

# Commutative Algebra

Keri Ann Sather-Wagstaff  
(Notes by Shuai Wei)

September 17, 2023



# Contents

<b>Introduction</b>	<b>1</b>
<b>1 Rings and Ideals</b>	<b>3</b>
Rings and Ring Homomorphisms . . . . .	3
Ideals and Generators . . . . .	4
Local Rings . . . . .	7
The Nilradical . . . . .	8
The Jacobson Radical . . . . .	9
Operations on Ideals . . . . .	9
Sum of Ideals . . . . .	9
Products of Ideals . . . . .	11
Prime Avoidence . . . . .	14
Colon Ideals . . . . .	15
Radicals of Ideals . . . . .	17
Extensions and Contractions . . . . .	19
Power Series Rings . . . . .	21
U.F.D. . . . .	26
Generalization of U.F.D. . . . .	27
<b>2 Zariski Topology</b>	<b>29</b>
Subspaces . . . . .	33
Continuous Functions and Homeomorphisms . . . . .	34
<b>3 Localization</b>	<b>41</b>
<b>4 Primary Decomposition</b>	<b>53</b>
<b>5 Modules and Integral Dependence</b>	<b>65</b>
Modules . . . . .	65
Integral Dependence . . . . .	66
<b>6 Appendix</b>	<b>77</b>
Hilbert–Samuel Multiplicity . . . . .	77

# Introduction

The study and application of commutative rings with identity.

(a) Commutative algebra in calculus. We have  $\mathcal{C}(\mathbb{R}) = \{\text{continuous functions } \mathbb{R} \rightarrow \mathbb{R}\}$  and  $\mathcal{D}(\mathbb{R}) = \{\text{differentiable functions } \mathbb{R} \rightarrow \mathbb{R}\}$  are both commutative rings with identity.

(b) Commutative algebra in graph theory. Let  $G$  be a finite simple graph with vertex set  $V = \{v_1, \dots, v_d\}$ . The *edge ideal* of  $G$  is  $I(G) = \langle v_i v_j \mid v_i v_j \text{ is an edge in } G \rangle \leq K[v_1, \dots, v_d]$ .

algebraic properties of  $I(G) \iff$  combinatorial properties of  $G$ .

(c) Commutative algebra in combinatorics. A simplicial complex  $\Delta$  on  $V$ . Stanley-Reisner ideal  $J(\Delta) \leq K[v_1, \dots, v_d]$ .

algebraic properties of  $J(\Delta) \iff$  combinatorics properties of  $\Delta$ .

Let  $\mathcal{P}$  be a poset and  $\Delta(\mathcal{P}) = \text{“order complex of } \mathcal{P}\text{”} = \{\text{chains in } \mathcal{P}\}$ . Study  $\mathcal{P}$  via  $J(\Delta(\mathcal{P}))$ .

(d) Commutative algebra in number theory. Number theory is the study of solutions of polynomial equations over  $\mathbb{Z}$ . Given an intermediate field  $\mathbb{Q} \subseteq K \subseteq \mathbb{C}$ , let

$$R = \{\alpha \in K \mid \exists \text{ an monic } f \in \mathbb{Z}[x] \text{ s.t. } f(\alpha) = 0\},$$

then  $\mathbb{Z} \subseteq R \subseteq K$  are subrings. (Chapter 5)

(e) Commutative algebra in algebraic geometry. Algebraic geometry is the study of solution sets for systems of polynomial equations over fields. Let  $k$  be a field,  $f_1, \dots, f_m \in k[X_1, \dots, X_d]$ ,

$$V := V(f_1, \dots, f_m) = \{\underline{x} \in k^d \mid f_i(\underline{x}) = 0, \forall i = 1, \dots, m\},$$

where  $V$  is for “variety”, and

$$I(V) = \{f \in k[X_1, \dots, X_d] \mid f(\underline{x}) = 0, \forall \underline{x} \in V\} \leq k[X_1, \dots, X_d].$$

algebraic properties of  $I(V) \iff$  geometric properties of  $V$ .

Why modules? Because in number theory,  $R = \{\alpha \in K \mid \exists \text{ monic } f \in \mathbb{Z}[x] \text{ s.t. } f(\alpha) = 0\}$  is a subring of  $K$ .

**Challenge-exercise:** prove this by definition. For  $\alpha, \beta \in R$ , note there exist  $f, g \in \mathbb{Z}[X]$  monic such that  $f(\alpha) = 0 = f(\beta)$ , then try to prove or construct monic polynomials  $s, d, p \in \mathbb{Z}[X]$  such that  $s(\alpha + \beta) = 0$ ,  $d(\alpha - \beta) = 0$  and  $p(\alpha\beta) = 0$ .

Proof is a straightforward application of modules.

Why topology? To study geometry, need continuity. Let  $V = V(f_1, \dots, f_m)$ ,  $W = V(g_1, \dots, g_n)$  and  $\phi : V \rightarrow W$ . What does it mean for  $\phi$  to be continuous if  $k = \mathbb{F}_3$ ? Need a notion of open sets in  $V$  and  $W$ .

# Chapter 1

## Rings and Ideals

Let  $R$  be a commutative ring with identity.

### Rings and Ring Homomorphisms

**Fact 1.1.**  $R = 0$  if and only if  $1_R = 0_R$ .

**Fact 1.2.** (a)  $1_R$  and  $0_R$  are both unique.

(b) For any  $r \in R$ ,  $-r$  is unique.

(c) If  $r \in R$  is a unit, then there exists a unique  $r^{-1} \in R$  such that  $rr^{-1} = 1_R = r^{-1}r$ .

**Definition 1.3.** A *(unital) homomorphism of commutative rings with identity* is a function  $\phi : R \rightarrow S$  with  $R$  and  $S$  commutative rings with identity, such that for all  $r, r' \in R$ ,

(a)  $\phi(r + r') = \phi(r) + \phi(r')$ ,

(b)  $\phi(rr') = \phi(r)\phi(r')$ ,

(c)  $\phi(1_R) = 1_S$ .

It is also known as “ring homomorphism”.

**Fact 1.4.** Let  $\phi : R \rightarrow S$  be a ring homomorphism.

(a)  $\phi(0_R) = 0_S$ .

(b)  $\phi(-r) = -\phi(r)$  for  $r \in R$ .

(c)  $\phi(r - s) = \phi(r) - \phi(s)$  for  $r, s \in R$ .

(d)  $\phi(\sum_{i=1}^m r_i s_i) = \sum_{i=1}^m \phi(r_i)\phi(s_i)$  for  $r_1, \dots, r_m, s_1, \dots, s_m \in R$ .

(e) If  $r$  is a unit in  $R$ , then  $\phi(r)$  is a unit in  $S$  and  $\phi(r)^{-1} = \phi(r^{-1})$ .

(f) A composition of ring homomorphisms is a ring homomorphism.

**Definition 1.5.** A *subring* of  $R$  is a subset  $S \subseteq R$  such that  $S$  is a commutative ring with identity under the operations for  $R$  and such that  $1_S = 1_R$ , i.e.,  $1_R \in S$ .

**Fact 1.6** (Subring test). A subset  $S \subseteq R$  is a subring if and only if it is closed under  $+$ ,  $\cdot$ ,  $-$  and  $1_R \in S$ .

**Example 1.7.** Subring test: need  $\emptyset \neq S \subseteq R$ ,  $S$  is closed under  $+$ ,  $\cdot$ ,  $-$  and  $1_R \in S$ .

If  $S$  is not closed under  $-$ , then fail. Let  $\mathbb{N}_0 = \{0, 1, 2, \dots\} \subseteq \mathbb{Z}$  not a subring.

If  $1_R \notin S$ , then fail. Let  $R = \mathbb{F}_3 \times \mathbb{F}_3 \supseteq \{(a, a) \mid a \in \mathbb{F}_3\} =: S$ . Then  $S$  is a subring of  $R$ . Although  $S_1 := \{(a, 0) \mid a \in \mathbb{F}_3\} \cong \mathbb{F}_3 \cong \{(0, a) \mid a \in \mathbb{F}_3\} =: S_2$  are rings but not subrings of  $R$  since  $1_R = (1, 1) \notin S_1$  and  $1_R = (1, 1) \notin S_2$ .

**Fact 1.8.** If  $S \subseteq R$  is a subring, then the inclusion map  $\varepsilon : S \rightarrow R$  given by  $\varepsilon(s) = s$  is a ring homomorphism.

## Ideals and Generators

**Definition 1.9.** An *ideal* of  $R$  is a non-empty subset  $\mathfrak{a} \subseteq R$ , an additive subgroup such that for all  $r \in R$  and  $a \in \mathfrak{a}$ ,  $ra \in \mathfrak{a}$ , i.e., closed under scalar multiplication.

An ideal  $\mathfrak{a} \leq R$  is *prime* if  $\mathfrak{a} \neq R$  and for any  $a, b \in R$ , if  $a, b \notin \mathfrak{a}$ , then  $ab \notin \mathfrak{a}$ , i.e., if  $ab \in \mathfrak{a}$ , then  $a \in \mathfrak{a}$  or  $b \in \mathfrak{a}$ .

An ideal  $\mathfrak{a} \leq R$  is *maximal* if  $\mathfrak{a} \neq R$  and for any ideal  $\mathfrak{b} \leq R$ , if  $\mathfrak{a} \subseteq \mathfrak{b} \subseteq R$ , then either  $\mathfrak{a} = \mathfrak{b}$  or  $\mathfrak{b} = R$ .

**Fact 1.10** (Ideal test). If  $\mathfrak{a} \neq \emptyset$  and  $\mathfrak{a}$  is closed under scalar multiplication  $\cdot$ , then  $-a = (-1_R)a \in \mathfrak{a}$  for  $a \in \mathfrak{a}$ , also, since  $\mathfrak{a}$  is closed under  $+$ , it is automatically closed under  $-$ .

Thus, A subset  $\mathfrak{a} \subseteq R$  is an ideal if and only if  $\mathfrak{a} \neq \emptyset$  and  $\mathfrak{a}$  is closed under  $+$  and scalar multiplication  $\cdot$ .

**Example 1.11.** (a) Let  $R = \mathbb{Z}$ , then ideals of  $R$  are of the form  $n\mathbb{Z} = \{nm \mid m \in \mathbb{Z}\}$ , where  $n \in \mathbb{Z}$ .

$n\mathbb{Z}$  is prime if and only if  $n = 0$  or  $|n|$  is prime.

$n\mathbb{Z}$  is maximal if and only if  $|n|$  is prime.

(b) If  $I_\lambda \leq R$  for  $\lambda \in \Lambda$ , then  $\bigcap_{\lambda \in \Lambda} I_\lambda \leq R$ .

(c) If  $r_1, \dots, r_m \in R$ , then

$$\begin{aligned} \langle r_1, \dots, r_m \rangle &= \langle r_1, \dots, r_m \rangle R = (r_1, \dots, r_m) = (r_1, \dots, r_m)R = \bigcap_{r_1, \dots, r_m \in I \leq R} I \\ &= \left\{ \sum_{i=1}^m a_i r_i \mid a_i \in R, \forall i = 1, \dots, m \right\} \leq R. \end{aligned}$$

In particular,

$$\langle r \rangle = \langle r \rangle R = (r) = (r)R = rR = Rr = \{ar \mid a \in R\} = \bigcap_{r \in I \leq R} I, \forall r \in R.$$

(d) If  $A \subseteq R$ , then  $\langle A \rangle = \bigcap_{A \subseteq I \leq R} I$  and

$$\langle A \rangle = RAR = AR = RA = \left\{ \sum_{a \in A}^{\text{finite}} r_a a \mid r_a \in R, \forall a \in \mathfrak{a} \right\}.$$

**Fact 1.12.** For any  $r_1, \dots, r_m \in R$ ,  $\langle r_1, \dots, r_m \rangle$  is the smallest ideal of  $R$  containing  $r_1, \dots, r_m$ , i.e., for any  $\mathfrak{a} \leq R$ ,  $r_1, \dots, r_m \in \mathfrak{a}$  if and only if  $\langle r_1, \dots, r_m \rangle \subseteq \mathfrak{a}$ . Similarly,  $A \subseteq \mathfrak{a}$  if and only if  $\langle A \rangle \subseteq \mathfrak{a}$ , e.g., if  $A \leq R$ , then  $A = \langle A \rangle$ .

**Construction 1.13.** Let  $\mathfrak{a} \leq R$ . For any  $r \in R$ ,  $r + \mathfrak{a} = \{r + a \mid a \in \mathfrak{a}\} = \bar{r}$ . Let

$$R/\mathfrak{a} := \{r + \mathfrak{a} \mid r \in R\}.$$

Then  $R/\mathfrak{a}$  is a commutative ring with identity with  $\bar{r} \pm \bar{s} = \overline{r \pm s}$ ,  $\bar{r}\bar{s} = \overline{rs}$ ,  $0_{R/\mathfrak{a}} = \overline{0_R}$  and  $1_{R/\mathfrak{a}} = \overline{1_R}$ .

Let  $\pi : R \rightarrow R/\mathfrak{a}$  be given by  $\pi(r) = \bar{r}$ . Then  $\pi$  is a well-defined ring epimorphism.

(UMP) For any  $\phi : R \rightarrow S$  ring homomorphism, if  $\phi(\mathfrak{a}) = 0$ , then there exists a unique ring homomorphism  $\bar{\phi} : R/\mathfrak{a} \rightarrow S$  making the following diagram commute.

$$\begin{array}{ccc} R & \xrightarrow{\phi} & S \\ \pi \downarrow & \nearrow \bar{\phi} & \uparrow \\ R/\mathfrak{a} & & \end{array}$$

$r \mapsto \phi(r)$   
 $\bar{r} \mapsto \bar{\phi}(\bar{r})$   
 $\exists ! \bar{\phi}$

Note  $\phi(\mathfrak{a}) = 0$  if and only if  $\mathfrak{a} \subseteq \text{Ker}(\phi)$ . In particular, if  $\mathfrak{a} = \langle A \rangle$ , then  $\mathfrak{a} \subseteq \text{Ker}(\phi)$  if and only if  $A \subseteq \text{Ker}(\phi)$ .

**Fact 1.14.** Let  $\mathfrak{a} \leq R$ .

- (a)  $\mathfrak{a}$  is prime if and only if  $R/\mathfrak{a}$  is an integral domain.
- (b)  $\mathfrak{a}$  is maximal if and only if  $R/\mathfrak{a}$  is a field.
- (c) If  $R$  is a field, then it is an integral domain.

So if  $\mathfrak{a}$  is maximal, then  $\mathfrak{a}$  is prime.

**Fact 1.15** (Ideal correspondence for quotients). Let  $\mathfrak{a} \leq R$  and  $\pi : R \rightarrow R/\mathfrak{a}$  be the canonical ring epimorphism.

$$\begin{aligned} \{\text{ideals } I \leq R/\mathfrak{a}\} &\rightleftarrows \{\text{ideals } J \leq R \mid \mathfrak{a} \subseteq J\} \\ I &\mapsto \pi^{-1}(I) = \{r \in R \mid r + \mathfrak{a} \in I\} \supseteq \pi^{-1}(0) = \mathfrak{a} \\ J/\mathfrak{a} &\leftarrow J \supseteq \mathfrak{a} \\ \{\text{ideals } I \leq R/\mathfrak{a}\} &\rightleftarrows \{\text{ideals } J \leq R \mid \mathfrak{a} \subseteq J\} \\ \{\text{primes ideals of } R/\mathfrak{a}\} &\rightleftarrows \{\text{prime ideals } \mathfrak{p} \leq R \mid \mathfrak{a} \subseteq \mathfrak{p}\} \\ \{\text{maximal ideals of } R/\mathfrak{a}\} &\rightleftarrows \{\text{maximal ideals } \mathfrak{m} \leq R \mid \mathfrak{a} \subseteq \mathfrak{m}\}. \end{aligned}$$



In both  $R$  and  $R/\mathfrak{a}$ , maximal ideals are a subset of prime ideals and prime ideals are a subset of ideals.

Claim.  $\frac{R/\mathfrak{a}}{J/\mathfrak{a}} \cong \frac{R}{J}$ .

$$\begin{array}{ccccc}
 R & \xrightarrow{p} & R/\mathfrak{a} & \xrightarrow{\tau} & \frac{R/\mathfrak{a}}{J/\mathfrak{a}} \\
 \downarrow \pi & & \downarrow & \nearrow & \nearrow \\
 r & \mapsto & \bar{r} & \mapsto & \bar{\bar{r}} \\
 \downarrow & & \downarrow & & \downarrow \\
 \bar{r} & \mapsto & \bar{\bar{r}} & \mapsto & \bar{\bar{\bar{r}}} \\
 \downarrow & & \downarrow & & \downarrow \\
 R/J & & & & 
 \end{array}$$

$\exists ! \bar{\phi}$

It is straightforward to show that  $J = \text{Ker}(\tau \circ p)$ . Then the first isomorphism theorem says the map  $\bar{\phi}$  is a ring isomorphism.

**Notation.**  $\text{Spec}(R) = \{\text{primes ideals of } R\}$ , called the *prime spectrum of } R*.

The variety determined by an ideal  $\mathfrak{a} \leq R$  is  $V(\mathfrak{a}) = \{\mathfrak{p} \in \text{Spec}(R) \mid \mathfrak{p} \supseteq \mathfrak{a}\}$ .

$\text{m-Spec}(R) = \{\text{maximal ideals of } R\} \subseteq \text{Spec}(R)$ .

**Fact 1.16.** Let  $\phi : R \rightarrow S$  be a ring homomorphism. Then  $\text{Ker}(\phi) \leq R$ ,  $\text{Im}(\phi) \subseteq S$  is a subring and  $\text{Im}(\phi) \cong R/\text{Ker}(\phi)$ .

If  $S$  is an integral domain, then so is  $\text{Im}(\phi)$ . Hence  $\text{Ker}(\phi)$  is prime.

More generally,  $\phi^{-1}(\mathfrak{b}) = \{x \in R \mid \phi(x) \in \mathfrak{b}\} \leq R$  for  $\mathfrak{b} \leq S$ .

$$\begin{array}{ccccc}
 R & \xrightarrow{\phi} & S & \xrightarrow{\pi} & S/\mathfrak{q} \\
 \downarrow p & & \downarrow & \nearrow & \nearrow \\
 r & \mapsto & \phi(r) & \mapsto & \overline{\phi(r)} \\
 \downarrow & & \downarrow & & \downarrow \\
 \bar{r} & \mapsto & \bar{\phi(r)} & \mapsto & \bar{\bar{\phi(r)}} \\
 \downarrow & & \downarrow & & \downarrow \\
 \frac{R}{\phi^{-1}(\mathfrak{q})} & & & & 
 \end{array}$$

$\exists ! \overline{\pi \circ \phi}$

Let  $\mathfrak{q} \in \text{Spec}(S)$ . Then  $S/\mathfrak{q}$  is an integral domain. Also, since  $R/\text{Ker}(\pi \circ \phi) \cong \text{Im}(\pi \circ \phi) \subseteq S/\mathfrak{q}$ , we have  $R/\text{Ker}(\pi \circ \phi)$  is an integral domain and then  $\text{Ker}(\pi \circ \phi)$  is prime. Observe  $\phi^{-1}(\mathfrak{q}) = \text{Ker}(\pi \circ \phi)$  is then prime, i.e.,  $\phi^{-1}(\mathfrak{q}) \in \text{Spec}(R)$ . Thus,  $\phi$  induces a well-defined map  $\phi^* : \text{Spec}(S) \rightarrow \text{Spec}(R)$  given by  $\phi^*(\mathfrak{q}) = \phi^{-1}(\mathfrak{q})$ .

**Example.** Let  $\phi : \mathbb{Z} \rightarrow \mathbb{Q}$  be an inclusion map. Note  $\mathfrak{q} := (0)\mathbb{Q} \leq \mathbb{Q}$  is maximal, but  $\phi^{-1}(\mathfrak{q}) = \phi^{-1}(0) = \text{Ker}(\phi) = 0\mathbb{Z}$ , which is not maximal in  $\mathbb{Z}$ . So the map  $\phi^*$  does not take maximal ideals to maximal ideals in general.

**Fact 1.17.** We have the following.

(a) Let  $R \neq 0$ . Then  $R$  has a maximal ideal  $\mathfrak{m}$  and so  $R$  has a prime ideal. Moreover, for any  $\mathfrak{a} \leq R$ , there exists a maximal ideal  $\mathfrak{m} \supseteq \mathfrak{a}$ . In particular,  $V(\mathfrak{a}) = \{\mathfrak{p} \in \text{Spec}(R) \mid \mathfrak{p} \supseteq \mathfrak{a}\} \neq \emptyset$ .

One generally proves the second statement first, then derives the first statement as the special case  $\mathfrak{a} = 0$ . Next, we show how to derive the second statement from the first one.

(b) Let  $\mathfrak{a} \leq R$ . Then  $0 \neq R/\mathfrak{a}$  is a commutative ring with identity. So  $R/\mathfrak{a}$  has a maximal ideal and by Fact 1.15, it is of the form  $\mathfrak{m}/\mathfrak{a}$ , where  $\mathfrak{m}$  is a maximal ideal of  $R$  containing  $\mathfrak{a}$ .

## Local Rings

**Definition 1.18.**  $R$  is *local* if it has a unique maximal ideal  $\mathfrak{m}$ , also known as “*quasi-local*”. The *residue field* of  $R$  is  $R/\mathfrak{m}$ .

