is a maximal ideal and  $\dim B = 1$ .

## 7. DERIVED GEOMETRY

### REFERENCES

[Ati69] Michael Atiyah, *Introduction to commutative algebra*, Addison-Wesley, 1969.

SUSTECH

Email address: 11711505@mail.sustech.edu.cn