“Assume  $(R, \mathfrak{m}, k)$  is local” or “assume  $(R, \mathfrak{m})$  is local”, shorthand, we mean  $\mathfrak{m}$  is the unique maximal ideal of  $R$  and  $k = R/\mathfrak{m}$ .

**Example 1.19.** (a) Any field is local with the maximal ideal  $(0)$ .

(b) Let  $n \geq 1$  and  $p$  be prime in  $\mathbb{Z}$ . Note  $0 \neq \mathbb{Z}/\langle p^n \rangle$  has a maximal ideal  $\mathfrak{m} = \langle p \rangle / \langle p^n \rangle$ , where  $\langle p \rangle$  is a maximal ideal of  $\mathbb{Z}$  containing  $\langle p^n \rangle$ . Assume there is  $\mathfrak{m}_1 \leq R$  maximal such that  $\mathfrak{m}_1 \supseteq \langle p^n \rangle$ . Then  $\mathfrak{m}_1$  is prime, so  $p \in \mathfrak{m}_1$  and hence  $\langle p \rangle \subseteq \mathfrak{m}_1$ . Since  $\langle p \rangle$  is prime in  $\mathbb{Z}$  and  $\mathbb{Z}$  is a PID,  $\langle p \rangle$  is maximal. So  $\langle p \rangle = \mathfrak{m}_1$ . Thus,  $\langle p \rangle$  is the unique maximal ideal containing  $\langle p^n \rangle$  and so  $\mathbb{Z}/\langle p^n \rangle$  is local. Similarly, we can show  $\langle p \rangle$  is the unique prime ideal containing  $\langle p^n \rangle$ , so  $\text{Spec}(\mathbb{Z}/\langle p^n \rangle) = \{\langle p \rangle / \langle p^n \rangle\}$ .

(c) Let  $k$  be a field. As in part (b), we see that  $R = k[X]/\langle X^n \rangle$  is local with  $\mathfrak{m} = \langle X \rangle / \langle X^n \rangle$ . In fact,  $\text{Spec}(R) = \{\langle X \rangle / \langle X^n \rangle\}$ .

(d) Let  $k$  be a field and  $R = k[X_1, \dots, X_d] / \langle X_1^{a_1}, \dots, X_d^{a_d} \rangle$ , where  $a_i \geq 1$  for  $i = 1, \dots, d$ . Then  $R$  is local with  $\mathfrak{m} = \langle X_1, \dots, X_d \rangle / \langle X_1^{a_1}, \dots, X_d^{a_d} \rangle$ . In fact,  $\text{Spec}(R) = \{\langle X_1, \dots, X_d \rangle / \langle X_1^{a_1}, \dots, X_d^{a_d} \rangle\}$ .

**Fact 1.20.** If  $(R, \mathfrak{m})$  is local and  $\mathfrak{a} \leq R$ , then  $(R/\mathfrak{a}, \mathfrak{m}/\mathfrak{a})$  is also local and  $\frac{R/\mathfrak{a}}{\mathfrak{m}/\mathfrak{a}} \cong R/\mathfrak{m}$ , so these rings have canonically isomorphic residue fields. The converse fails in general by Example 1.19.

**Notation 1.21.** Let  $R^\times = R^* = \mathcal{U}(R) = \{\text{units of } R\}$ .

**Proposition 1.22.** The following are equivalent.

- (i)  $R$  is local.
- (ii)  $R \setminus R^\times \leq R$ .
- (iii) There exists  $\mathfrak{a} \leq R$  such that  $R \setminus \mathfrak{a} \subseteq R^\times$ .

When these are satisfied,  $\mathfrak{m} = R \setminus R^\times = \mathfrak{a}$ .

*Proof.* “(i) $\Rightarrow$ (ii)”. Assume  $(R, \mathfrak{m})$  is local.

Claim.  $\mathfrak{m} = R \setminus R^\times$ . It suffices to show  $R \setminus \mathfrak{m} = R^\times$ . “ $\supseteq$ ”. Let  $u \in R^\times$ . Then  $\langle u \rangle = R$  and so  $u \notin \mathfrak{m} \leq R$ , i.e.,  $u \in R \setminus \mathfrak{m}$ . Hence  $R^\times \subseteq R \setminus \mathfrak{m}$ . “ $\subseteq$ ”. Let  $x \in R \setminus R^\times$ . Then  $\langle x \rangle \leq R$ . Since  $\mathfrak{m}$  is the unique maximal ideal in  $R$ ,  $\langle x \rangle \subseteq \mathfrak{m}$ , i.e.,  $x \in \mathfrak{m}$ . Thus,  $R \setminus R^\times \subseteq \mathfrak{m}$ , i.e.,  $R \setminus \mathfrak{m} \subseteq R^\times$ .

“(ii) $\Rightarrow$ (iii)”. Assume  $R \setminus R^\times \leq R$ . Set  $\mathfrak{a} = R \setminus R^\times$ . Then  $R \setminus \mathfrak{a} = R^\times$ .

“(iii) $\Rightarrow$ (i)”. Let  $\mathfrak{a} \leq R$  such that  $R \setminus \mathfrak{a} \subseteq R^\times$ .

Claim.  $\mathfrak{a} = R \setminus R^\times$ . “ $\supseteq$ ”. It is straightforward. “ $\subseteq$ ”. Let  $a \in \mathfrak{a} \leq R$ , then  $a \notin R^\times$  since  $\mathfrak{a} \leq R$ , so  $a \in R \setminus R^\times$  and hence  $\mathfrak{a} \subseteq R \setminus R^\times$ . Thus,  $\mathfrak{a} = R \setminus R^\times$ .

Let  $\mathfrak{n} \leq R$  be maximal and  $y \in \mathfrak{n}$ . Then  $y \notin R^\times$ . So  $y \in R \setminus R^\times = \mathfrak{a}$ . Thus,  $\mathfrak{n} \subseteq \mathfrak{a} \leq R$ . Since  $\mathfrak{n}$  is maximal,  $\mathfrak{n} = \mathfrak{a}$ . Thus,  $\mathfrak{a}$  is the unique maximal ideal in  $R$  and so  $R$  is local.  $\square$

**Proposition 1.23.** Let  $\mathfrak{m} \leq R$  be maximal such that  $1 + \mathfrak{m} \subseteq R^\times$ . Then  $R$  is local.

*Proof.* By the previous proposition, it suffices to show  $R \setminus \mathfrak{m} \subseteq R^\times$ . Let  $x \in R \setminus \mathfrak{m}$ . Set  $\langle x, \mathfrak{m} \rangle = \langle \{x\} \cup \mathfrak{m} \rangle = \{ax + m \mid a \in R, m \in \mathfrak{m}\}$ . Since  $x \notin \mathfrak{m}$ ,  $\mathfrak{m} \subsetneq \langle x, \mathfrak{m} \rangle \leq R$ . Also, since  $\mathfrak{m}$  is maximal,  $\langle x, \mathfrak{m} \rangle = R$ . So  $ax + m = 1$  for some  $a \in R$  and  $m \in \mathfrak{m}$ , i.e.,  $ax = 1 - m \in 1 + \mathfrak{m} \subseteq R^\times$ . Thus,  $a, x \in R^\times$ .  $\square$

## The Nilradical

**Definition 1.24.**  $x \in R$  is *nilpotent* if there exists  $n \geq 1$  such that  $x^n = 0$ . The *nilradical* of  $R$  is

$$\text{Nil}(R) = \mathcal{N}(R) = \mathfrak{N}_R = \mathfrak{N} = \{\text{nilpotent elements of } R\}^\dagger.$$

**Example 1.25.** In the ring  $\mathbb{Z}/\langle p^n \rangle$ , we have  $\bar{p}$  is nilpotent. It is similar in  $k[X]/\langle X^n \rangle$  and  $k[X_1, \dots, X_n]/\langle X_1^{a_1}, \dots, X_d^{a_d} \rangle$ , where  $k$  is a field,  $n \geq 1$  and  $a_1 \cdots, a_d \geq 1$ .

**Proposition 1.26.** We have the following.

- (a)  $\text{Nil}(R) \leq R$ .
- (b)  $\text{Nil}(R/\text{Nil}(R)) = \{0\}$ .
- (c)  $\text{Nil}(R) = R$  if and only if  $R = 0$ .
- (d)  $\text{Nil}(R) = \bigcap_{\mathfrak{p} \in \text{Spec}(R)} \mathfrak{p}$ .

*Proof.* (a) Since  $0 \in \text{Nil}(R)$ ,  $\text{Nil}(R) \neq \emptyset$ . Let  $r \in R$  and  $a, b \in \text{Nil}(R)$ . Then there exists  $m, n \geq 1$  such that  $a^m = 0 = b^n$ . Then  $(ra)^m = r^m a^m = 0$  and so  $ra \in \text{Nil}(R)$ . By the binomial theorem,  $(a+b)^{m+n} = \sum_{i=0}^{m+n} \binom{m+n}{i} a^i b^{m+n-i} = 0$ . Since for  $i = 0, \dots, m+n$ , either  $i \geq m$  or  $i < m$ , i.e.,  $i \geq m$  or  $m+n-i \geq n$ , we have  $a^i = 0$  when  $i \geq m$ , and  $b^{m+n-i} = 0$  when  $m+n-i \geq n$ . So  $(a+b)^{m+n} = 0$  and thus  $a+b \in \text{Nil}(R)$ .

(b) Let  $\bar{x} \in \text{Nil}(R/\text{Nil}(R))$ . Then there exists  $n \geq 1$  such that  $\bar{x}^n = \bar{x}^n = 0$ , i.e.,  $x^n \in \text{Nil}(R)$ . So there exists  $m \geq 1$  such that  $(x^n)^m = 0$ , i.e.,  $x^{mn} = 0$ . Thus,  $x \in \text{Nil}(R)$ , i.e.,  $\bar{x} = 0$ .

(c) We have  $\text{Nil}(R) = R$  if and only if  $1 \in \text{Nil}(R)$  if and only if there exists  $n \geq 1$  such that  $1 = 1^n = 0$  if and only if  $1 = 0$  if and only if  $R = 0$ .

(d) “ $\subseteq$ ”. Let  $x \in \text{Nil}(R)$ . Then there exists  $n \geq 1$  such that  $x^n = 0 \in \mathfrak{p}$  for  $\mathfrak{p} \in \text{Spec}(R)$ . So  $x \in \mathfrak{p}$  for  $\mathfrak{p} \in \text{Spec}(R)$ . Thus,  $x \in \bigcap_{\mathfrak{p} \in \text{Spec}(R)} \mathfrak{p}$ .

“ $\supseteq$ ”. Let  $x \in R \setminus \text{Nil}(R)$ . Need to show  $x \notin \bigcap_{\mathfrak{p} \in \text{Spec}(R)} \mathfrak{p}$ . It is equivalent to show there exists  $\mathfrak{p} \in \text{Spec}(R)$  such that  $x \notin \mathfrak{p}$ . Let  $\Sigma = \{\mathfrak{a} \leq R \mid x, x^2, x^3, \dots \notin \mathfrak{a}\}$ . Since  $x \notin \text{Nil}(R)$ ,  $x^k \neq 0$  for  $k \geq 1$ . So  $(0) \in \Sigma$  and then  $\Sigma \neq \emptyset$ . Let  $\mathcal{C} \subseteq \Sigma$  be chain. Then we have  $\mathfrak{q} := \bigcup_{\mathfrak{a} \in \mathcal{C}} \mathfrak{a} \leq R$ . Suppose  $x^n \in \mathfrak{q}$  for some  $n \geq 1$ . Then  $x^n \in \mathfrak{a}$  for some  $\mathfrak{a} \in \mathcal{C} \subseteq \Sigma$ , contradicting  $\mathfrak{a} \in \Sigma$ . So  $x^n \notin \mathfrak{q}$  for  $n \geq 1$  and hence  $\mathfrak{q} \in \Sigma$ . Hence  $\mathfrak{q}$  is an upper bound for  $\mathcal{C}$  in  $\Sigma$ . Since the chain  $\mathcal{C} \subseteq \Sigma$  is arbitrary, by Zorn's lemma,  $\Sigma$  has a maximal element  $I$ . Claim.  $I \in \text{Spec}(R)$ . Suppose  $I = R$ . Then  $x \in R = I$ , contradicting  $I \in \Sigma$ . So  $I \subsetneq R$ . Let  $r, s \in R \setminus I$ . Then  $I \subsetneq \langle r, I \rangle \leq R$  and  $I \subsetneq \langle s, I \rangle \leq R$ . By the maximality of  $I$  in  $\Sigma$ , we have  $\langle r, I \rangle, \langle s, I \rangle \notin \Sigma$ . So there exists  $m, n \geq 1$  such that  $x^m \in \langle r, I \rangle$  and  $x^n \in \langle s, I \rangle$ . Then  $x^m = ar + i$  for some  $a \in R$  and  $i \in I$ , and  $x^n = bs + j$  for some  $b \in R$  and  $j \in I$ . So  $x^{m+n} = x^m x^n = (ar + i)(bs + j) = abrs + \underbrace{(arj + bsi + ij)}_{\in I} \in \langle rs, I \rangle$ . Hence  $\langle rs, I \rangle \notin \Sigma$ .

Therefore, since  $I \in \Sigma$ , we have  $I \neq \langle rs, I \rangle$ , so  $rs \notin I$ . Thus,  $I \in \text{Spec}(R)$  such that  $x \notin I$ .  $\square$

**Example.** Let  $k$  be a field and  $R = k[X_1, \dots, X_d]/\langle X_1^{a_1}, \dots, X_d^{a_d} \rangle \neq 0$ , where  $a_i \geq 1$  for  $i = 1, \dots, d$ . Then  $\text{Nil}(R) = \langle X_1, \dots, X_d \rangle / \langle X_1^{a_1}, \dots, X_d^{a_d} \rangle$ .

<sup>†</sup> $\text{Nil}(R) \subseteq \text{ZD}(R)$ , but not conversely.

*Proof.* Method 1. Since  $\text{Spec}(R) = \{\langle X_1, \dots, X_d \rangle / \langle X_1^{a_1}, \dots, X_d^{a_d} \rangle\}$ ,  $\text{Nil}(R) = \bigcap_{\mathfrak{p} \in \text{Spec}(R)} \mathfrak{p} = \langle X_1, \dots, X_d \rangle / \langle X_1^{a_1}, \dots, X_d^{a_d} \rangle$ .

Method 2. Since  $\overline{X_i} \in \text{Nil}(R) \leq R$  for  $i = 1, \dots, d$ , we have  $\overline{\langle X_1, \dots, X_d \rangle} = \langle \overline{X_1}, \dots, \overline{X_d} \rangle \subseteq \text{Nil}(R) \subsetneq R$  since  $R \neq 0$ . Also, since  $\overline{\langle X_1, \dots, X_d \rangle}$  is maximal, we have  $\text{Nil}(R) = \overline{\langle X_1, \dots, X_d \rangle}$ .  $\square$

**Fact.** If  $\mathfrak{a} \leq R$  and  $r_1, \dots, r_n \in R$ , then  $R/\mathfrak{a} \supseteq \langle \bar{r}_1, \dots, \bar{r}_n \rangle = \langle r_1, \dots, r_n, \mathfrak{a} \rangle / \mathfrak{a}$ . In particular, if  $\langle r_1, \dots, r_n \rangle \supseteq \mathfrak{a}$ , then  $\langle \bar{r}_1, \dots, \bar{r}_n \rangle = \langle r_1, \dots, r_n \rangle / \mathfrak{a}$ .

## The Jacobson Radical

**Definition 1.27.** The *Jacobson radical* of  $R$  is

$$\text{Jac}(R) = \mathfrak{J}(R) = \bigcap_{\mathfrak{m} \leq R \text{ max'l}} \mathfrak{m}.$$

**Fact 1.28.**

$$\text{Jac}(R) \supseteq \text{Nil}(R) = \bigcap_{\mathfrak{p} \in \text{Spec}(R)} \mathfrak{p}.$$

**Proposition 1.29.**

$$\mathfrak{J}(R) = \{x \in R \mid 1 - xy \in R^\times, \forall y \in R\}.$$

*Proof.* “ $\subseteq$ ”. Let  $x \in \mathfrak{J}(R)$ . By way of contradiction, suppose there is  $y \in R$  such that  $1 - xy \notin R^\times$ . Then there exists  $\mathfrak{m} \leq R$  maximal such that  $1 - xy \in \mathfrak{m}$ . Since  $x \in \mathfrak{J}(R) \subseteq \mathfrak{m}$ ,  $xy \in \mathfrak{m}$ . So  $1 = (1 - xy) + xy \in \mathfrak{m}$ , a contradiction.

“ $\supseteq$ ”. Argue by contrapositive. Let  $x \in R$  such that  $1 - xy \in R^\times$  for any  $y \in Y$ . Suppose  $x \notin \mathfrak{J}(R)$ . Then there exists  $\mathfrak{m} \leq R$  maximal such that  $x \notin \mathfrak{m}$ . So  $\mathfrak{m} \subsetneq \langle \mathfrak{m}, x \rangle \subseteq R$ . Hence  $\langle x, \mathfrak{m} \rangle = R$ . Then there exists  $y \in R$  and  $m \in \mathfrak{m}$  such that  $xy + m = 1$ , i.e.,  $1 - xy = m \in \mathfrak{m}$ . So  $1 - xy \notin R^\times$ , a contradiction.  $\square$

## Operations on Ideals

Let  $\mathfrak{a}, \mathfrak{b}, \mathfrak{c} \leq R$ ,  $\mathfrak{a}_1, \dots, \mathfrak{a}_n \leq R$ ,  $S_\lambda \subseteq R$  and  $\mathfrak{a}_\lambda, \mathfrak{b}_\lambda \leq R$  for  $\lambda \in \Lambda$ , where  $\Lambda$  is an index set.

### Sums of Ideals

**Definition 1.30.**

$$\mathfrak{a} + \mathfrak{b} = \langle \mathfrak{a} \cup \mathfrak{b} \rangle = \bigcap_{\mathfrak{a} \cup \mathfrak{b} \subseteq I \leq R} I.$$

**Fact 1.31.** We have the following.

- (a)  $\mathfrak{a} + \mathfrak{b} \subseteq \mathfrak{c}$  if and only if  $\mathfrak{a} \cup \mathfrak{b} \subseteq \mathfrak{c}$ .
- (b)  $\mathfrak{a} + \mathfrak{b}$  is the (unique) smallest ideal of  $R$  that contains  $\mathfrak{a} \cup \mathfrak{b}$ .
- (c)  $\mathfrak{a} + \mathfrak{b} = \{a + b \mid a \in \mathfrak{a}, b \in \mathfrak{b}\}$ .
- (d) If  $\mathfrak{a} = \langle S \rangle$  and  $\mathfrak{b} = \langle T \rangle$ , then  $\mathfrak{a} + \mathfrak{b} = \langle S \cup T \rangle$ .

(e) If  $\mathfrak{a} = \langle x_1, \dots, x_m \rangle$  and  $\mathfrak{b} = \langle y_1, \dots, y_n \rangle$ , then  $\mathfrak{a} + \mathfrak{b} = \langle x_1, \dots, x_m, y_1, \dots, y_n \rangle$ .

(f) If  $x \in R$ , then  $\langle x, \mathfrak{a} \rangle = \langle x \rangle + \mathfrak{a}$ .

(g)  $\mathfrak{a} + (\mathfrak{b} + \mathfrak{c}) = (\mathfrak{a} + \mathfrak{b}) + \mathfrak{c}$ .

*Proof.* (a) and (b) are by definition.

(c) Set  $I = \{a + b \mid a \in \mathfrak{a}, b \in \mathfrak{b}\}$ . Check  $I$  is an ideal of  $R$ . For  $a \in \mathfrak{a}$ ,  $a = a + 0 \in I$  and for  $b \in \mathfrak{b}$ ,  $b = 0 + b \in I$ . So  $\mathfrak{a} \cup \mathfrak{b} \subseteq I$ . By (a),  $\mathfrak{a} + \mathfrak{b} \subseteq I$ . On the other hand, for  $a + b \in I$  with  $a \in \mathfrak{a}$  and  $b \in \mathfrak{b}$ , we have  $a, b \in \mathfrak{a} \cup \mathfrak{b} \subseteq \mathfrak{a} + \mathfrak{b} \subseteq R$ , so  $a + b \in \mathfrak{a} + \mathfrak{b}$ .

(d) Let  $I \leq R$ . Note  $I \supseteq \mathfrak{a} \cup \mathfrak{b}$  if and only if  $I \supseteq \mathfrak{a}, \mathfrak{b}$  if and only if  $I \supseteq \langle S \rangle, \langle T \rangle$  if and only if  $I \supseteq S, T$  if and only if  $I \supseteq S \cup T$ . So  $\mathfrak{a} + \mathfrak{b} = \bigcap_{\mathfrak{a} \cup \mathfrak{b} \subseteq I \leq R} I = \bigcap_{S \cup T \subseteq I \leq R} I = \langle S \cup T \rangle$ .

(e) By (d).

(f) By (c).

(g) The essential point is  $\mathfrak{a} + (\mathfrak{b} + \mathfrak{c}) = \langle \mathfrak{a} \cup (\mathfrak{b} \cup \mathfrak{c}) \rangle = \langle (\mathfrak{a} \cup \mathfrak{b}) \cup \mathfrak{c} \rangle = (\mathfrak{a} + \mathfrak{b}) + \mathfrak{c}$ .  $\square$

**Example.**  $m\mathbb{Z} + n\mathbb{Z} = \langle m, n \rangle \mathbb{Z} = \gcd(m, n)\mathbb{Z}$ , where  $m \neq 0$  or  $n \neq 0$ .

**Recall.**  $\text{Spec}(R) = \{\text{prime ideals of } R\}$ . For  $S \subseteq R$ ,  $V(S) = \{\mathfrak{p} \in \text{Spec}(R) \mid \mathfrak{p} \supseteq S\}$ .

**Proposition 1.32.** Let  $S \subseteq R$ .

(a)  $V(S) = V(\langle S \rangle)$ .

(b)  $\mathfrak{a} = R$  if and only if  $V(\mathfrak{a}) = \emptyset$ .

(c)  $\mathfrak{a} \subseteq \text{Nil}(R)$  if and only if  $V(\mathfrak{a}) = \text{Spec}(R)$ .

(d) If  $\mathfrak{a} \subseteq \mathfrak{b}$ , then  $V(\mathfrak{a}) \supseteq V(\mathfrak{b})^\dagger$ . If  $S \subseteq T \subseteq R$ , then  $V(S) \supseteq V(T)$ .

*Proof.* (d) Since  $S \subseteq T \subseteq R$ , we have  $V(S) \supseteq V(T)$  by definition.

(a)  $\mathfrak{p} \in V(S)$  if and only if  $\mathfrak{p} \supseteq S$  if and only if  $\mathfrak{p} \supseteq \langle S \rangle$  if and only if  $\mathfrak{p} \in V(\langle S \rangle)$ .

(b) We have  $\mathfrak{a} = R$  if and only if  $\mathfrak{b} \not\supseteq \mathfrak{a}$  for any  $\mathfrak{b} \leq R$  if and only if  $\mathfrak{m} \not\supseteq \mathfrak{a}$  for any  $\mathfrak{m} \leq R$  maximal if and only if  $\mathfrak{p} \not\supseteq \mathfrak{a}$  for any  $\mathfrak{p} \in \text{Spec}(R)$  by Fact 1.14 and Fact 1.17.

(c)  $\mathfrak{a} \subseteq \text{Nil}(R)$  if and only if  $\mathfrak{p} \supseteq \mathfrak{a}$  for all  $\mathfrak{p} \in \text{Spec}(R)$  by Proposition 1.26(d) if and only if  $V(\mathfrak{a}) = \text{Spec}(R)$ .  $\square$

**Proposition 1.33.** We have the following.

(a)  $V(\mathfrak{a} + \mathfrak{b}) = V(\mathfrak{a} \cup \mathfrak{b}) = V(\mathfrak{a}) \cap V(\mathfrak{b})$ .

(b)  $V(\mathfrak{a}) \cap V(\mathfrak{b}) = \emptyset$  if and only if  $\mathfrak{a} + \mathfrak{b} = R$ .

*Proof.* (a) Since  $\mathfrak{a} + \mathfrak{b} = \langle \mathfrak{a} \cup \mathfrak{b} \rangle$ ,  $V(\mathfrak{a} + \mathfrak{b}) = V(\langle \mathfrak{a} \cup \mathfrak{b} \rangle) = V(\mathfrak{a} \cup \mathfrak{b})$ .

Let  $\mathfrak{p} \in \text{Spec}(R)$ . Note  $\mathfrak{p} \supseteq \mathfrak{a} \cup \mathfrak{b}$  if and only if  $\mathfrak{p} \supseteq \mathfrak{a}$  and  $\mathfrak{p} \supseteq \mathfrak{b}$ . So  $V(\mathfrak{a} \cup \mathfrak{b}) = V(\mathfrak{a}) \cap V(\mathfrak{b})$ .

---

$^\dagger V(\mathfrak{a}) \subseteq V(\mathfrak{b})$  if and only if  $\text{rad}(\mathfrak{a}) \supseteq \text{rad}(\mathfrak{b})$ ;  $V(\mathfrak{a}) = V(\mathfrak{b})$  if and only if  $\text{rad}(\mathfrak{a}) = \text{rad}(\mathfrak{b})$ .

(b)  $V(\mathfrak{a}) \cap V(\mathfrak{b}) = \emptyset$  if and only if  $V(\mathfrak{a} + \mathfrak{b}) = \emptyset$  by part (a) if and only if  $\mathfrak{a} + \mathfrak{b} = R$  by Proposition 1.32(b).  $\square$

**Remark.** The sum  $\mathfrak{a}_1 + \cdots + \mathfrak{a}_n$  is defined for  $\mathfrak{a}_1, \dots, \mathfrak{a}_n$  for all  $n \in \mathbb{Z}_{\geq 3}$  and same properties as above hold for finite sums.

**Definition 1.34.**

$$\sum_{\lambda} \mathfrak{a}_{\lambda} = \langle \bigcup_{\lambda \in \Lambda} \mathfrak{a}_{\lambda} \rangle = \bigcap_{\substack{\bigcup_{\lambda \in \Lambda} \mathfrak{a}_{\lambda} \subseteq I \leq R}} I.$$

**Fact 1.35.** We have the following.

- (a)  $\sum_{\lambda \in \Lambda} \mathfrak{a}_{\lambda} \subseteq \mathfrak{c}$  if and only if  $\bigcup_{\lambda \in \Lambda} \mathfrak{a}_{\lambda} \subseteq \mathfrak{c}$ .
- (b)  $\sum_{\lambda \in \Lambda} \mathfrak{a}_{\lambda}$  is the (unique) smallest ideal of  $R$  containing  $\bigcup_{\lambda \in \Lambda} \mathfrak{a}_{\lambda}$ .
- (c)  $\sum_{\lambda \in \Lambda} \mathfrak{a}_{\lambda} = \{\sum_{\lambda \in \Lambda}^{\text{finite}} a_{\lambda} \mid a_{\lambda} \in \mathfrak{a}_{\lambda}, \forall \lambda \in \Lambda\}$ .
- (d) If  $\mathfrak{a}_{\lambda} = \langle S_{\lambda} \rangle$  for  $\lambda \in \Lambda$ , then  $\sum_{\lambda \in \Lambda} \mathfrak{a}_{\lambda} = \langle \bigcup_{\lambda \in \Lambda} S_{\lambda} \rangle$ .

**Fact 1.36.** We have the following.

- (a)  $V(\sum_{\lambda \in \Lambda} \mathfrak{a}_{\lambda}) = V(\bigcup_{\lambda \in \Lambda} \mathfrak{a}_{\lambda}) = \bigcap_{\lambda \in \Lambda} V(\mathfrak{a}_{\lambda})$ .
- (b)  $\bigcap_{\lambda \in \Lambda} V(\mathfrak{a}_{\lambda}) = \emptyset$  if and only if  $\sum_{\lambda \in \Lambda} \mathfrak{a}_{\lambda} = R$ .

## Products of Ideals

**Definition 1.37.**

$$\mathfrak{a}\mathfrak{b} = \langle N \rangle = \bigcap_{N \subseteq I \leq R} I,$$

where  $N = \{ab \mid a \in \mathfrak{a}, b \in \mathfrak{b}\}$ .

**Fact 1.38.** Let  $N = \{ab \mid a \in \mathfrak{a}, b \in \mathfrak{b}\}$ .

- (a)  $\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{c}$  if and only if  $N \subseteq \mathfrak{c}$ .
- (b)  $\mathfrak{a}\mathfrak{b}$  is the (unique) smallest ideal of  $R$  containing  $N$ .
- (c)  $\mathfrak{a}\mathfrak{b} = \{\sum_i^{\text{finite}} a_i b_i \mid a_i \in \mathfrak{a}, b_i \in \mathfrak{b}, \forall i\}$ .
- (d) If  $\mathfrak{a} = \langle S \rangle$  and  $\mathfrak{b} = \langle T \rangle$ , then  $\mathfrak{a}\mathfrak{b} = \langle st \mid s \in S, t \in T \rangle$ .
- (e) If  $\mathfrak{a} = \langle x_1, \dots, x_m \rangle$  and  $\mathfrak{b} = \langle y_1, \dots, y_n \rangle$ , then  $\mathfrak{a}\mathfrak{b} = \langle x_i y_j \mid i = 1, \dots, m, j = 1, \dots, n \rangle$ .
- (f)  $\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{a} \cap \mathfrak{b}$ .

*Proof.* (c) Let  $I = \{\sum_i^{\text{finite}} a_i b_i \mid a_i \in \mathfrak{a}, b_i \in \mathfrak{b}\}$ . Check  $I \leq R$  through  $I \subseteq \mathfrak{a}\mathfrak{b} \subseteq I$  like Fact 1.31(c).

(f) Method 1. For any  $a \in \mathfrak{a} \leq R$ , we have  $ab \in \mathfrak{a}$  for any  $b \in \mathfrak{b}$ . For any  $b \in \mathfrak{b} \leq R$ , we have  $ab \in \mathfrak{b}$  for any  $a \in \mathfrak{a}$ . So  $ab \in \mathfrak{a} \cap \mathfrak{b}$  for any  $a \in \mathfrak{a}$  and  $b \in \mathfrak{b}$ . Hence  $\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{a} \cap \mathfrak{b}$  by Fact 1.12.

Method 2. It follows from  $\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{a}R = \mathfrak{a}$  and  $\mathfrak{a}\mathfrak{b} \subseteq R\mathfrak{b} = \mathfrak{b}$ .  $\square$

**Proposition 1.39.** We have the following.

(a)  $V(\mathfrak{a}\mathfrak{b}) = V(\mathfrak{a} \cap \mathfrak{b}) = V(\mathfrak{a}) \cup V(\mathfrak{b})$ .

(b)  $V(\mathfrak{a}) \cup V(\mathfrak{b}) = \text{Spec}(R)$  if and only if  $\mathfrak{a}\mathfrak{b} \subseteq \text{Nil}(R)$  if and only if  $\mathfrak{a} \cap \mathfrak{b} \subseteq \text{Nil}(R)$ .

*Proof.* (a) Let  $\mathfrak{p} \in \text{Spec}(R)$ . Claim.  $\mathfrak{p} \supseteq \mathfrak{a}\mathfrak{b}$  if and only if  $\mathfrak{p} \supseteq \mathfrak{a}$  or  $\mathfrak{p} \supseteq \mathfrak{b}^*$ . “ $\Leftarrow$ ”. Let  $\mathfrak{p} \supseteq \mathfrak{a}$  or  $\mathfrak{p} \supseteq \mathfrak{b}$ . Then  $\mathfrak{p} = \mathfrak{p}R \supseteq \mathfrak{a}R \supseteq \mathfrak{a}\mathfrak{b}$  or  $\mathfrak{p} = \mathfrak{p}R \supseteq R\mathfrak{b} \supseteq \mathfrak{a}\mathfrak{b}$ . “ $\Rightarrow$ ”. Let  $\mathfrak{p} \supseteq \mathfrak{a}\mathfrak{b}$ . Suppose  $\mathfrak{p} \not\supseteq \mathfrak{a}$  and  $\mathfrak{p} \not\supseteq \mathfrak{b}$ . Then there exists  $a \in \mathfrak{a} \setminus \mathfrak{p}$  and exists  $b \in \mathfrak{b} \setminus \mathfrak{p}$ . Since  $\mathfrak{p} \in \text{Spec}(R)$ ,  $ab \notin \mathfrak{p}$ , contradicting  $ab \in \mathfrak{a}\mathfrak{b} \subseteq \mathfrak{p}$ . Hence  $\mathfrak{p} \supseteq \mathfrak{a}\mathfrak{b}$  if and only if  $\mathfrak{p} \supseteq \mathfrak{a}$  or  $\mathfrak{p} \supseteq \mathfrak{b}$ . So  $V(\mathfrak{a}\mathfrak{b}) = V(\mathfrak{a}) \cup V(\mathfrak{b})$ .

Since  $\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{a} \cap \mathfrak{b}$ ,  $V(\mathfrak{a}\mathfrak{b}) \supseteq V(\mathfrak{a} \cap \mathfrak{b})$ . Let  $\mathfrak{p} \in V(\mathfrak{a}\mathfrak{b})$ . Then  $\mathfrak{p} \supseteq \mathfrak{a}\mathfrak{b}$ . So  $\mathfrak{p} \supseteq \mathfrak{a}$  or  $\mathfrak{p} \supseteq \mathfrak{b}$ . Hence  $\mathfrak{p} \supseteq \mathfrak{a} \cap \mathfrak{b}$  and then  $\mathfrak{p} \in V(\mathfrak{a} \cap \mathfrak{b})$ . So  $V(\mathfrak{a}\mathfrak{b}) \subseteq V(\mathfrak{a} \cap \mathfrak{b})$ . Thus,  $V(\mathfrak{a}\mathfrak{b}) = V(\mathfrak{a} \cap \mathfrak{b})^\dagger$ .

(b)  $V(\mathfrak{a}) \cup V(\mathfrak{b}) = \text{Spec}(R)$  if and only if  $V(\mathfrak{a}\mathfrak{b}) = \text{Spec}(R)$  by part (a) if and only if  $\mathfrak{a}\mathfrak{b} \subseteq \text{Nil}(R)$  by Proposition 1.32(c) and similarly for  $\mathfrak{a} \cap \mathfrak{b}$ .  $\square$

**Proposition 1.40.** We have the following.

(a)  $\mathfrak{a}\mathfrak{b} = \mathfrak{b}\mathfrak{a}$  and  $(\mathfrak{a}\mathfrak{b})\mathfrak{c} = \mathfrak{a}(\mathfrak{b}\mathfrak{c})$ .

(b)  $\mathfrak{a}(\mathfrak{b} + \mathfrak{c}) = \mathfrak{a}\mathfrak{b} + \mathfrak{a}\mathfrak{c}$ .

(c)  $\mathfrak{a} \cap \mathfrak{b} = \mathfrak{a}\mathfrak{b}$  if  $\mathfrak{a} + \mathfrak{b} = R$ , i.e.,  $\mathfrak{a}$  and  $\mathfrak{b}$  are “coprime” or “comaximal”.

The converse holds if  $R$  is a PID and  $\mathfrak{a}, \mathfrak{b} \neq 0$ .

*Proof.* (a) and (b) are straightforward.

(c) “ $\supseteq$ ”. We always have  $\mathfrak{a} \cap \mathfrak{b} \supseteq \mathfrak{a}\mathfrak{b}$ .

“ $\subseteq$ ”. Assume  $\mathfrak{a} + \mathfrak{b} = R$ .

Method 1. Note  $1 = a + b$  for some  $a \in \mathfrak{a}$  and  $b \in \mathfrak{b}$ . Let  $x \in \mathfrak{a} \cap \mathfrak{b}$ . Then  $x \in \mathfrak{b}$  and  $x \in \mathfrak{a}$ . So  $x = 1 \cdot x = (a + b)x = ax + bx = ax + xb \in \mathfrak{a}\mathfrak{b}$ . Hence  $\mathfrak{a} \cap \mathfrak{b} \subseteq \mathfrak{a}\mathfrak{b}$ .

Method 2. Note  $\mathfrak{a} \cap \mathfrak{b} = R(\mathfrak{a} \cap \mathfrak{b}) = (\mathfrak{a} + \mathfrak{b})(\mathfrak{a} \cap \mathfrak{b}) = \underbrace{\mathfrak{a}(\mathfrak{a} \cap \mathfrak{b})}_{\subseteq \mathfrak{b}} + \underbrace{\mathfrak{b}(\mathfrak{a} \cap \mathfrak{b})}_{\subseteq \mathfrak{a}} \subseteq \mathfrak{a}\mathfrak{b}$  by (a) and (b).

Conversely, assume  $R$  is a PID and  $\mathfrak{a}, \mathfrak{b} \neq 0$ . Then  $R$  is a UFD, so each reducible element has a unique factorization into multiple of irreducible elements, also, since  $R$  is a PID, every irreducible element is actually prime. Hence we can write  $\mathfrak{a} = p_1^{e_1} \cdots p_n^{e_n} R$  and  $\mathfrak{b} = p_1^{f_1} \cdots p_n^{f_n} R$  with  $e_i, f_i \geq 0$  for  $i = 1, \dots, n$ , and  $p_1, \dots, p_n \in R$  are non-associate prime elements. Assume  $\mathfrak{a} \cap \mathfrak{b} = \mathfrak{a}\mathfrak{b}$ . Since  $\mathfrak{a} = \langle p_1^{e_1} \cdots p_n^{e_n} \rangle$  and  $\mathfrak{b} = \langle p_1^{f_1} \cdots p_n^{f_n} \rangle$ ,  $\mathfrak{a} \cap \mathfrak{b} = \text{lcm}(p_1^{e_1} \cdots p_n^{e_n}, p_1^{f_1} \cdots p_n^{f_n})R = p_1^{\max\{e_1, f_1\}} \cdots p_n^{\max\{e_n, f_n\}} R$ . By Fact 1.38(e),  $\mathfrak{a}\mathfrak{b} = p_1^{e_1+f_1} \cdots p_n^{e_n+f_n}$ . So  $\max\{e_i, f_i\} = e_i + f_i$ , i.e.,  $e_i = 0$  or  $f_i = 0$  for  $i = 1, \dots, n$ . In other words, for  $\mathfrak{p} \in \text{Spec}(R)$ , either  $\mathfrak{a} \not\subseteq \mathfrak{p}$  or  $\mathfrak{b} \not\subseteq \mathfrak{p}^\dagger$ . So  $V(\mathfrak{a}) \cap V(\mathfrak{b}) = \emptyset$  for  $\mathfrak{p} \in \text{Spec}(R)$ . Thus,  $\mathfrak{a} + \mathfrak{b} = R$  by Proposition 1.33(b).  $\square$

**Remark.** The product  $\mathfrak{a}_1 \cdots \mathfrak{a}_n$  is defined for  $\mathfrak{a}_1, \dots, \mathfrak{a}_n$  for all  $n \in \mathbb{Z}_{\geq 3}$ .

\*In some texts, this is the definition of prime ideal.

$^\dagger$ Let  $\mathfrak{p} \in \text{Spec}(R)$ . Then by (f),  $\mathfrak{p} \supseteq \mathfrak{a} \cap \mathfrak{b} \supseteq \mathfrak{a}\mathfrak{b}$  if and only if  $\mathfrak{p} \supseteq \mathfrak{a}$  or  $\mathfrak{p} \supseteq \mathfrak{b}$ , to get  $V(\mathfrak{a} \cap \mathfrak{b}) = V(\mathfrak{a}) \cup V(\mathfrak{b})$ .

$^\ddagger$ Let  $p \in R$  be prime and  $a \in R$ . Then  $p \mid a$  if and only if  $\langle p \rangle \supseteq \langle a \rangle$ . Furthermore, if  $a$  has a prime factorization, then  $p \mid a$  if and only if  $p$  occurs in the prime factorization of  $a$ .

**Example 1.41.** Let  $R = k[X, Y]$ ,  $\mathfrak{a} = \langle X \rangle$  and  $\mathfrak{b} = \langle Y \rangle$ . Then  $\mathfrak{a} \cap \mathfrak{b} = \langle XY \rangle = \mathfrak{a}\mathfrak{b}$  by Fact 1.38(e). But  $\mathfrak{a} + \mathfrak{b} = \langle X, Y \rangle \subsetneq R$ . So the converse in Proposition 1.40(c) fails in general.

**Definition 1.42.** Let  $n \geq 1$ . Let  $\mathfrak{a}^n = \underbrace{\mathfrak{a} \cdots \mathfrak{a}}_{n \text{ times}}$  and  $\mathfrak{a}^0 = R$ .

**Warning 1.43.**  $\mathfrak{a}^n$  is **not** generated by  $\{a^n \mid a \in \mathfrak{a}\}$ . For example, if  $R = \mathbb{F}_2[X, Y]$  and  $\mathfrak{a} = \langle X, Y \rangle$ , then  $\mathfrak{a}^2 = \langle X^2, XY, Y^2 \rangle \neq \langle f^2 \mid f \in \mathfrak{a} \rangle \not\supseteq XY$ .

**Fact 1.44.** Let  $n \geq 1$  and  $N = \{a_1 \cdots a_n \mid a_i \in \mathfrak{a}, \forall i = 1, \dots, n\}$ .

- (a)  $\mathfrak{a}^n = \langle N \rangle$  and for any  $\mathfrak{b} \leq R$ , we have  $\mathfrak{a}^n \subseteq \mathfrak{b}$  if and only if  $N \subseteq \mathfrak{b}$ .
- (b)  $\mathfrak{a}^n$  is the (unique) smallest ideal of  $R$  containing  $N$ .
- (c)  $\mathfrak{a}^n = \{\sum_i^{\text{finite}} a_{i1} \cdots a_{in} \mid a_{ij} \in \mathfrak{a}, \forall i, \forall j = 1, \dots, n\}$ .
- (d) If  $\mathfrak{a} = \langle S \rangle$ , then  $\mathfrak{a}^n = \langle s_1 \cdots s_n \mid s_i \in S, \forall i = 1, \dots, n \rangle$ .
- (e) If  $\mathfrak{a} = \langle x_1, \dots, x_m \rangle$ , then  $\mathfrak{a}^n = \langle x_{i_1} \cdots x_{i_n} \mid i_j \in \{1, \dots, m\}, \forall j = 1, \dots, n \rangle$ .

**Fact 1.45.**  $V(\mathfrak{a}^n) = V(\mathfrak{a})$ .

*Proof.* By Proposition 1.39,  $V(\mathfrak{a}^n) = \bigcup_{i=1}^n V(\mathfrak{a}) = V(\mathfrak{a})$ . □

**Proposition 1.46** (Chinese Remainder Theorem). We have the following.

- (a) The function  $\phi : R \rightarrow (R/\mathfrak{a}_1) \times \cdots \times (R/\mathfrak{a}_n)$  given by  $\phi(x) = (\bar{x}, \dots, \bar{x}) = (x + \mathfrak{a}_1, \dots, x + \mathfrak{a}_n)$  is a well-defined ring homomorphism.
- (b) If  $\mathfrak{a}_i + \mathfrak{a}_j = R$  for  $1 \leq i, j \leq n$  with  $i \neq j$ , i.e.,  $\{\mathfrak{a}_1, \dots, \mathfrak{a}_n\}$  are pairwise coprime, then  $\bigcap_{i=1}^n \mathfrak{a}_i = \mathfrak{a}_1 \cdots \mathfrak{a}_n$  and  $\mathfrak{a}_i + (\bigcap_{j=1, j \neq i}^n \mathfrak{a}_j)R = R$  for  $i = 1, \dots, n$ .
- (c)  $\phi$  is surjective if and only if  $\mathfrak{a}_i + \mathfrak{a}_j = R$  for  $1 \leq i, j \leq n$  with  $i \neq j$ .
- (d)  $\text{Ker}(\phi) = \bigcap_{i=1}^n \mathfrak{a}_i$ .
- (e) If  $\mathfrak{a}_i + \mathfrak{a}_j = R$  for  $1 \leq i, j \leq n$  with  $i \neq j$  and  $\bigcap_{i=1}^n \mathfrak{a}_i = 0$ , then  $R \cong (R/\mathfrak{a}_1) \times \cdots \times (R/\mathfrak{a}_n)$ .

*Proof.* (b) Let  $i \in \{1, \dots, n\}$ . To show  $\mathfrak{a}_i + (\bigcap_{j \neq i} \mathfrak{a}_j)R = R$ , it suffices to show  $V(\mathfrak{a}_i) \cap \left( \bigcup_{j \neq i} V(\mathfrak{a}_j) \right) = V(\mathfrak{a}_i) \cap V\left( \bigcap_{j \neq i} \mathfrak{a}_j \right) = V(\mathfrak{a}_i + \bigcap_{j \neq i} \mathfrak{a}_j) = \emptyset$ . Suppose  $V(\mathfrak{a}_i) \cap \left( \bigcup_{j \neq i} V(\mathfrak{a}_j) \right) \neq \emptyset$ . Then there exists  $\mathfrak{p} \in V(\mathfrak{a}_i) \cap V(\mathfrak{a}_j) = V(\mathfrak{a}_i + \mathfrak{a}_j) = V(R) = \emptyset$  for some  $j \neq i$ , a contradiction.

Now for  $\bigcap_{i=1}^n \mathfrak{a}_i = \mathfrak{a}_1 \cdots \mathfrak{a}_n$ , prove by induction on  $n$ . Base case  $n = 1$ : trivial. Base case  $n = 2$ : by Proposition 1.40(c). Induction step: assume  $n \in \mathbb{Z}_{\geq 3}$  and  $\bigcap_{i=1}^{n-1} \mathfrak{a}_i = \mathfrak{a}_1 \cdots \mathfrak{a}_{n-1}$ . Then  $\mathfrak{a}_n + \mathfrak{a}_1 \cdots \mathfrak{a}_{n-1} = \mathfrak{a}_n + \bigcap_{j=1}^{n-1} \mathfrak{a}_j = R$ . So by Proposition 1.40(c), we have  $\bigcap_{i=1}^n \mathfrak{a}_i = (\bigcap_{i=1}^{n-1} \mathfrak{a}_i) \cap \mathfrak{a}_n = (\mathfrak{a}_1 \cdots \mathfrak{a}_{n-1}) \cap \mathfrak{a}_n = (\mathfrak{a}_1 \cdots \mathfrak{a}_{n-1})\mathfrak{a}_n = \mathfrak{a}_1 \cdots \mathfrak{a}_n$ .

- (c) “ $\Rightarrow$ ”. Assume  $\phi$  is surjective. In particular, there exists  $x \in R$  such that  $(\bar{1}, \bar{0}, \dots, \bar{0}) = \phi(x) = (\bar{x}, \bar{x}, \dots, \bar{x})$ . So  $x + \mathfrak{a}_1 = 1 + \mathfrak{a}_1$  and  $x + \mathfrak{a}_i = 0 + \mathfrak{a}_i$  for  $i = 2, \dots, n$ . Hence  $1 - x \in \mathfrak{a}_1$  and  $x \in \mathfrak{a}_i$  for



$i = 2, \dots, n$ . Also, since  $\underset{\in \mathfrak{a}_i}{(x)} + \underset{\in \mathfrak{a}_1}{(1-x)} = 1$ , we have  $\mathfrak{a}_i + \mathfrak{a}_1 = R$  for  $i = 2, \dots, n$ . Similarly, consider

$$(\bar{0}, \dots, \bar{0}, \underset{\uparrow j\text{th}}{\bar{1}}, \bar{0}, \dots, \bar{0}) \rightsquigarrow \mathfrak{a}_i + \mathfrak{a}_j = R \text{ for } 1 \leq i, j \leq n \text{ with } i \neq j.$$

“ $\Leftarrow$ ”. Assume  $\mathfrak{a}_i + \mathfrak{a}_j = R$  for  $1 \leq i, j \leq n$  with  $i \neq j$ . By (b),  $\mathfrak{a}_1 + (\bigcap_{j=2}^n \mathfrak{a}_j)R = R$ . So  $a_1 + y = 1$  with  $a_1 \in \mathfrak{a}_1$  and  $y \in \bigcap_{j=2}^n \mathfrak{a}_j$ , i.e.,  $1 - y = a_1 \in \mathfrak{a}_1$  and  $y \in \mathfrak{a}_j$  for  $j = 2, \dots, n$ . Then  $\phi(y) = (\bar{y}, \bar{y}, \dots, \bar{y}) = (y + \mathfrak{a}_1, y + \mathfrak{a}_2, \dots, y + \mathfrak{a}_n) = (1 + \mathfrak{a}_1, 0 + \mathfrak{a}_2, \dots, 0 + \mathfrak{a}_n) = (\bar{1}, \bar{0}, \dots, \bar{0})$ . Similarly, for  $j = 1, \dots, n$ , there exists  $y_j$  such that  $\phi(y_j) = (\bar{0}, \dots, \bar{0}, \underset{\uparrow j\text{th}}{\bar{1}}, \bar{0}, \dots, \bar{0})$ . Then for

any  $(\bar{r}_1, \dots, \bar{r}_n) \in \frac{R}{\mathfrak{a}_1} \times \dots \times \frac{R}{\mathfrak{a}_n}$ ,  $(\bar{r}_1, \dots, \bar{r}_n) = \sum_{j=1}^n r_j (\bar{0}, \dots, \bar{0}, \underset{\uparrow j\text{th}}{\bar{1}}, \bar{0}, \dots, \bar{0}) = \sum_{j=1}^n r_j \phi(y_j) = \phi(\sum_{j=1}^n r_j y_j)$ . So  $\phi$  is surjective.  $\square$

**Proposition 1.47.** Let  $\mathfrak{a}_1, \dots, \mathfrak{a}_n \leq R$  and  $\mathfrak{p} \in \text{Spec}(R)$ .

- (a) If  $\mathfrak{p} = \mathfrak{a}_1 \cdots \mathfrak{a}_n$ , then  $\mathfrak{p} = \mathfrak{a}_i$  for some  $i \in \{1, \dots, n\}$ .
- (b) If  $\mathfrak{p} \supseteq \mathfrak{a}_1 \cap \dots \cap \mathfrak{a}_n$ , then  $\mathfrak{p} \supseteq \mathfrak{a}_i$  for some  $i \in \{1, \dots, n\}$ .
- (c) If  $\mathfrak{p} = \mathfrak{a}_1 \cap \dots \cap \mathfrak{a}_n$ , then  $\mathfrak{p} = \mathfrak{a}_i$  for some  $i \in \{1, \dots, n\}$ .

*Proof.* (b) Assume  $\mathfrak{p} \supseteq \mathfrak{a}_1 \cap \dots \cap \mathfrak{a}_n \supseteq \mathfrak{a}_1 \cdots \mathfrak{a}_n$  by Fact 1.38(f). Since  $\mathfrak{p} \in \text{Spec}(R)$ , there exists some  $i \in \{1, \dots, n\}$  such that  $\mathfrak{p} \supseteq \mathfrak{a}_i$ .

(c) By (b), there exists  $i \in \{1, \dots, n\}$  such that  $\mathfrak{a}_i \subseteq \mathfrak{p} = \mathfrak{a}_1 \cap \dots \cap \mathfrak{a}_n \subseteq \mathfrak{a}_i$ . So  $\mathfrak{p} = \mathfrak{a}_i$ .

(a) Since  $\mathfrak{p} \supseteq \mathfrak{a}_1 \cdots \mathfrak{a}_n$ , we have  $\mathfrak{p} \supseteq \mathfrak{a}_i$  for some  $i \in \{1, \dots, n\}$ . Also, we have  $\mathfrak{p} = \mathfrak{a}_1 \cdots \mathfrak{a}_n \subseteq \mathfrak{a}_i$ .  $\square$

**Example.** The converses fail in general. Let  $R = k[X, Y]$ ,  $\mathfrak{p} = \mathfrak{a}_1 = \langle X \rangle$  and  $\mathfrak{a}_2 = \langle Y \rangle$ . Then  $\mathfrak{a}_1 \cap \mathfrak{a}_2 = \langle XY \rangle \neq \langle X \rangle = \mathfrak{p} = \langle X \rangle \neq \langle XY \rangle = \mathfrak{a}_1 \mathfrak{a}_2$ .

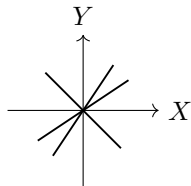
## Prime Avoidence

**Lemma 1.48.** Let  $k$  be an infinite field,  $0 \neq V$  a vector space over  $k$ , and  $V_1, \dots, V_n \subsetneq V$ . Then  $\bigcup_{i=1}^n V_i \subsetneq V$ .

*Proof.* Induction on  $n$ . Base case  $n = 1$ : trivial.

Induction step: assume  $n \geq 2$  and  $\bigcup_{i \neq j} V_i \subsetneq V$  for  $j = 1, \dots, n$ . Then there exists  $0 \neq v_j \in V \setminus \{\bigcup_{i \neq j} V_i\}$  for  $j = 1, \dots, n$ . By way of contradiction, suppose  $\bigcup_{i=1}^n V_i = V$ . Then  $v_j \in \{\bigcup_{i=1}^n V_i\} \setminus \{\bigcup_{i \neq j} V_i\} \subseteq V_j$  for  $j = 1, \dots, n$ . Let  $1 \leq i, j \leq n$  with  $i \neq j$ . Since  $v_j \neq 0$ , we have  $v_i + \lambda v_j \neq v_i + \mu v_j$  for any  $\lambda \neq \mu$  in  $k$ . Since  $k$  is infinite, there exists  $l$  such that  $V_l$  contains two distinct elements  $v_i + \lambda v_j$  and  $v_i + \mu v_j$  with  $0 \neq \lambda, \mu \in k$ . Then  $(\lambda - \mu)v_j = (v_i + \lambda v_j) - (v_i + \mu v_j) \in V_l$ . Since  $\lambda \neq \mu$ , we have  $v_j \in V_l$ . Since  $v_j \notin V_k$  for any  $k \neq j$  and  $v_j \in V_j$ , we have  $l = j$ . Also, since  $(\lambda^{-1} - \mu^{-1})v_i = \lambda^{-1}(v_i + \lambda v_j) - \mu^{-1}(v_i + \mu v_j) \in V_l$ , we have  $v_i \in V_l$  and then similarly, we have  $l = i$ . Hence  $i = l = j$ , a contradiction.  $\square$

**Example 1.49.** If  $k = \mathbb{R}$  and  $V = \mathbb{R}^2$ , then the lemma says that  $\mathbb{R}^2$  is not a finite union of lines through the origin, which is straightforward to show.



If  $|k| < \infty$ , then the lemma fails. For example,  $V = k^2 = \bigcup_{v \in k^2} \{v\} = \bigcup_{0 \neq v \in k^2} \text{span}\{v\}$  but  $0 \neq \text{span}(v) \not\subseteq k^2 = V$  for  $0 \neq v \in k^2$ .

The same technique shows that can't replace  $V_1, \dots, V_n$  with  $V_1, V_2, \dots$  over  $\mathbb{Q}$ .

**Theorem 1.50** (Prime avoidance, general version). *Let  $\mathfrak{b}_1, \dots, \mathfrak{b}_n, \mathfrak{a} \leq R$ . Assume*

(a)  *$R$  contains an infinite field  $k$  as a subring, or*

(b)  *$\mathfrak{b}_3, \dots, \mathfrak{b}_n \in \text{Spec}(R)$ .*

*Then if  $\mathfrak{a} \not\subseteq \mathfrak{b}_i$  for all  $i = 1, \dots, n$ , then  $\mathfrak{a} \not\subseteq \bigcup_{i=1}^n \mathfrak{b}_i$ .*

*Proof.* (a) For each  $i = 1, \dots, n$ , since  $\mathfrak{a} \not\subseteq \mathfrak{b}_i$ ,  $\mathfrak{a} \cap \mathfrak{b}_i \subsetneq \mathfrak{a}$ . Also, since  $\mathfrak{a}$  is a  $k$ -vector space, by Lemma 1.48,  $\mathfrak{a} \cap \bigcup_{i=1}^n \mathfrak{b}_i = \bigcup_{i=1}^n (\mathfrak{a} \cap \mathfrak{b}_i) \subsetneq \mathfrak{a}$ . So  $\mathfrak{a} \not\subseteq \bigcup_{i=1}^n \mathfrak{b}_i$ .

(b) Induct on  $n$ . Base case  $n = 1$ : done. Base case  $n = 2$ . Let  $a_i \in \mathfrak{a} \setminus \mathfrak{b}_i$  for  $i = 1, 2$ . Then  $a_1 + a_2 \in \mathfrak{a}$ . Suppose  $\mathfrak{a} \subseteq \mathfrak{b}_1 \cup \mathfrak{b}_2$ . Then  $a_1 + a_2 \in \mathfrak{b}_1 \cup \mathfrak{b}_2$ , say  $a_1 + a_2 \in \mathfrak{b}_2$ . Since  $a_1 \in \mathfrak{a} \subseteq \mathfrak{b}_1 \cup \mathfrak{b}_2$  and  $a_1 \notin \mathfrak{b}_1$ ,  $a_1 \in \mathfrak{b}_2$ . So  $a_2 = (a_1 + a_2) - a_1 \in \mathfrak{b}_2$ , a contradiction.

Induction step  $n \geq 3$ . Let  $\mathfrak{a} \not\subseteq \mathfrak{b}_i$  for  $i = 1, \dots, n$ . Assume  $\mathfrak{a} \not\subseteq \bigcup_{i \neq j} \mathfrak{b}_i$  for  $j = 1, \dots, n$ . Then there exists  $a_j \in \mathfrak{a} \setminus \{\bigcup_{i \neq j} \mathfrak{b}_i\}$  for  $j = 1, \dots, n$ . By way of contradiction, suppose  $\mathfrak{a} \subseteq \bigcup_{i=1}^n \mathfrak{b}_i$ . Then  $a_j \in \bigcup_{i=1}^n \mathfrak{b}_i \setminus \{\bigcup_{i \neq j} \mathfrak{b}_i\} \subseteq \mathfrak{b}_j$  for  $j = 1, \dots, n$ . Note  $a_1 \cdots a_{n-1} + a_n \in \mathfrak{a} \subseteq \bigcup_{i=1}^n \mathfrak{b}_i$ . So there exists  $l \in \{1, \dots, n\}$  such that  $a_1 \cdots a_{n-1} + a_n \in \mathfrak{b}_l$ . Suppose  $l = n$ . Since  $a_n \in \mathfrak{b}_n$ ,  $a_1 \cdots a_{n-1} \in \mathfrak{b}_n$ . Since  $n \geq 3$ , we have  $\mathfrak{b}_n \in \text{Spec}(R)$  and then  $a_i \in \mathfrak{b}_n$  for some  $1 < i < n$ , a contradiction. Hence we must have  $l < n$ . But since  $a_1 \cdots a_l \cdots a_{n-1} \in \mathfrak{b}_l$ , we have  $a_n \in \mathfrak{b}_l$ , a contradiction.  $\square$

**Theorem 1.51** (Prime avoidance). *Let  $\mathfrak{p}_1, \dots, \mathfrak{p}_n \in \text{Spec}(R)$ . If  $\mathfrak{a} \subseteq \bigcup_{i=1}^n \mathfrak{p}_i$ , then  $\mathfrak{a} \subseteq \mathfrak{p}_i$  for some  $i \in \{1, \dots, n\}$ , i.e., if  $\mathfrak{a} \not\subseteq \mathfrak{p}_i$  for  $i = 1, \dots, r$ , then  $\mathfrak{a} \not\subseteq \bigcup_{i=1}^n \mathfrak{p}_i$ .*

**Fact** (Avoidance for monomial ideals). Let  $A$  be a nonzero commutative ring with identity and  $\mathfrak{a}, \mathfrak{b}_1, \dots, \mathfrak{b}_n$  be monomial ideals of  $A[X_1, \dots, X_d]$ . If  $\mathfrak{a} \subseteq \bigcup_{i=1}^n \mathfrak{b}_i$ ,  $\mathfrak{a} \subseteq \mathfrak{b}_i$  for some  $i \in \{1, \dots, n\}$ .

*Proof.* By Dickson's lemma,  $\mathfrak{a} = \langle f_1, \dots, f_m \rangle$  for some monomials  $f_1, \dots, f_m \in A[X_1, \dots, X_d]$ . Then  $f_1 + \cdots + f_m \in \mathfrak{a} \subseteq \bigcup_{i=1}^n \mathfrak{b}_i$ . So  $f_1 + \cdots + f_m \in \mathfrak{b}_i$  for some  $i \in \{1, \dots, n\}$ . But  $\mathfrak{b}_i$  is a monomial ideal, so  $f_1, \dots, f_m \in \mathfrak{b}_i$ . Thus,  $\mathfrak{a} = \langle f_1, \dots, f_m \rangle \subseteq \mathfrak{b}_i$ .  $\square$

## Colon Ideals

**Definition 1.52.** Let  $S \subseteq R$ .

(a) Define the *colon ideal* by

$$(\mathfrak{a} : S) := \{r \in R \mid rs \in \mathfrak{a}, \forall s \in S\} \leq R.^\dagger$$

---

<sup>†</sup>For instance,  $(m\mathbb{Z} : n\mathbb{Z}) = (\frac{m}{(m,n)})\mathbb{Z}$  for  $m, n \geq 1$ .

(b) Define the *annihilator* of  $S$  by

$$\text{Ann}_R(S) := (0 : S) = \{r \in R \mid rs = 0, \forall s \in S\} \leq R.$$

In this notation, the set of *all zero divisors* of  $R$  is

$$\text{ZD}(R) = \bigcup_{x \neq 0} \text{Ann}_R(x).$$

**Example 1.53.** Let  $R = k[X, Y]$ .

$$(a) \ (\langle XY \rangle : \{X, Y\}) = (\langle XY \rangle : \langle X, Y \rangle) = (\langle XY \rangle : \langle X \rangle) \cap (\langle XY \rangle : \langle Y \rangle) = \langle Y \rangle \cap \langle X \rangle = \langle XY \rangle.$$

(b)

$$\begin{aligned} (\langle X^2, XY \rangle : \{X, Y\}) &= (\langle X^2, XY \rangle : \langle X, Y \rangle) = ((\langle X^2 \rangle : \langle X \rangle) + (\langle X^2 \rangle : \langle Y \rangle)) \\ &\quad \cap ((\langle XY \rangle : \langle X \rangle) + (\langle XY \rangle : \langle Y \rangle)) = (\langle X \rangle + \langle X^2 \rangle) \cap (\langle Y \rangle + \langle X \rangle) \\ &= \langle X \rangle \cap \langle X, Y \rangle = \langle X, XY \rangle = \langle X \rangle. \end{aligned}$$

**Fact 1.54.** Let  $S, T \subseteq R$ .

$$(a) \ \mathfrak{a} \subseteq (\mathfrak{a} : S) \leq R.$$

$$(b) \ (\mathfrak{a} : \mathfrak{b})\mathfrak{b} \subseteq \mathfrak{a}.$$

$$(c) \text{ If } S \subseteq T, \text{ then } (\mathfrak{a} : S) \supseteq (\mathfrak{a} : T).$$

$$(d) \text{ If } \mathfrak{a} \subseteq \mathfrak{b}, \text{ then } (\mathfrak{a} : S) \subseteq (\mathfrak{b} : S).$$

$$(e) \ (\mathfrak{a} : S) = (\mathfrak{a} : \langle S \rangle).$$

$$(f) \ \mathfrak{b} \subseteq \mathfrak{a} \text{ if and only if } (\mathfrak{a} : \mathfrak{b}) = R.$$

$$(g) \ (\mathfrak{a} : \bigcup_{\lambda \in \Lambda} S_\lambda) = \bigcap_{\lambda \in \Lambda} (\mathfrak{a} : S_\lambda).$$

$$(h) \ (\mathfrak{a} : \sum_{\lambda \in \Lambda} \mathfrak{b}_\lambda) = (\mathfrak{a} : \bigcup_{\lambda \in \Lambda} \mathfrak{b}_\lambda) = \bigcap_{\lambda \in \Lambda} (\mathfrak{a} : \mathfrak{b}_\lambda).$$

$$(i) \ (\bigcap_{\lambda} \mathfrak{a}_\lambda : S) = \bigcap_{\lambda \in \Lambda} (\mathfrak{a}_\lambda : S).$$

$$(j) \ ((\mathfrak{a} : \mathfrak{b}) : \mathfrak{c}) = (\mathfrak{a} : \mathfrak{b}\mathfrak{c}) = ((\mathfrak{a} : \mathfrak{c}) : \mathfrak{b}).$$

*Proof.* (b) For each  $r \in (\mathfrak{a} : \mathfrak{b})$  and each  $b \in \mathfrak{b}$ , we have  $br \in \mathfrak{a}$ . It then follows from Fact 1.12.

(e) “ $\supseteq$ ”. Since  $S \subseteq \langle S \rangle$ , by (c),  $(\mathfrak{a} : S) \supseteq (\mathfrak{a} : \langle S \rangle)$ . “ $\subseteq$ ”. Let  $r \in (\mathfrak{a} : S)$ . Then  $rs \in \mathfrak{a}$  for  $s \in S$ . Let  $s \in \langle S \rangle$ . Then  $s = \sum_i^{\text{finite}} a_i s_i$  for some  $a_i \in R$  and  $s_i \in S$  for each  $i$ . So  $rs = r(\sum_i^{\text{finite}} a_i s_i) = \sum_i^{\text{finite}} a_i(rs_i) \in \mathfrak{a}$ . Hence  $r \in (\mathfrak{a} : \langle S \rangle)$ .

(h) This follows from (e) and (g).

(j) It is enough to prove the first equality since  $\mathfrak{b}\mathfrak{c} = \mathfrak{c}\mathfrak{b}$ . Note  $r \in ((\mathfrak{a} : \mathfrak{b}) : \mathfrak{c})$  if and only if  $rc \in (\mathfrak{a} : \mathfrak{b})$  for  $c \in \mathfrak{c}$  if and only if  $r(bc) = (rc)b \in \mathfrak{a}$  for any  $b \in \mathfrak{b}$  and  $c \in \mathfrak{c}$  if and only if  $r \in (\mathfrak{a} : \mathfrak{b}\mathfrak{c})$  by (e).  $\square$

**Example 1.55.** Let  $R = k[X, Y]$ . It is straightforward to show the following.

- (a)  $(\langle XY \rangle : \langle X, Y \rangle) = (\langle XY \rangle : \{X, Y\}) = (\langle XY \rangle : X) \cap (\langle XY \rangle : Y) = \langle Y \rangle \cap \langle X \rangle = \langle XY \rangle$ .
- (b)  $(\langle X^2, XY \rangle : \langle X, Y \rangle) = (\langle X^2, XY \rangle : \{X, Y\}) = (\langle X^2, XY \rangle : X) \cap (\langle X^2, XY \rangle : Y) = \langle X, Y \rangle \cap \langle X \rangle = \langle X \rangle$ .

## Radicals of Ideals

**Definition 1.56.** The *radical* of  $\mathfrak{a} \leq R$  is

$$\text{rad}(\mathfrak{a}) = \text{r}(\mathfrak{a}) = \sqrt{\mathfrak{a}} = \{x \in R \mid x^n \in \mathfrak{a}, \forall n \gg 0\} = \{x \in R \mid x^n \in \mathfrak{a} \text{ for some } n \geq 1\}.$$

**Remark.**  $\text{rad}(0) = \text{Nil}(R)$ .

**Example 1.57.** In  $R = k[X, Y]$ , we have

$$\begin{aligned} \text{rad}(\langle X^2Y, XY^2 \rangle) &= \text{m-rad}(\langle X^2Y, XY^2 \rangle) = \text{m-rad}(\langle X^2Y \rangle + \langle XY^2 \rangle) \\ &= \text{m-rad}(\langle X^2Y \rangle) + \text{m-rad}(\langle XY^2 \rangle) = \langle XY \rangle + \langle XY \rangle = \langle XY \rangle. \end{aligned}$$

**Fact 1.58.** Let  $\pi : R \rightarrow R/\mathfrak{a}$  be the natural projection.

- (a)  $\text{rad}(\mathfrak{a}) = \pi^{-1}(\text{Nil}(R/\mathfrak{a})) \leq R$ .
- (b) If  $\mathfrak{a} \subseteq \mathfrak{b}$ , then  $\text{rad}(\mathfrak{a}) \subseteq \text{rad}(\mathfrak{b})$ .
- (c)  $\mathfrak{a} \subseteq \text{rad}(\mathfrak{a}) = \text{rad}(\text{rad}(\mathfrak{a}))$ .
- (d)  $\text{rad}(\mathfrak{a}\mathfrak{b}) = \text{rad}(\mathfrak{a} \cap \mathfrak{b}) = \text{rad}(\mathfrak{a}) \cap \text{rad}(\mathfrak{b})$ .
- (e)  $\text{rad}(\mathfrak{a}) = R$  if and only if  $\mathfrak{a} = R$ .
- (f)  $\text{rad}(\mathfrak{a} + \mathfrak{b}) = \text{rad}(\text{rad}(\mathfrak{a}) + \text{rad}(\mathfrak{b}))$ .
- (g)  $\text{rad}(\mathfrak{a}) = \bigcap_{\mathfrak{p} \in V(\mathfrak{a})} \mathfrak{p}$ .
- (h)  $\text{rad}(\bigcap_{i=1}^n \mathfrak{p}_i^{e_i}) = \bigcap_{i=1}^n \mathfrak{p}_i$ , where  $\mathfrak{p}_i \in \text{Spec}(R)$  and  $e_i \geq 1$  for  $i = 1, \dots, n$ .
- (i)  $\mathfrak{a} + \mathfrak{b} = R$  if and only if  $\text{rad}(\mathfrak{a}) + \text{rad}(\mathfrak{b}) = R$ .

*Proof.* (a) Let  $r \in R$ . Then  $r \in \pi^{-1}(\text{Nil}(R/\mathfrak{a}))$  if and only if  $\pi(r) \in \text{Nil}(R/\mathfrak{a})$  if and only if  $\bar{r}^n = 0$  in  $R/\mathfrak{a}$  for some  $n \geq 1$  if and only if  $r^n \in \mathfrak{a}$  for some  $n \geq 1$  if and only if  $r \in \text{rad}(\mathfrak{a})$ .

(b) It is straightforward.

(c) Since  $a^1 = a \in \mathfrak{a}$  for any  $a \in \mathfrak{a}$ , we have  $a \in \text{rad}(\mathfrak{a})$  for  $a \in \mathfrak{a}$ . So  $\mathfrak{a} \subseteq \text{rad}(\mathfrak{a})$ . Then by (b),  $\text{rad}(\mathfrak{a}) \subseteq \text{rad}(\text{rad}(\mathfrak{a}))$ . Let  $r \in \text{rad}(\text{rad}(\mathfrak{a}))$ . Then there exists  $n \geq 1$  such that  $r^n \in \text{rad}(\mathfrak{a})$ . So there exists  $m \geq 1$  such that  $r^{mn} = (r^n)^m \in \mathfrak{a}$ . Hence  $r \in \text{rad}(\mathfrak{a})$ .

(d) Since  $\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{a} \cap \mathfrak{b} \subseteq \mathfrak{a}, \mathfrak{b}$ , by (b), we have  $\text{rad}(\mathfrak{a}\mathfrak{b}) \subseteq \text{rad}(\mathfrak{a} \cap \mathfrak{b}) \subseteq \text{rad}(\mathfrak{a}), \text{rad}(\mathfrak{b})$  and then  $\text{rad}(\mathfrak{a}\mathfrak{b}) \subseteq \text{rad}(\mathfrak{a} \cap \mathfrak{b}) \subseteq \text{rad}(\mathfrak{a}) \cap \text{rad}(\mathfrak{b})$ . On the other hand, let  $x \in \text{rad}(\mathfrak{a}) \cap \text{rad}(\mathfrak{b})$ . Then there exist  $m, n \geq 1$  such that  $x^m \in \mathfrak{a}$  and  $x^n \in \mathfrak{b}$ . So  $x^{m+n} = x^m \cdot x^n \in \mathfrak{a}\mathfrak{b}$ . Hence  $x \in \text{rad}(\mathfrak{a}\mathfrak{b})$ .

(e)  $\mathfrak{a} = R$  if and only if  $1 \in \mathfrak{a}$  if and only if  $1^n \in \mathfrak{a}$  if and only if  $\text{rad}(\mathfrak{a}) = R$ .

(f) Since  $\mathfrak{a} + \mathfrak{b} \subseteq \text{rad}(\mathfrak{a}) + \text{rad}(\mathfrak{b})$ , we have  $\text{rad}(\mathfrak{a} + \mathfrak{b}) \subseteq \text{rad}(\text{rad}(\mathfrak{a}) + \text{rad}(\mathfrak{b}))$ . Let  $x \in \text{rad}(\text{rad}(\mathfrak{a}) + \text{rad}(\mathfrak{b}))$ . Then there exists  $n \geq 1$  such that  $x^n \in \text{rad}(\mathfrak{a}) + \text{rad}(\mathfrak{b})$ . So there exist  $a \in \text{rad}(\mathfrak{a})$  and  $b \in \text{rad}(\mathfrak{b})$  such that  $x^n = a + b$ . Then there exist  $j, k \geq 1$  such that  $a^j \in \mathfrak{a}$  and  $b^k \in \mathfrak{b}$ . So  $x^{n(j+k)} = (x^n)^{j+k} = (a+b)^{j+k} = \sum_{l=0}^{j+k} \binom{j+k}{l} a^l b^{j+k-l}$ . Since for  $0 \leq l \leq j+k$ , either  $l \geq j$  or  $l < j$ , i.e.,  $l \geq j$  or  $j+k-l > k$ , we have  $a^l \in \mathfrak{a}$  when  $l \geq j$ , and  $b^{j+k-l} \in \mathfrak{b}$  when  $j+k-l > k$ . So  $x^{n(j+k)} = 0$ . Thus,  $x \in \text{rad}(\mathfrak{a} + \mathfrak{b})$ .

(g) By Fact 1.15,  $\text{Spec}(R/\mathfrak{a}) = \{\mathfrak{p}/\mathfrak{a} \mid \mathfrak{p} \in V(\mathfrak{a})\}$ . So  $\text{Nil}(R/\mathfrak{a}) = \bigcap_{\mathfrak{p} \in \text{Spec}(R/\mathfrak{a})} \mathfrak{p} = \bigcap_{\mathfrak{p} \in V(\mathfrak{a})} \mathfrak{p}/\mathfrak{a}$ . Then by (a),  $\text{rad}(\mathfrak{a}) = \pi^{-1}(\text{Nil}(R/\mathfrak{a})) = \pi^{-1}(\bigcap_{\mathfrak{p} \in V(\mathfrak{a})} \mathfrak{p}/\mathfrak{a}) = \bigcap_{\mathfrak{p} \in V(\mathfrak{a})} \pi^{-1}(\mathfrak{p}/\mathfrak{a}) = \bigcap_{\mathfrak{p} \in V(\mathfrak{a})} \mathfrak{p}$ .

(h) Since  $\mathfrak{p}_i \in \text{Spec}(R)$ ,  $\mathfrak{p}_i \in V(\mathfrak{p}_i)$  and then  $\mathfrak{p}_i \subseteq \text{rad}(\mathfrak{p}_i) = \bigcap_{\mathfrak{p} \in V(\mathfrak{p}_i)} \mathfrak{p} \subseteq \mathfrak{p}_i$ , i.e.,  $\mathfrak{p}_i = \text{rad}(\mathfrak{p}_i)$  for  $i = 1, \dots, n$ . Then by (d),  $\text{rad}(\bigcap_{i=1}^n \mathfrak{p}_i^{e_i}) = \bigcap_{i=1}^n \text{rad}(\mathfrak{p}_i^{e_i}) = \bigcap_{i=1}^n \text{rad}(\mathfrak{p}_i) = \bigcap_{i=1}^n \mathfrak{p}_i$ .

(i) By (e) and (f),  $\mathfrak{a} + \mathfrak{b} = R$  if and only if  $\text{rad}(\mathfrak{a} + \mathfrak{b}) = R$  if and only if  $\text{rad}(\text{rad}(\mathfrak{a}) + \text{rad}(\mathfrak{b})) = R$  if and only if  $\text{rad}(\mathfrak{a}) + \text{rad}(\mathfrak{b}) = R$ .  $\square$

**Example 1.59.** (b) Example of  $\mathfrak{a} \not\subseteq \mathfrak{b}$  when  $\text{rad}(\mathfrak{a}) \subseteq \text{rad}(\mathfrak{b})$ . Let  $R = \mathbb{Z}$ . Then  $\text{rad}(\langle 2 \rangle) = \langle 2 \rangle = \text{rad}(\langle 4 \rangle)$ , but  $\langle 2 \rangle \not\subseteq \langle 4 \rangle$ .

(c) Example of  $\mathfrak{a} \subsetneq \text{rad}(\mathfrak{a})$ . Let  $R = \mathbb{Z}$ . Then  $\langle 4 \rangle \subsetneq \langle 2 \rangle = \text{rad}(\langle 4 \rangle)$ .

(d) Example of  $\text{rad}(\bigcap_{i=1}^{\infty} \mathfrak{a}_i) \subsetneq \bigcap_{i=1}^{\infty} \text{rad}(\mathfrak{a}_i)$ . Let  $R = k[X_1, X_2, \dots]$ ,  $\mathfrak{a}_1 = \langle X_1 \rangle$ ,  $\mathfrak{a}_2 = \langle X_1^2, X_2^2 \rangle$ ,  $\dots$ ,  $\mathfrak{a}_i = \langle X_1^i, \dots, X_i^i \rangle$ ,  $\dots$ . Since  $\langle X_1, \dots, X_i \rangle \in \text{Spec}(R)$  for  $i \geq 1$ , by (f) and (g), we have  $\text{rad}(\mathfrak{a}_i) = \text{rad}(\langle X_1^i, \dots, X_i^i \rangle) = \text{rad}(\langle X_1, \dots, X_i \rangle) = \langle X_1, \dots, X_i \rangle$  for  $i \geq 1$ . So  $\bigcap_{i=1}^{\infty} \text{rad}(\mathfrak{a}_i) = \bigcap_{i=1}^{\infty} \langle X_1, \dots, X_i \rangle = \langle X_1 \rangle \supsetneq 0 = \text{rad}(0) = \text{rad}(\bigcap_{i=1}^{\infty} \mathfrak{a}_i)$ .

(f) Example of  $\text{rad}(\mathfrak{a} + \mathfrak{b}) \supsetneq \text{rad}(\mathfrak{a}) + \text{rad}(\mathfrak{b})$ . Let  $R = k[X, Y]$ ,  $\mathfrak{a} = \langle X + Y^2 \rangle$  and  $\mathfrak{b} = \langle X \rangle$ . Then  $\mathfrak{a}, \mathfrak{b} \in \text{Spec}(R)$ . Also, since  $\langle X, Y \rangle \in \text{Spec}(R)$ ,  $\text{rad}(\mathfrak{a}) + \text{rad}(\mathfrak{b}) = \mathfrak{a} + \mathfrak{b} = \langle X + Y^2, X \rangle = \langle X, Y^2 \rangle \subsetneq \langle X, Y \rangle = \text{rad}(\langle X, Y^2 \rangle) = \text{rad}(\mathfrak{a} + \mathfrak{b})$ .

**Example 1.60.** (a) Let  $R = \mathbb{F}_2[X, Y]$ ,  $\mathfrak{a} = \langle X, Y \rangle$ ,  $\mathfrak{b}_1 = \langle X, XY, Y^2 \rangle = \langle X, X^2, XY, Y^2 \rangle$ ,  $\mathfrak{b}_2 = \langle X + Y, X^2, XY, Y^2 \rangle$  and  $\mathfrak{b}_3 = \langle Y, X^2, XY \rangle = \langle Y, X^2, XY, Y^2 \rangle$ . Then  $\mathfrak{a} \not\subseteq \mathfrak{b}_i$  for  $i = 1, 2, 3$ . Let  $f \in \mathfrak{a}$ . Then  $f$  can be written as

$$\begin{aligned} f &= Xg(X) + X^2\alpha(X, Y) + XY\gamma(X, Y) + Y^2\beta(X, Y) + Yh(Y) \\ &= X^2 \cdot \frac{g(X) - g(0)}{X} + (Xg(0) + Yh(0)) + Y^2 \cdot \frac{h(Y) - h(0)}{Y} \\ &\quad + X^2\alpha(X, Y) + XY\gamma(X, Y) + Y^2\beta(X, Y). \end{aligned}$$

for some  $g \in \mathbb{F}_2[X]$ ,  $h \in \mathbb{F}_2[Y]$  and  $\alpha, \beta, \gamma \in \mathbb{F}_2[X, Y]$ . Since  $g(0), h(0) \in \{0, 1\}$ ,  $f \in \mathfrak{b}_1 \cup \mathfrak{b}_2 \cup \mathfrak{b}_3$ . Also, since  $\mathfrak{b}_1 \cup \mathfrak{b}_2 \cup \mathfrak{b}_3 \subseteq \mathfrak{a}$ , we have  $\mathfrak{a} = \mathfrak{b}_1 \cup \mathfrak{b}_2 \cup \mathfrak{b}_3$ .

(b) Let  $R = \frac{\mathbb{F}_2[X, Y]}{\langle X^2, XY, Y^2 \rangle}$  and  $x = \overline{X}, y = \overline{Y} \in R$ . Then  $R \cong \mathbb{F}_2 \oplus \mathbb{F}_2x \oplus \mathbb{F}_2y$  and  $\mathfrak{a} := \langle x, y \rangle \cong \mathbb{F}_2x \oplus \mathbb{F}_2y$  as  $\mathbb{F}_2$ -vector space. Let  $\mathfrak{b}_1 = \langle x \rangle$ ,  $\mathfrak{b}_2 = \langle x + y \rangle$  and  $\mathfrak{b}_3 = \langle y \rangle$ . Then  $\mathfrak{a} \not\subseteq \mathfrak{b}_i$  for  $i = 1, 2, 3$ , but  $\mathfrak{a} = \mathfrak{b}_1 \cup \mathfrak{b}_2 \cup \mathfrak{b}_3$ .

## Extensions and Contractions

Let  $f : R \rightarrow S$  be a ring homomorphism,  $\mathfrak{a}, \mathfrak{a}_1, \mathfrak{a}_2 \leq R$  and  $\mathfrak{b}, \mathfrak{b}_1, \mathfrak{b}_2 \leq S$ .

**Definition 1.61.** The *extension* of  $\mathfrak{a}$  along  $f$  is

$$\mathfrak{a}^e = \mathfrak{a}S = \langle f(\mathfrak{a}) \rangle S = f(\mathfrak{a})S = \left\{ \sum_i^{\text{finite}} f(a_i)s_i \mid a_i \in \mathfrak{a}, s_i \in S, \forall i \right\} \leq S.$$

The *contraction* of  $\mathfrak{b}$  along  $f$  is

$$\mathfrak{b}^c = f^{-1}(\mathfrak{b}) \leq R.$$

**Example 1.62.** (a) Let  $R$  be an integral domain with the field of fraction  $Q(R)$ . Then  $R \subseteq Q(R)$  with the inclusion map  $\epsilon : R \rightarrow Q(R)$  given by  $\epsilon(r) = r/1$ . Note  $0Q(R) = 0$  and  $\mathfrak{a}Q(R) = Q(R)$  for  $0 \neq \mathfrak{a} \leq R$ .

(b) Note  $\langle X \rangle k[X] \subseteq k[X] \subseteq k[X, Y]$ ,  $(\langle X \rangle k[X]) k[X, Y] = \langle X \rangle k[X, Y]$ .

(c) Let  $R \subseteq S$  be rings and  $\epsilon : R \xrightarrow{\subseteq} S$ . If  $\mathfrak{b} \leq S$ , then  $\epsilon^{-1}(\mathfrak{b}) = \mathfrak{b} \cap R$ .

(d) Let  $\epsilon : k[X] \xrightarrow{\subseteq} k[X, Y]$ . Since  $\langle X, Y \rangle k[X, Y] \leq k[X, Y]$ , we have  $\epsilon^{-1}(\langle X, Y \rangle k[X, Y]) = \langle X, Y \rangle k[X, Y] \cap k[X] = \langle X \rangle k[X]$ .

**Proposition 1.63.** We have the following.

(a)  $\mathfrak{a} \subseteq f^{-1}(\mathfrak{a}S)$  and  $f^{-1}(\mathfrak{b})S \subseteq \mathfrak{b}$ . If  $\mathfrak{a}_1 \subseteq \mathfrak{a}_2$ , then  $\mathfrak{a}_1S \subseteq \mathfrak{a}_2S$ . If  $\mathfrak{b}_1 \subseteq \mathfrak{b}_2$ , then  $f^{-1}(\mathfrak{b}_1) \subseteq f^{-1}(\mathfrak{b}_2)$ . If  $T \subseteq R$ , then  $\langle T \rangle R S = \langle f(T) \rangle S$ .

Example of  $\mathfrak{a} \subsetneq f^{-1}(\mathfrak{a}S)$ . Let  $f : R = \mathbb{Z} \xrightarrow{\subseteq} S = \mathbb{Q}$  and  $\mathfrak{a} = \langle 2 \rangle R$ . Then  $f^{-1}(\mathfrak{a}S) = f^{-1}(S) = R \supsetneq \langle 2 \rangle R = \mathfrak{a}$ .

Example of  $f^{-1}(\mathfrak{b})S \subsetneq \mathfrak{b}$ . Let  $f : R = k[X] \xrightarrow{\subseteq} S = k[X, Y]$ . Let  $\mathfrak{b} = \langle Y \rangle S$ . Then  $f^{-1}(\mathfrak{b}) = 0$  and so  $f^{-1}(\mathfrak{b})S = 0 \subsetneq \langle Y \rangle S = \mathfrak{b}$ .

(b)  $\mathfrak{a}S = f^{-1}(\mathfrak{a}S)S$  and  $f^{-1}(\mathfrak{b}) = f^{-1}(f^{-1}(\mathfrak{b})S)$ , i.e.,  $\mathfrak{a}^e = \mathfrak{a}^{eee}$  and  $\mathfrak{b}^c = \mathfrak{b}^{cec}$ .<sup>†</sup>

(c)  $(\mathfrak{a}_1 + \mathfrak{a}_2)S = \mathfrak{a}_1S + \mathfrak{a}_2S$  and  $f^{-1}(\mathfrak{b}_1 + \mathfrak{b}_2) \supseteq f^{-1}(\mathfrak{b}_1) + f^{-1}(\mathfrak{b}_2)$ .

Example of  $f^{-1}(\mathfrak{b}_1 + \mathfrak{b}_2) \supsetneq f^{-1}(\mathfrak{b}_1) + f^{-1}(\mathfrak{b}_2)$ . Let  $f : R = k \xrightarrow{\subseteq} S = k[X]$ ,  $\mathfrak{b}_1 = \langle X \rangle S$  and  $\mathfrak{b}_2 = \langle X + 1 \rangle S$ . Then  $f^{-1}(\mathfrak{b}_1) = 0 = f^{-1}(\mathfrak{b}_2)$ . So  $f^{-1}(\mathfrak{b}_1 + \mathfrak{b}_2) = f^{-1}(S) = R \supsetneq 0 = f^{-1}(\mathfrak{b}_1) + f^{-1}(\mathfrak{b}_2)$ .

(d)  $(\mathfrak{a}_1 \cap \mathfrak{a}_2)S \subseteq \mathfrak{a}_1S \cap \mathfrak{a}_2S$  and  $f^{-1}(\mathfrak{b}_1 \cap \mathfrak{b}_2) = f^{-1}(\mathfrak{b}_1) \cap f^{-1}(\mathfrak{b}_2)$ .

Example of  $(\mathfrak{a}_1 \cap \mathfrak{a}_2)S \subsetneq \mathfrak{a}_1S \cap \mathfrak{a}_2S$ . Let  $f : R = k[X, Y] \rightarrow S = k[X, Y]/\langle X, Y \rangle^2$ ,  $\mathfrak{a}_1 = \langle X \rangle R$  and  $\mathfrak{a}_2 = \langle X + Y^2 \rangle R$ . Then  $\mathfrak{a}_1 \cap \mathfrak{a}_2 = \langle X(X + Y^2) \rangle R = \langle X^2 + XY^2 \rangle R$ ,  $\mathfrak{a}_1S = \langle \bar{X} \rangle S$  and  $\mathfrak{a}_2S = \langle \bar{X} + \bar{Y}^2 \rangle S = \langle \bar{X} \rangle S$ . So  $(\mathfrak{a}_1 \cap \mathfrak{a}_2)S = \langle \bar{X}^2 + \bar{X}\bar{Y}^2 \rangle S = 0 \subsetneq \langle \bar{X} \rangle S = \mathfrak{a}_1S \cap \mathfrak{a}_2S$ .

(e)  $(\mathfrak{a}_1\mathfrak{a}_2)S = (\mathfrak{a}_1S)(\mathfrak{a}_2S)$  and  $f^{-1}(\mathfrak{b}_1\mathfrak{b}_2) \supseteq f^{-1}(\mathfrak{b}_1)f^{-1}(\mathfrak{b}_2)$ .

Example of  $f^{-1}(\mathfrak{b}_1) \cap f^{-1}(\mathfrak{b}_2) = f^{-1}(\mathfrak{b}_1 \cap \mathfrak{b}_2) \supseteq f^{-1}(\mathfrak{b}_1\mathfrak{b}_2) \supsetneq f^{-1}(\mathfrak{b}_1)f^{-1}(\mathfrak{b}_2)$ . Let  $f : R = k[X] \rightarrow S = k[X]/(X(X - 1)) = k[X]/(X^2 - X) \cong k[X]/\langle X \rangle \times k[X]/\langle X - 1 \rangle \cong k \times k$  by [Chinese Remainder Theorem](#). Note in  $k \times k$ ,  $(1, 0) = (1, 0)^2$ . Let  $\mathfrak{b}_1 = \langle \bar{X} \rangle S = \mathfrak{b}_2$ . Then  $\mathfrak{b}_1\mathfrak{b}_2 = \langle \bar{X}^2 \rangle S = \langle \bar{X} \rangle S = \mathfrak{b}_1$ . So  $f^{-1}(\mathfrak{b}_1\mathfrak{b}_2) = f^{-1}(\mathfrak{b}_1) = f^{-1}(\langle \bar{X} \rangle S) = \langle X \rangle R \supsetneq \langle X^2 \rangle R = f^{-1}(\mathfrak{b}_1)f^{-1}(\mathfrak{b}_2)$ .

<sup>†</sup>We have a bijection  $\{\mathfrak{a} \leq R \mid \mathfrak{a}^{ee} = \mathfrak{a}\} \rightleftharpoons \{\mathfrak{b} \leq S \mid \mathfrak{b}^{ce} = \mathfrak{b}\}$  given by  $\mathfrak{a} \mapsto \mathfrak{a}^e$  and  $\mathfrak{b}^c \mapsto \mathfrak{b}$ .

(f)  $(\mathfrak{a}_1 : \mathfrak{a}_2)S \subseteq (\mathfrak{a}_1S : \mathfrak{a}_2S)$  and  $f^{-1}(\mathfrak{b}_1 : \mathfrak{b}_2) \subseteq (f^{-1}(\mathfrak{b}_1) : f^{-1}(\mathfrak{b}_2))$ .

Example of  $(\mathfrak{a}_1 : \mathfrak{a}_2)S \subsetneq (\mathfrak{a}_1S : \mathfrak{a}_2S)$ . Let  $f : R = k[X] \rightarrow S = k[X]/\langle X \rangle \cong k$ ,  $\mathfrak{a}_1 = \langle X^2 \rangle R$  and  $\mathfrak{a}_2 = \langle X \rangle R$ . Then  $\mathfrak{a}_1S = 0 = \mathfrak{a}_2S$  and so  $(\mathfrak{a}_1S : \mathfrak{a}_2S) = (0 : 0) = S \supsetneq 0 = \langle X \rangle S = (\langle X^2 \rangle : \langle X \rangle)S = (\mathfrak{a}_1 : \mathfrak{a}_2)S$ .

Example of  $f^{-1}(\mathfrak{b}_1 : \mathfrak{b}_2) \subsetneq (f^{-1}(\mathfrak{b}_1) : f^{-1}(\mathfrak{b}_2))$ . Let  $f : R = k \xrightarrow{\cong} S = k[X]$ ,  $\mathfrak{b}_1 = \langle X \rangle S$  and  $\mathfrak{b}_2 = \langle X - 1 \rangle S$ . Then  $(\mathfrak{b}_1 : \mathfrak{b}_2) = (\langle X \rangle : \langle X - 1 \rangle) = \langle X \rangle$  and  $f^{-1}(\mathfrak{b}_1) = 0 = f^{-1}(\mathfrak{b}_2)$ . So  $f^{-1}(\mathfrak{b}_1 : \mathfrak{b}_2) = f^{-1}(\langle X \rangle) = 0 \subsetneq R = (0 : 0) = (f^{-1}(\mathfrak{b}_1) : f^{-1}(\mathfrak{b}_2))$ .

(g)  $\text{rad}(\mathfrak{a})S \subseteq \text{rad}(\mathfrak{a}S)$  and  $f^{-1}(\text{rad}(\mathfrak{b})) = \text{rad}(f^{-1}(\mathfrak{b}))$ .

Example of  $\text{rad}(\mathfrak{a})S \subsetneq \text{rad}(\mathfrak{a}S)$ . Let  $f : R = k[X] \rightarrow S = k[X]/\langle X^2 \rangle$  and  $\mathfrak{a} = 0R$ . Then  $\text{rad}(\mathfrak{a})S = \text{rad}(0R)S = 0S = 0 \subsetneq \langle \bar{X} \rangle S = \text{rad}(0S) = \text{rad}(\mathfrak{a}S)$ .

*Proof.* (a) Note  $\mathfrak{a} \subseteq f^{-1}(f(\mathfrak{a})) \subseteq f^{-1}(f(\mathfrak{a})S) = f^{-1}(\mathfrak{a}S)$ .

To show  $\langle f(f^{-1}(\mathfrak{b})) \rangle S = f^{-1}(\mathfrak{b})S \subseteq \mathfrak{b}$ , it suffices to show  $\langle f(f^{-1}(\mathfrak{b})) \rangle \subseteq \mathfrak{b}$ , then it is equivalent to show  $f(f^{-1}(\mathfrak{b})) \subseteq \mathfrak{b}$ , which is true.

A set of generators of  $(\langle T \rangle R)S$  over  $S$  is

$$\left\{ f \left( \sum_i^{\text{finite}} t_i r_i \right) = \sum_i^{\text{finite}} f(t_i) f(r_i) \mid t_i \in T, r_i \in S, \forall i \right\} \subseteq \langle f(T) \rangle S.$$

A set of generators of  $\langle f(T) \rangle S$  over  $S$  is  $\{f(t) \mid t \in T\} = \{f(t \cdot 1) \mid t \in T\}$  which is a subset of the generators of  $(\langle T \rangle R)S$ .

(b) “ $\subseteq$ ”. By (a),  $\mathfrak{a} \subseteq f^{-1}(\mathfrak{a}S)$ , so  $\mathfrak{a}S \subseteq f^{-1}(\mathfrak{a}S)S$ . “ $\supseteq$ ”. A set of generators of  $f^{-1}(\mathfrak{a}S)S$  over  $S$  is  $\{f(x) \mid x \in f^{-1}(\mathfrak{a}S)\} = f(f^{-1}(\mathfrak{a}S)) \subseteq \mathfrak{a}S$ .

“ $\subseteq$ ”. By (a),  $\mathfrak{b} \supseteq f^{-1}(\mathfrak{b})S$ , so  $f^{-1}(\mathfrak{b}) \supseteq f^{-1}(f^{-1}(\mathfrak{b})S)$ . “ $\supseteq$ ”. Let  $x \in f^{-1}(\mathfrak{b})$ . Then  $f(x) = f(x) \cdot 1 \in \langle f(f^{-1}(\mathfrak{b})) \rangle S = f^{-1}(\mathfrak{b})S$ . So  $x \in f^{-1}(f^{-1}(\mathfrak{b})S)$ .

(c) “ $\supseteq$ ”. Since  $\mathfrak{a}_1 + \mathfrak{a}_2 \supseteq \mathfrak{a}_1, \mathfrak{a}_2$ , we have  $(\mathfrak{a}_1 + \mathfrak{a}_2)S \supseteq \mathfrak{a}_1S, \mathfrak{a}_2S$ . So  $(\mathfrak{a}_1 + \mathfrak{a}_2)S \supseteq \mathfrak{a}_1S + \mathfrak{a}_2S$ . “ $\subseteq$ ”. A set of generators of  $(\mathfrak{a}_1 + \mathfrak{a}_2)S$  over  $S$  is  $\{f(a_1 + a_2) = f(a_1) + f(a_2) \mid a_1 \in \mathfrak{a}_1, a_2 \in \mathfrak{a}_2\} \subseteq \mathfrak{a}_1S + \mathfrak{a}_2S$ .

(d) Since  $\mathfrak{a}_1 \cap \mathfrak{a}_2 \subseteq \mathfrak{a}_1, \mathfrak{a}_2$ ,  $(\mathfrak{a}_1 \cap \mathfrak{a}_2)S \subseteq \mathfrak{a}_1S, \mathfrak{a}_2S$ . So  $(\mathfrak{a}_1 \cap \mathfrak{a}_2)S \subseteq \mathfrak{a}_1S \cap \mathfrak{a}_2S$ .

Note  $x \in f^{-1}(\mathfrak{b}_1 \cap \mathfrak{b}_2)$  if and only if  $f(x) \in \mathfrak{b}_1 \cap \mathfrak{b}_2$  if and only if  $f(x) \in \mathfrak{b}_1, \mathfrak{b}_2$  if and only if  $x \in f^{-1}(\mathfrak{b}_1), f^{-1}(\mathfrak{b}_2)$  if and only if  $x \in f^{-1}(\mathfrak{b}_1) \cap f^{-1}(\mathfrak{b}_2)$ .

(e) “ $\subseteq$ ”. A set of generators of  $(\mathfrak{a}_1 \mathfrak{a}_2)S$  over  $S$  is

$$\left\{ f \left( \sum_i^{\text{finite}} \alpha_i \beta_i \right) = \sum_i^{\text{finite}} f(\alpha_i) f(\beta_i) \mid \alpha_i \in \mathfrak{a}_1, \beta_i \in \mathfrak{a}_2, \forall i \right\} \subseteq (\mathfrak{a}_1S)(\mathfrak{a}_2S).$$

“ $\supseteq$ ”. Note

$$\begin{aligned} (\mathfrak{a}_1S)(\mathfrak{a}_2S) &= (f(\mathfrak{a}_1)S)(f(\mathfrak{a}_2)S) = (f(\mathfrak{a}_1)f(\mathfrak{a}_2))S = \langle f(a_1)f(a_2) \mid a_1 \in \mathfrak{a}_1, a_2 \in \mathfrak{a}_2 \rangle S \\ &= \langle f(a_1a_2) \mid a_1 \in \mathfrak{a}_1, a_2 \in \mathfrak{a}_2 \rangle S \subseteq \langle f(\mathfrak{a}_1\mathfrak{a}_2) \rangle S = (\mathfrak{a}_1\mathfrak{a}_2)S. \end{aligned}$$

Moreover, let  $\sum_{i=1}^n a_{1i}a_{2i} \in f^{-1}(\mathfrak{b}_1)f^{-1}(\mathfrak{b}_2)$  for some  $n \geq 1$ ,  $a_{1i} \in f^{-1}(\mathfrak{b}_1)$  and  $a_{2i} \in f^{-1}(\mathfrak{b}_2)$  for  $i = 1, \dots, n$ . Then  $f(a_{1i}) \in \mathfrak{b}_1$  and  $f(a_{2i}) \in \mathfrak{b}_2$  for  $i = 1, \dots, n$ . Since  $f$  is a ring homomorphism,  $f(\sum_{i=1}^n a_{1i}a_{2i}) = \sum_{i=1}^n f(a_{1i})f(a_{2i}) \in \mathfrak{b}_1\mathfrak{b}_2$ . So  $\sum_{i=1}^n a_{1i}a_{2i} \in f^{-1}(\mathfrak{b}_1\mathfrak{b}_2)$ .

(f) A set of generators of  $(\mathfrak{a}_1 : \mathfrak{a}_2)S$  over  $S$  is

$$\begin{aligned} \{f(r) \mid r \in (\mathfrak{a}_1 : \mathfrak{a}_2)\} &= \{f(r) \mid r\mathfrak{a}_2 \subseteq \mathfrak{a}_1\} \subseteq \{f(r) \mid rf(\mathfrak{a}_2) \subseteq f(\mathfrak{a}_1)\} \subseteq \{s \in S \mid sf(\mathfrak{a}_2) \subseteq f(\mathfrak{a}_1)\} \\ &= \{s \in S \mid sf(\mathfrak{a}_2)S \subseteq f(\mathfrak{a}_1)S\} = \{s \in S \mid s\mathfrak{a}_2S \subseteq \mathfrak{a}_1S\} = (\mathfrak{a}_1S : \mathfrak{a}_2S). \end{aligned}$$

Note

$$\begin{aligned} f^{-1}(\mathfrak{b}_1 : \mathfrak{b}_2) &= \{f^{-1}(s) \mid s \in (\mathfrak{b}_1 : \mathfrak{b}_2)\} = \{f^{-1}(s) \mid s\mathfrak{b}_2 \subseteq \mathfrak{b}_1\} \subseteq \{f^{-1}(s) \mid sf^{-1}(\mathfrak{b}_2) \subseteq f^{-1}(\mathfrak{b}_1)\} \\ &\subseteq \{r \in R \mid rf^{-1}(\mathfrak{b}_2) \subseteq f^{-1}(\mathfrak{b}_1)\} = (f^{-1}(\mathfrak{b}_1) : f^{-1}(\mathfrak{b}_2)). \end{aligned}$$

(g) Let  $s \in \text{rad}(\mathfrak{a})S$ . Then there exist  $m \geq 1$ ,  $a_i \in \text{rad}(\mathfrak{a})$  and  $s_i \in S$  for  $i = 1, \dots, m$  such that  $s = \sum_{i=1}^m f(a_i)s_i$ . Since  $a_i \in \text{rad}(\mathfrak{a})$ , there exists  $n_i \geq 1$  such that  $a_i^{n_i} \in \mathfrak{a}$  for  $i = 1, \dots, m$ . Let  $n = n_1 + \dots + n_m$ . Note if  $k_1 + \dots + k_m = n$  with  $k_1, \dots, k_m \geq 0$ , then there exists some  $i \in \{1, \dots, m\}$  such that  $k_i \geq n_i$  and so  $a_i^{k_i} \in \mathfrak{a}$ . Hence

$$s^n = \left( \sum_{i=1}^m f(a_i)s_i \right)^n = \sum_{k_1 + \dots + k_m = n} \frac{n!}{k_1! \dots k_m!} f(a_1^{k_1} \dots a_m^{k_m}) s_1^{k_1} \dots s_m^{k_m} \subseteq f(\mathfrak{a})S = \mathfrak{a}S.$$

Thus,  $s \in \text{rad}(\mathfrak{a}S)$ .

Note  $x \in f^{-1}(\text{rad}(\mathfrak{b}))$  if and only if  $f(x) \in \text{rad}(\mathfrak{b})$  if and only if  $f(x^n) = f(x)^n \in \mathfrak{b}$  for some  $n \geq 1$  if and only if  $x^n \in f^{-1}(\mathfrak{b})$  for some  $n \geq 1$  if and only if  $x \in \text{rad}(f^{-1}(\mathfrak{b}))$ .  $\square$

**Proposition 1.64.**  $R^\times + \text{Nil}(R) \subseteq R^\times$ . For any  $u \in R^\times$  and  $x \in \text{Nil}(R)$ , we have  $u + x \in R^\times$ . For example,  $1 + x \in R^\times$ .

*Proof.* For any  $y \in \text{Nil}(R)$ , there is a  $n \geq 1$  such that  $y^n = 0$ , so  $(1 - y + y^2 - \dots + (-1)^{n-1}y^{n-1})(1 + y) = 1 - y^n = 1$ , hence  $1 + y \in R^\times$ .

Let  $u \in R^\times$  and  $x \in \text{Nil}(R)$ . Then  $u^{-1}x \in \text{Nil}(R)$ . So  $1 + u^{-1}x \in R^\times$ . Thus,  $u + x = u(1 + (u^{-1}x)) \in R^\times$ .  $\square$

## Power Series Rings

Let  $A$  be a nonzero commutative ring with identity.

**Definition 1.65.**

$$A[[X]] = \{f = \sum_{i=0}^{\infty} a_i X^i \mid a_i \in A, \forall i \geq 0\} \cong \prod_{i=0}^{\infty} A$$

with addition and multiplication defined by  $(\sum_{i=0}^{\infty} a_i X^i) + (\sum_{i=0}^{\infty} b_i X^i) = \sum_{i=0}^{\infty} (a_i + b_i) X^i$  and  $(\sum_{i=0}^{\infty} a_i X^i)(\sum_{i=0}^{\infty} b_i X^i) = \sum_{i=0}^{\infty} c_i X^i$ , where  $c_i = \sum_{j=0}^i a_j b_{i-j} = \sum_{p+q=i} a_p b_q$  for  $i \geq 0$ . Then  $A[[X]]$  is called a *power series ring* with  $0_{A[[X]]} = 0_A = \sum_{i=0}^{\infty} 0_A X^i$  and  $1_{A[[X]]} = 1_A = 1_A + \sum_{i=0}^{\infty} 0_A X^i$ . More generally,  $\mathfrak{a}[[X]] = \{\sum_{i=0}^{\infty} a_i X^i \mid a_i \in \mathfrak{a}, \forall i \geq 0\}$  for  $\mathfrak{a} \leq A$ .

**Example 1.66.**  $e^X = \sum_{i=0}^{\infty} \frac{1}{i!} X^i \in \mathbb{R}[[X]]$ .

**Theorem 1.67.**  $A[[X]]$  is a commutative ring with identity  $1_A$  and  $A \subseteq A[X] \subseteq A[[X]]$  are subrings.



**Proposition 1.68.** Let  $f(X) = \sum_{i=0}^{\infty} a_i X^i$  with  $a_i \in A$  for  $i \geq 0$ .

(a)  $f \in A[[X]]^\times$  if and only if  $a_0 \in A^\times$ .

(b) If  $\varphi : A \rightarrow B$  is a ring homomorphism, then there exists a well-defined ring homomorphism  $\varphi[[X]] : A[[X]] \rightarrow B[[X]]$  taking  $\sum_{i=0}^{\infty} \alpha_i X^i$  to  $\sum_{i=0}^{\infty} \varphi(\alpha_i) X^i$  and  $A[[X]] \geq \text{Ker}(\varphi[[X]]) = \text{Ker}(\varphi)[[X]]$ .

(c) For any  $\mathfrak{a} \leq A$ ,  $\mathfrak{a} \cdot A[[X]] \subseteq \mathfrak{a}[[X]] \leq A[[X]]$  and  $A[[X]]/\mathfrak{a}[[X]] \cong \frac{A}{\mathfrak{a}}[[X]]$ . In addition, if  $\mathfrak{a} \leq A$  is finitely generated,  $\mathfrak{a} \cdot A[[X]] = \mathfrak{a}[[X]]$ .

(d) Let  $\mathfrak{a} \leq A$ . Then

$$\langle X, \mathfrak{a} \rangle A[[X]] = X \cdot A[[X]] + \mathfrak{a} \cdot A[[X]] = XA[[X]] + \mathfrak{a}[[X]] = \left\{ \sum_{i=0}^{\infty} b_i X^i \mid b_0 \in \mathfrak{a}, b_i \in A, \forall i \geq 1 \right\} \leq A[[X]]$$

and  $A[[X]]/\langle X, \mathfrak{a} \rangle A[[X]] \cong A/\mathfrak{a}$ . In particular,  $\langle X \rangle A[[X]] = \{\sum_{i=1}^{\infty} b_i X^i \mid b_i \in A, \forall i \geq 1\} \leq A[[X]]$  and  $A[[X]]/\langle X \rangle A[[X]] \cong A$ .

(e) If  $f \in \text{Nil}(A[[X]])$ , then  $a_i \in \text{Nil}(A)$  for  $i \geq 0$ . The converse holds if  $\langle a_0, a_1, a_2, \dots \rangle$  is finitely generated. Also,  $\text{Nil}(A) \cdot A[[X]] \subseteq \text{Nil}(A[[X]]) \subseteq \text{Nil}(A)[[X]]$ .

(f)  $f \in \text{Jac}(A[[X]])$  if and only if  $a_0 \in \text{Jac}(A)$ . Also,  $\text{Jac}(A[[X]]) = \langle \text{Jac}(A), X \rangle A[[X]]$ .

(g)  $A[[X]]$  is an integral domain if and only if  $A$  is an integral domain. Also,  $A[[X]]$  is never a field.

(h)  $\mathfrak{a} \leq A$  is prime if and only if  $\mathfrak{a}[[X]] \leq A[[X]]$  is prime if and only if  $\langle \mathfrak{a}, X \rangle A[[X]] \leq A[[X]]$  is prime.

Let  $\epsilon : A \xrightarrow{\subseteq} A[[X]]$ . Then  $\epsilon^* : \text{Spec}(A[[X]]) \rightarrow \text{Spec}(A)$  taking  $\mathfrak{p}[[X]]$  to  $\epsilon^{-1}(\mathfrak{p}[[X]])$  is always onto and never 1-1.

(i)  $\mathfrak{a} \leq A$  is maximal if and only if  $\langle \mathfrak{a}, X \rangle A[[X]] \leq A[[X]]$  is maximal. Also,  $\mathfrak{a}[[X]] \leq A[[X]]$  is never maximal.

(j) Let  $\mathfrak{m} \in \text{m-Spec}(A[[X]])$ . Then

- (1)  $\mathfrak{m} \cap A \in \text{m-Spec}(A)$ ,
- (2)  $X \in \mathfrak{m}$ ,
- (3)  $\mathfrak{m} = \langle \mathfrak{m} \cap A, X \rangle A[[X]]$ .

Therefore,

$$\begin{aligned} \text{m-Spec}(A) &\xrightleftharpoons[\epsilon^*]{\Lambda} \text{m-Spec}(A[[X]]) \\ &\mathfrak{n} \mapsto \langle \mathfrak{n}, X \rangle A[[X]] \\ \mathfrak{m} \cap A &\leftrightarrow \mathfrak{m} \end{aligned}$$

*Proof.* (a) “ $\Rightarrow$ ”. Let  $f \in A[[X]]^\times$  with the multiplicative inverse  $f^{-1}(X) = \sum_{i=0}^{\infty} b_i X^i \in A[[X]]$  with  $b_i \in A$  for  $i \geq 0$ . Then  $1_A = f \cdot f^{-1} = (\sum_{i=0}^{\infty} a_i X^i)(\sum_{j=0}^{\infty} b_j X^j) = a_0 b_0 + (a_0 b_1 + a_1 b_0)X + \dots$ . So  $a_0 b_0 = 1_A$  and hence  $a_0 \in A^\times$ .

“ $\Leftarrow$ ”. We try to find  $g = \sum_{j=0}^{\infty} b_j X^j \in A[[X]]$  such that  $fg = 1$ , i.e.,  $1 = \sum_{i=0}^{\infty} (\sum_{j=0}^i a_j b_{i-j}) X^i$ . Then  $a_0 b_0 = 1$ ,  $a_0 b_1 + a_1 b_0 = 0$ ,  $a_0 b_2 + a_1 b_1 + a_2 b_0 = 0$ ,  $\dots$ . If  $a_0 = 1$ , then  $b_0 = a_0 b_0 = 1$  and we can solve  $b_n$  for  $n \geq 1$  one by one, so  $g$  is the inverse of  $f$  and hence  $f \in A[[X]]$ . If  $a_0 \neq 1$ , since  $a_0 b_0 = 1$ , we have  $a_0 \in A^\times$  and so by definition of multiplication in  $A[[X]]$ ,

$$f = \sum_{i=0}^{\infty} a_i X^i = \sum_{i=0}^{\infty} a_0 (a_0^{-1} a_i) X^i = a_0 \underbrace{\left( 1 + \sum_{i=1}^{\infty} (a_0^{-1} a_i) X^i \right)}_{\in A[[X]]^\times} \in A[[X]]^\times.$$

(b) It is straightforward to show  $\varphi[[X]]$  is a well-defined ring homomorphism with

$$\begin{aligned} \text{Ker}(\varphi[[X]]) &= \left\{ \sum_{i=0}^{\infty} \alpha_i X^i \mid \sum_{i=0}^{\infty} \varphi(\alpha_i) X^i = 0 \right\} = \left\{ \sum_{i=0}^{\infty} \alpha_i X^i \mid \varphi(\alpha_i) = 0, \forall i \geq 0 \right\} \\ &= \left\{ \sum_{i=0}^{\infty} \alpha_i X^i \mid \alpha_i \in \text{Ker}(\varphi), \forall i \geq 0 \right\} = \text{Ker}(\varphi)[[X]]. \end{aligned}$$

(c) Let  $\tau : A \twoheadrightarrow A/\mathfrak{a}$  be the natural projection. Then by (b),  $\tau[[X]] : A[[X]] \rightarrow \frac{A}{\mathfrak{a}}[[X]]$  is a well-defined ring homomorphism with  $A[[X]] \geq \text{Ker}(\tau[[X]]) = \text{Ker}(\tau)[[X]] = \mathfrak{a}[[X]]$ . Since  $\tau$  is onto, by the first isomorphism theorem,  $A[[X]]/\mathfrak{a}[[X]] \cong \frac{A}{\mathfrak{a}}[[X]]$ . Since  $\mathfrak{a} \subseteq \text{Ker}(\tau[[X]])$ , we have  $\langle \mathfrak{a} \rangle A[[X]] \subseteq \text{Ker}(\tau[[X]]) = \mathfrak{a}[[X]]$ .

In addition, assume  $\mathfrak{a} = (\alpha_1, \dots, \alpha_n)A$  for some  $\alpha_1, \dots, \alpha_n \in \mathfrak{a}$ . Let  $f \in \mathfrak{a}[[X]]$ . Then  $a_i \in \mathfrak{a} = (\alpha_1, \dots, \alpha_n)A$  for  $i \geq 0$ . So for  $i \geq 0$ , we have  $a_i = \sum_{j=1}^n b_{ij} \alpha_j$  for some  $b_{i1}, \dots, b_{in} \in A$ . Hence by the definition of addition and multiplication in  $A[[X]]$ ,

$$f = \sum_{i=0}^{\infty} a_i X^i = \sum_{i=0}^{\infty} \left( \sum_{j=1}^n b_{ij} \alpha_j \right) X^i = \sum_{j=1}^n \left( \sum_{i=0}^{\infty} \alpha_j b_{ij} X^i \right) = \sum_{j=1}^n \alpha_j \left( \sum_{i=0}^{\infty} b_{ij} X^i \right) \in \langle \mathfrak{a} \rangle A[[X]].$$

(d) Note

$$\begin{array}{ccc} A[[X]] & \xrightarrow{\pi} & A \\ \tau[[X]] \downarrow & \begin{array}{ccc} \sum_{i=0}^{\infty} b_i X^i & \longmapsto & b_0 \\ \downarrow & & \downarrow \\ \sum_{i=0}^{\infty} \bar{b}_i X^i & \longmapsto & \bar{b}_0 \end{array} & \downarrow \tau \\ \frac{A}{\mathfrak{a}}[[X]] & \xrightarrow{\pi'} & \frac{A}{\mathfrak{a}} \end{array}$$

It is straightforward to show  $\pi$  and  $\pi^{-1}$  are well-defined ring epimorphisms and the diagram commutes.

Note

$$\text{Ker}(\pi) = \left\{ \sum_{i=1}^{\infty} b_i X^i \mid b_i \in A, \forall i \geq 1 \right\} = X \left\{ \sum_{i=0}^{\infty} b_{i+1} X^i \mid b_{i+1} \in A, \forall i \geq 0 \right\} = X \cdot A[[X]].$$

In general,

$$A[[X]] \geq \text{Ker}(\tau \circ \pi) = \left\{ \sum_{i=0}^{\infty} b_i X^i \mid b_0 \in \mathfrak{a}, b_i \in A, \forall i \geq 1 \right\} =: I.$$

Let  $\sum_{i=0}^{\infty} b_i X^i \in I$  with  $b_0 \in \mathfrak{a}$  and  $b_i \in A$  for  $i \geq 1$ . Then  $\sum_{i=0}^{\infty} b_i X^i = b_0 + X \sum_{i=0}^{\infty} b_{i+1} X^i \in \mathfrak{a} + XA[[X]] \subseteq \langle X, \mathfrak{a} \rangle A[[X]]$ . So  $I \subseteq \langle X, \mathfrak{a} \rangle A[[X]]$ .

Since  $X = 0 + 1 \cdot X$  and  $0 \in \mathfrak{a}$  and  $1 \in A$ , we have  $X \in I \leq A[[X]]$ . Also, for  $\sum_{i=0}^{\infty} b_i X^i \in \mathfrak{a}[[X]] \leq A[[X]]$  with  $b_0 \in \mathfrak{a}$  and  $b_i \in \mathfrak{a} \subseteq A$  for  $i \geq 1$ , we have  $\sum_{i=0}^{\infty} b_i X^i \in I$  and so  $\mathfrak{a}[[X]] \subseteq I$ . Hence  $\langle X \rangle A[[X]] + \mathfrak{a}[[X]] \subseteq I$ .

Thus, by (c),

$$\langle X, \mathfrak{a} \rangle A[[X]] \supseteq I \supseteq \langle X \rangle A[[X]] + \mathfrak{a}[[X]] \supseteq \langle X \rangle A[[X]] + \langle \mathfrak{a} \rangle A[[X]] = \langle X, \mathfrak{a} \rangle A[[X]].$$

So  $\langle X, \mathfrak{a} \rangle A[[X]] = \langle X \rangle A[[X]] + \langle \mathfrak{a} \rangle A[[X]] = \langle X \rangle A[[X]] + \mathfrak{a}[[X]] = I = \text{Ker}(\tau \circ \pi)$ . By the first isomorphism theorem,  $A[[X]]/\langle X, \mathfrak{a} \rangle A[[X]] \cong A/\mathfrak{a}$ .

(e) Assume  $f \in \text{Nil}(A[[X]])$ . Then  $0 = f^n = a_0^n + Xg(X)$  for some  $n \geq 1$  and  $g \in A[[X]]$ . So  $a_0^n = 0$  and then  $a_0 \in \text{Nil}(A) \subseteq \text{Nil}(A[[X]])$ . Hence  $\sum_{i=1}^{\infty} a_i X^i = f - a_0 \in \text{Nil}(A[[X]])$ . Similarly, we have  $a_1 \in \text{Nil}(A[[X]])$ . By induction,  $a_i \in \text{Nil}(A)$  for  $i \geq 0$ .

So we can conclude  $\text{Nil}(A[[X]]) \subseteq \text{Nil}(A)[[X]]$ . Furthermore, since  $\text{Nil}(A) \subseteq \text{Nil}(A[[X]]) \leq A[[X]]$ , we have  $\text{Nil}(A) = \text{Nil}(\text{Nil}(A)) \subseteq \text{Nil}(A[[X]]) \leq A[[X]]$  and then  $\text{Nil}(A) \cdot A[[X]] \subseteq \text{Nil}(A[[X]])$ . Thus,  $\text{Nil}(A) \cdot A[[X]] \subseteq \text{Nil}(A[[X]]) \subseteq \text{Nil}(A)[[X]]$ .

Assume  $a_i \in \text{Nil}(A)$  for  $i \geq 0$  and  $\langle a_0, a_1, \dots \rangle$  is finitely generated. Then  $\langle a_0, a_1, \dots \rangle = \langle a_0, a_1, \dots, a_t \rangle$  for some  $t \geq 1$ . So  $f = \sum_{i=0}^{\infty} a_i X^i = \sum_{j=0}^t a_j f_j$ , where  $f_j \in \text{Nil}(A) \cdot A[[X]] \subseteq \text{Nil}(A[[X]]) \leq A[[X]]$  for  $j = 0, \dots, t$ . Thus,  $f \in \text{Nil}(A[[X]])$ .

(f) “ $\Rightarrow$ ”. Assume  $f \in \text{Jac}(A[[X]])$ . Then by Proposition 1.29,  $1 - fg \in A[[X]]^\times$  for  $g \in A[[X]]$ . So  $(1 - a_0 a) + a_1 a x + a_2 a x^2 + \dots = 1 - fa \in A[[X]]^\times$  for  $a \in A$ . Then by (a),  $1 - a_0 a \in A^\times$  for  $a \in A$ . Hence  $a_0 \in \text{Jac}(A)$  by Proposition 1.29.

“ $\Leftarrow$ ”. If  $a_0 \in \text{Jac}(A)$ , then  $1 - a_0 a \in A^\times$  for  $a \in A$ . Let  $g = \sum_{i=0}^{\infty} b_i X^i \in A[[X]]$  with  $b_i \in A$  for  $i \geq 0$ . To show  $f \in \text{Jac}(A[[X]])$ . Need to show  $1 - fg \in A[[X]]^\times$ . By (a), it is equivalent to show the constant term of  $1 - fg$  is in  $A^\times$ . Note  $1 - fg = 1 - (\sum_{i=0}^{\infty} a_i X^i)(\sum_{i=0}^{\infty} b_i X^i) = \underbrace{(1 - a_0 b_0)}_{\in A^\times} + \dots$ .

Thus,  $\text{Jac}(A[[X]]) = \{\sum_{i=0}^{\infty} a_i X^i \mid a_0 \in \text{Jac}(A)\} = \langle \text{Jac}(A), X \rangle A[[X]]$  by (d).

(g) Define  $\text{ord}(f) = \inf\{i \geq 0 \mid a_i \neq 0\}$ . Then  $\text{ord}(fg) \geq \text{ord}(f) + \text{ord}(g)$  with equality if, e.g.,  $A$  is an integral domain.

“ $\Leftarrow$ ”. Let  $A$  be an integral domain and  $f, g \neq 0$  in  $A[[X]]$ . Then  $\text{ord}(f), \text{ord}(g) \neq \infty$ . So  $\text{ord}(fg) = \text{ord}(f) + \text{ord}(g) \neq \infty$ . Hence  $fg \neq 0$ .

“ $\Rightarrow$ ”. Let  $A[[X]]$  be an integral domain. Since  $0 \neq A$  is a subring of  $A[[X]]$ ,  $A$  is also an integral domain.

Since  $X \in A[[X]]$  and the constant term of  $X$  is 0, which is not in  $A^\times$ , by (a),  $X \notin A[[X]]^\times$ . So  $A[[X]]$  is not a field.

(h) Note  $\mathfrak{a} \leq A$  is prime if and only if  $A/\mathfrak{a}$  is an integral domain if and only if  $\frac{A[X]}{\mathfrak{a}[X]}$  is an integral domain by (g) if and only if  $A[X]/\mathfrak{a}[X]$  is an integral domain by (c) if and only if  $\mathfrak{a}[X] \leq A[X]$  is prime.

Note  $\mathfrak{a} \leq A$  is prime if and only if  $A/\mathfrak{a}$  is an integral domain if and only if  $\frac{A[X]}{\langle X, \mathfrak{a} \rangle A[X]}$  is an integral domain by (d) if and only if  $\langle \mathfrak{a}, X \rangle A[X] \leq A[X]$  is prime.

Let  $\mathfrak{p} \in \text{Spec}(A)$ . Then  $\mathfrak{p}[X], \langle \mathfrak{p}, X \rangle A[X] \in \text{Spec}(A[X])$ .

By the proof of (c) and (d), we have  $\mathfrak{p}[X] \cap A = \mathfrak{p}$  and  $\langle \mathfrak{p}, X \rangle A[X] \cap A = \mathfrak{p}$ . So by Fact 1.16,

$$\epsilon^*(\mathfrak{p}[X]) = \epsilon^{-1}(\mathfrak{p}[X]) = \mathfrak{p}[X] \cap A = \mathfrak{p} = (\langle \mathfrak{p}, X \rangle A[X]) \cap A = \epsilon^{-1}(\langle \mathfrak{p}, X \rangle A[X]) = \epsilon^*(\langle \mathfrak{p}, X \rangle A[X]).$$

Thus,  $\epsilon^*$  is onto. Also, since  $X \notin \mathfrak{p}[X]$ , but  $X \in \langle \mathfrak{p}, X \rangle A[X]$ , we have  $\mathfrak{p}[X] \neq \langle \mathfrak{p}, X \rangle A[X]$  and then  $\epsilon^*$  is not 1-1.

(i) Note  $\mathfrak{a} \leq A$  is maximal if and only if  $A/\mathfrak{a}$  is a field if and only if  $A[X]/\langle X, \mathfrak{a} \rangle A[X]$  is a field by (d) if and only if  $\langle \mathfrak{a}, X \rangle A[X] \leq A[X]$  is maximal.

Since  $\frac{A[X]}{\mathfrak{a}[X]}$  is not a field by (g),  $A[X]/\mathfrak{a}[X]$  is not a field by (c), then  $\mathfrak{a}[X] \leq A[X]$  is not maximal.

(j) (2) Since  $X \in \text{Jac}(A[X])$  by (f), and  $\mathfrak{m} \in \text{m-Spec}(A[X])$ , we have  $X \in \mathfrak{m}$ .

(1) By prime correspondence under quotients, we have  $\mathfrak{m}$  corresponds to a maximal ideal in  $A[X]/\langle X \rangle A[X] \cong A$  by (d).

$$\begin{array}{ccc} A[X] & \xrightarrow{\pi} & A[X]/\langle X \rangle A[X] \xrightarrow{\cong} A \\ \mathfrak{m} & \rightsquigarrow & \mathfrak{m}/\langle X \rangle A[X] \rightsquigarrow \mathfrak{n} \end{array}$$

Define  $\tau : A[X] \rightarrow A$  by  $\tau(f) = f(0)$ . Then we can find  $\mathfrak{n} \in \text{m-Spec}(A)$  such that  $\mathfrak{m} = \tau^{-1}(\mathfrak{n})$ . So

$$\mathfrak{m} \cap A = \epsilon^{-1}(\mathfrak{m}) = \epsilon^{-1}(\tau^{-1}(\mathfrak{n})) = (\tau \circ \epsilon)^{-1}(\mathfrak{n}) = \text{id}_A^{-1}(\mathfrak{n}) = \mathfrak{n} \in \text{m-Spec}(A).$$

(3) Since  $\mathfrak{m} \cap A, \langle X \rangle \subseteq \mathfrak{m}$ , we have  $\langle \mathfrak{m} \cap A, X \rangle \subseteq \mathfrak{m}$ . Since  $\mathfrak{m} \leq A[X]$  is maximal, and by (i) and (1),  $\langle \mathfrak{m} \cap A, X \rangle \leq A[X]$  are maximal, we have  $\langle \mathfrak{m} \cap A, X \rangle = \mathfrak{m}$ .

Note  $\epsilon^*(\text{m-Spec}(A[X])) \subseteq \text{m-Spec}(A)$  since by the proof of (1),  $\epsilon^*(\mathfrak{m}) = \epsilon^{-1}(\mathfrak{m}) \in \text{m-Spec}(A)$ .

Note  $\Lambda(\text{m-Spec}(A)) \subseteq \text{m-Spec}(A[X])$  since by (i),  $\Lambda(\mathfrak{n}) = \langle \mathfrak{n}, X \rangle A[X] \in \text{Spec}(A[X])$  for any  $\mathfrak{n} \in \text{Spec}(A)$ .

Note  $\Lambda(\epsilon^*(\mathfrak{m})) = \Lambda(\epsilon^{-1}(\mathfrak{m})) = \Lambda(\mathfrak{m} \cap A) = \langle \mathfrak{m} \cap A, X \rangle A[X] = \mathfrak{m}$  by (3).

Note  $\epsilon^*(\Lambda(\mathfrak{n})) = \epsilon^*(\langle \mathfrak{n}, X \rangle A[X]) = \epsilon^{-1}(\langle \mathfrak{n}, X \rangle A[X]) = \langle \mathfrak{n}, X \rangle \cap A = \mathfrak{n}$  by the proof of (c) for any  $\mathfrak{n} \leq \text{m-Spec}(A)$ .

Therefore, we have a 1-1 correspondence between  $\text{m-Spec}(A[X])$  and  $\text{m-Spec}(A)$ .  $\square$

**Example 1.69.** (c) Example of  $\langle \mathfrak{a} \rangle A[X] \subsetneq \mathfrak{a}[X]$  for some  $\mathfrak{a} \leq A$ . Let  $A = k[Y_1, Y_2, Y_3, \dots]$  and  $\mathfrak{a} = \langle Y_1, Y_2, Y_3, \dots \rangle A$ . Let  $f = \sum_{i=1}^{\infty} Y_i X^i \in \mathfrak{a}[X]$ . Claim.  $f \notin \langle \mathfrak{a} \rangle A[X] = \langle Y_1, Y_2, \dots \rangle A[X]$ . Suppose  $f \in \langle Y_1, Y_2, \dots \rangle A[X]$ . Then there exists  $m \geq 1$  and  $\sum_{j=0}^{\infty} b_{ij} X^j = g_i \in A[X]$  for  $i = 1, \dots, m$  such that  $\sum_{j=1}^{\infty} Y_j X^j = f = \sum_{i=1}^m g_i Y_i = \sum_{i=1}^m (\sum_{j=0}^{\infty} b_{ij} X^j) Y_i = \sum_{j=0}^{\infty} (\sum_{i=1}^m b_{ij} Y_i) X^j$ . So for  $j \geq 1$ , we have  $Y_j = \sum_{i=1}^m b_{ij} Y_i \in \langle Y_1, \dots, Y_m \rangle A$ . Then  $Y_{m+1} \in \langle Y_1, \dots, Y_m \rangle A$ , a contradiction.

(e) Example of  $f \notin \text{Nil}(A[[X]])$  when  $a_i \in \text{Nil}(A)$  for  $i \geq 0$ . Let  $A = \frac{\mathbb{Q}[Y_1, Y_2, Y_3, \dots]}{\langle Y_1^2, Y_2^3, Y_3^4, \dots, Y_i^{i+1}, \dots \rangle}$  and  $a_0 = 0 \in \text{Nil}(A)$  and  $a_i = \bar{Y}_i$  for  $i \geq 1$ . Then  $a_i^{i+1} = \bar{Y}_i^{i+1} = 0$  and so  $a_i \in \text{Nil}(A)$  for  $i \geq 1$ .

Claim.  $f \notin \text{Nil}(A[[X]])$ . Note  $f^2 = (\sum_{i=1}^{\infty} \bar{Y}_i X^i)^2 = \underbrace{\bar{Y}_1^2 X^2}_{=0} + \underbrace{(2\bar{Y}_1 \bar{Y}_2) X^3}_{\neq 0} + \dots$ , and  $f^3 = (\sum_{i=1}^{\infty} \bar{Y}_i X^i)^3 = \underbrace{\bar{Y}_1^3 X^3}_{=0} + \underbrace{(2\bar{Y}_1 \bar{Y}_2 + \bar{Y}_2^2) X^4}_{\neq 0} + \dots$ , and inductively, we find  $f^n$  has lots of nonzero coefficients for  $n \geq 1$ .

**Definition 1.70.** Define

$$A[[X, Y]] = A[[X]][[Y]],$$

and for  $d \geq 2$ ,

$$A[[X_1, \dots, X_d]] = A[[X_1, \dots, X_{d-1}]][[X_d]].$$

**Fact 1.71.**  $A[[X_1, \dots, X_d]] = \{\sum_{\underline{n} \in \mathbb{N}_0^d} a_{\underline{n}} \underline{X}^{\underline{n}} \mid a_{\underline{n}} \in A\}$  for  $d \geq 1$ , where  $\underline{X}^{\underline{n}} = X_1^{n_1} \dots X_d^{n_d}$  and  $\underline{n} = (n_1, \dots, n_d) \in \mathbb{N}_0^d$ .

**Warning 1.72.** The operations on  $A[[X_1, X_2, X_3, \dots]]$  are ambiguous.

## U.F.D.

Let  $k$  be a field.

**Definition 1.73.** An integral domain is a U.F.D. if it is *atomic* (every nonzero nonunit of  $R$  can be factored into irreducibles) and given two irreducible factorizations  $\alpha_1 \dots \alpha_n = \beta_1 \dots \beta_n$ ,

- (a)  $n = m$ ,
- (b) there exists  $\sigma \in S_n$  such that  $\alpha_i = u_i \beta_{\sigma(i)}$  with  $u_i \in R^\times$  for  $i = 1, \dots, n$ .

**Example 1.74.** Examples of UFD's:  $k$ ,  $\mathbb{Z}$ ,  $\mathbb{Z}[i]$ ,  $\mathbb{Z}[\frac{-1+\sqrt{-3}}{2}]$ ,  $\mathbb{Z}[\frac{-1+\sqrt{-19}}{2}]$ ,  $k[X]$ ,  $k[[X]]$ ,  $k[X_1, \dots, X_n]$ ,  $k[[X_1, \dots, X_n]]$  and  $k[[\{X_i\}_{i \in I}]]$ .

**Definition 1.75.** We say  $x \in R$  is *irreducible* if  $x = ab$ , then  $a$  or  $b$  is a unit.

**Definition 1.76.** We say  $x \in R$  is *prime* if  $x$  is a nonunit and  $x \mid a$  or  $x \mid b$  whenever  $x \mid ab$ .

**Example 1.77.** Examples of non-UFD's:

- (a)  $\mathbb{Z}[\sqrt{-5}] = \{m + n\sqrt{-5} \mid m, n \in \mathbb{Z}\}$ , where  $6 = (2)(3) = (1 + \sqrt{-5})(1 - \sqrt{-5})$ .
- (b)  $k[X^2, X^3] = \{a_0 + a_2 X^2 + a_3 X^3 + a_4 X^4 + \dots + a_n X^n \mid n \geq 0, a_i \in k, \forall i = 0, 2, 3, \dots, n\}$ , where  $X^6 = X^2 \cdot X^2 \cdot X^2 = X^3 \cdot X^3$  with  $X^2$  and  $X^3$  irreducible here.

**Definition 1.78.** An integral domain  $R$  is a UFD if every nonzero nonunit element is a product of primes.

**Theorem 1.79.** If  $R$  is a UFD, then so is

- (a)  $R[\{X_i\}_{i \in I}]$ ,

(b)  $R_U$ , where  $0 \notin U \subseteq R$  is multiplicatively closed.

**Fact 1.80.** If  $R$  is a UFD, it is integrally closed.

**Theorem 1.81.** Let  $R$  be an integral domain. Then  $R$  is a UFD if and only if every nonzero prime ideal contains some nonzero prime element.

**Theorem 1.82.** If  $R$  is a PID, then  $R[[X]]$  is a UFD.

**Example 1.83.** There exists some UFD's  $R$  such that  $R[[X]]$  is not a UFD.

**Question 1.84.** If  $R[[X]]$  is a UFD, is  $R[[X, Y]]$  a UFD?

**Example 1.85.** We have  $\mathbb{Q}[X] = \mathbb{Q} + X\mathbb{Q}[X]$ . Let

$$R = \mathbb{Z} + X\mathbb{Q}[X] = \{n + q_1x + \cdots + q_kX^k \mid n \in \mathbb{Z}, k \geq 1, q_i \in \mathbb{Q}, \forall i = 1, \dots, k\}.$$

Then  $x \in R$  cannot be factored into irreducibles since  $x = 13 \cdot \frac{x}{13} = 3 \cdot 13 \cdot \frac{x}{39} = 3^n \cdot 13^m \cdot \frac{x}{3^n 13^m}$  for  $n, m \geq 0$ .

**Example 1.86.** Let  $R = k[X_1, X_2, X_3, \dots, \frac{X_1}{X_2}, \frac{X_1}{X_2^2}, \frac{X_1}{X_2^3}, \dots, \frac{X_2}{X_3}, \frac{X_2}{X_3^2}, \dots, \dots, \frac{X_n}{X_{n+1}}, \frac{X_n}{X_{n+1}^2}, \dots]$ . Let  $\mathfrak{m}$  be the maximal ideal  $(X_1, X_2, X_3, \dots, \frac{X_n}{X_{n+1}}, \frac{X_n}{X_{n+1}^2}, \dots)$  of  $R$ . Then  $R_{\mathfrak{m}}$  has no irreducible elements and is not a field.

**Example 1.87.** We have  $\mathbb{Q}[X]/(X^2 - 2) \cong \mathbb{Q}(\sqrt{2})$ . Let  $\bar{\mathbb{Q}} = \mathbb{Q}(\{\alpha \mid f \in \mathbb{Q}[X] \text{ irreducible, } f(\alpha) = 0\})$ , i.e.,  $\bar{\mathbb{Q}}$  is the algebraic closure of  $\mathbb{Q}$ . Let  $\bar{\mathbb{Z}} = \{\alpha \in \bar{\mathbb{Q}} \mid g \in \mathbb{Z}[X] \text{ monic, } g(\alpha) = 0\}$ . Let  $\alpha \in \bar{\mathbb{Z}}$  and suppose  $\alpha$  is irreducible. Then there exists  $n \geq 1$  and  $a_i \in \mathbb{Z}$  for  $i = 0, \dots, n-1$  such that  $\alpha$  is a root of  $x^n + a_{n-1}x^{n-1} + \cdots + a_0$ . Consider  $x^{2n} + a_{n-1}x^{2n-2} + \cdots + a_0$  has a root  $\beta \in \bar{\mathbb{Z}}$  such that  $\beta^2 = \alpha$ .

## Generalization of U.F.D.

Let  $R$  be an integral domain.

**Definition 1.88.** We say  $R$  is an HFD (*half-factorial*) if  $R$  is atomic and given  $\alpha_1 \cdots \alpha_n = \beta_1 \cdots \beta_m$  irreducible factorizations, then  $n = m$ .

**Example 1.89.**  $\mathbb{Z}[\sqrt{-5}]$  is an HFD.  $\mathbb{Z}[\sqrt{-14}] = \{a + b\sqrt{-14} \mid a, b \in \mathbb{Z}\}$  is not a HFD since  $81 = 3 \cdot 3 \cdot 3 \cdot 3 = (5 + 2\sqrt{-14})(5 - 2\sqrt{-14})$ .

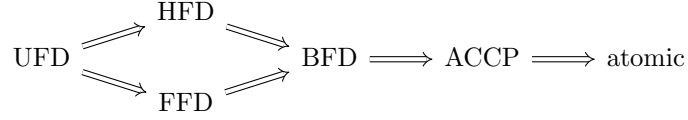
**Definition 1.90.**  $R$  is a FFD (*finite factorial*) if  $R$  is atomic and every nonzero nonunit has only finitely many factorizations (up to units).

**Example 1.91.** Any ring of algebraic integers is a FFD.

**Definition 1.92.**  $R$  is a BFD (*bounded*) if  $R$  is atomic and for all nonzero nonunit, there exists a bound on the length of irreducible factorizations.

**Definition 1.93.**  $R$  is ACCP (*ascending chain condition on principal ideals*) if  $(a_1) \subseteq (a_2) \subseteq (a_3) \subseteq \cdots$  stabilizes.

**Proposition 1.94.** We have



**Example 1.95.** In  $\mathbb{Q} + X\mathbb{R}[[X]]$ ,  $X^2$  has uncountable many factorizations all of which have length 2, for example,  $X^2 = X \cdot X = (\pi X)(\frac{X}{\pi})$ .

**Fact 1.96.** If  $R$  is a FFD, BFD, ACCP, so is  $R[X]$ .

**Fact 1.97.** If  $R$  is atomic, then  $R[X]$  is not necessarily atomic.

**Fact 1.98.** If  $R$  is not an integral domain, there is an example of a ring  $R$  with no irreducibles such that  $R[X]$  is atomic.

**Example 1.99.** Consider factorization only in a monoid  $\langle 0, 2, 3, 4, 5, 6 \rangle$ , 2, 3 are irreducibles.  $\langle \frac{1}{2 \cdot 3}, \frac{1}{2^2 \cdot 5}, \frac{1}{2^3 \cdot 7}, \dots, \frac{1}{2^n p_n}, \dots \rangle$  is atomic but not ACCP.

## Chapter 2

# Zariski Topology

Let  $R$  be a nonzero commutative ring with identity.

**Definition 2.1.** For  $\epsilon > 0$  and  $x \in \mathbb{R}^n$ , the *open ball* centered at  $x$  with radius  $\epsilon$  is

$$B_\epsilon(x) = \{y \in \mathbb{R}^n \mid |x - y| < \epsilon\}.$$

A subset  $U \subseteq \mathbb{R}^n$  is *open* if for any  $x \in U$ , there exists  $\epsilon > 0$  such that  $B_\epsilon(x) \subseteq U$ , i.e., if  $U$  is a union of (possibly infinitely many) open balls. e.g., if  $n = 1$ ,  $B_\epsilon(x) = (x - \epsilon, x + \epsilon)$  is an open interval.

More generally, this works for any metric space.

**Fact 2.2.**  $\mathbb{R}^n$  and  $\emptyset$  are both open in  $\mathbb{R}^n$ .

The set of open sets in  $\mathbb{R}^n$  is closed under arbitrary union and finite intersection, i.e., if  $U_\lambda$  is open for  $\lambda \in \Lambda$ , then  $\bigcup_{\lambda \in \Lambda} U_\lambda$  is open, and if  $U_i$  open for  $i = 1, \dots, d$ , then  $\bigcap_{i=1}^d U_i$  is open.

The set of open sets in  $\mathbb{R}^n$  is (usually) not closed under infinite intersections. For example,  $\bigcap_{i=1}^\infty (-1/i, 1/i) = \{0\}$ , is not open in  $\mathbb{R}^n$ .

**Definition 2.3.** A *topology* on a non-empty set  $X$  is a collection of sets  $\mathcal{T}$  of subsets of  $X$  ( $\mathcal{T} \subseteq \mathcal{P}(X)$ ) such that

- (a)  $\emptyset, X \in \mathcal{T}$ ,
- (b) for any  $\{U_\lambda\}_{\lambda \in \Lambda} \subseteq \mathcal{T}$ ,  $\bigcup_{\lambda \in \Lambda} U_\lambda \in \mathcal{T}$  and
- (c) for  $n \geq 1$  and  $U_1, \dots, U_n \in \mathcal{T}$ ,  $\bigcap_{i=1}^n U_i \in \mathcal{T}$ .

The elements of  $\mathcal{T}$  are the *open subsets* of  $X$ .

A *topological space* is a set  $X \neq \emptyset$  equipped with a topology  $\mathcal{T}$ .

**Example 2.4.** The *Euclidean topology* on  $\mathbb{R}^n$  is the topology on  $\mathbb{R}^n$  from Definition 2.1. More generally, this is the metric space topology.

**Definition 2.5.** The *Zariski topology* on  $\text{Spec}(R) = X$  has open sets

$$\{\text{Spec}(R) \setminus V(S) \mid S \subseteq R\} = \{\mathfrak{p} \in \text{Spec}(R) \mid \mathfrak{p} \not\supseteq S \subseteq R\}.$$

For example,  $X_f := \text{Spec}(R) \setminus V(\{f\}) = \{\mathfrak{p} \in \text{Spec}(R) \mid f \notin \mathfrak{p}\}$  is open in  $X$  for  $f \in R$ .



**Proposition 2.6.** If  $S \subseteq R$ , then  $V(S) = V(\langle S \rangle)$  and so  $\text{Spec}(R) \setminus V(S) = \text{Spec}(R) \setminus V(\langle S \rangle)$ . In other words, the open sets are exactly the sets  $\{\text{Spec}(R) \setminus V(\mathfrak{a}) \mid \mathfrak{a} \leq R\}$ .

**Notation.** Denote the Zariski open sets  $\mathcal{Z} = \{\text{Spec}(R) \setminus V(S) \mid S \subseteq R\} = \{\text{Spec}(R) \setminus V(\mathfrak{a}) \mid \mathfrak{a} \leq R\}$ .

**Example 2.7.** Compute  $\mathcal{Z}$  of  $\text{Spec}(\mathbb{Z}) = X$ . Since  $\mathbb{Z}$  is a P.I.D.,  $\mathcal{Z} = \{\text{Spec}(\mathbb{Z}) \setminus V(m) \mid m \geq 0\}$ . Since  $V(0) = \text{Spec}(\mathbb{Z})$ ,  $X_0 = \text{Spec}(\mathbb{Z}) \setminus V(0) = \emptyset$ , and since  $V(1) = \emptyset$ ,  $X_1 = \text{Spec}(\mathbb{Z}) \setminus V(1) = \text{Spec}(\mathbb{Z})$ . For  $m \geq 2$ , write  $m = p_1^{e_1} \cdots p_n^{e_n}$  with  $p_1, \dots, p_n$  distinct primes and  $e_1, \dots, e_n \geq 1$ , then  $V(m) = \{\langle p_1 \rangle, \dots, \langle p_n \rangle\}$  and so  $X_m = \text{Spec}(\mathbb{Z}) \setminus V(m) = X \setminus \{\langle p_1 \rangle, \dots, \langle p_n \rangle\}$ . Note  $\mathcal{Z} = \bigcup_{m=0}^{\infty} X_m$ . In particular,  $\mathfrak{p} = \{0\} \in \bigcap_{m=1}^{\infty} X_m$ , i.e.,  $\mathfrak{p} = \{0\}$  is in every non-empty open set of  $X$ .

**Fact 2.8.** Let  $X = \text{Spec}(R)$ . Then  $X_0 = X \setminus V(0) = \emptyset$  and  $X_1 = X \setminus V(1) = X$ .

**Proposition 2.9.** Let  $X = \text{Spec}(R)$ . Then  $\bigcap_{i=1}^n X_{f_i} = X_{f_1 \cdots f_n}$  for  $f_1, \dots, f_n \in R$ .

*Proof.* Let  $\mathfrak{p} \in X$ . Then  $\mathfrak{p} \in \bigcap_{i=1}^n X_{f_i}$  if and only if  $\mathfrak{p} \in X_{f_i}$  for  $i = 1, \dots, n$  if and only if  $f_i \notin \mathfrak{p}$  for  $i = 1, \dots, n$  if and only if  $f_1 \cdots f_n \notin \mathfrak{p}$  if and only if  $\mathfrak{p} \in X_{f_1 \cdots f_n}$ .  $\square$

**Definition 2.10.** If  $X$  is a topological space, then  $Y \subseteq X$  is *closed* if  $X \setminus Y$  open, i.e., if and only if  $Y = X \setminus U$  for some open subset  $U \subseteq X$ .

**Example 2.11.** In  $\text{Spec}(R) = X$ , the closed sets are  $\{V(S) \mid S \subseteq R\} = \{V(\mathfrak{a}) \mid \mathfrak{a} \leq R\}$ .

**Proposition 2.12.** Let  $X$  be a non-empty set,  $\mathcal{V} \subseteq \mathcal{P}(X)$  and  $\mathcal{V} = \{X \setminus Y \mid Y \in \mathcal{V}\}$ . Then  $\mathcal{V}$  is a topology on  $X$  if and if only  $\mathcal{V}$  satisfies the followings.

- (a)  $X, \emptyset \in \mathcal{V}$ ,
- (b) closed under arbitrary intersections, i.e., for any  $\{V_\lambda\}_{\lambda \in \Lambda} \subseteq \mathcal{V}$ , then  $\bigcap_{\lambda \in \Lambda} V_\lambda \in \mathcal{V}$ ,
- (c) closed under finite unions, i.e., for  $n \geq 1$  and  $V_1, \dots, V_n \in \mathcal{V}$ ,  $\bigcup_{i=1}^n V_i \in \mathcal{V}$ .

*Proof.* It follows from  $X \setminus \emptyset = \emptyset$ ,  $X \setminus X = \emptyset$  and  $\bigcap_{\lambda \in \Lambda} (X \setminus U_\lambda) = X \setminus (\bigcup_{\lambda \in \Lambda} U_\lambda)$ .  $\square$

**Theorem 2.13.** The Zariski topology on  $\text{Spec}(R) = X$  is a topology.

*Proof.* Note  $\mathcal{Z} = \{\text{Spec}(R) \setminus V(\mathfrak{a}) \mid \mathfrak{a} \leq R\}$ . Let  $\mathcal{V} = \{X \setminus Z \mid Z \in \mathcal{Z}\} = \{V(\mathfrak{a}) \mid \mathfrak{a} \leq R\}$ .

- (a)  $X = V(0) \in \mathcal{V}$  and  $\emptyset = V(1) \in \mathcal{V}$ ,
- (b) For  $\mathfrak{a}_\lambda \leq \mathfrak{a}$  for any  $\lambda \in \Lambda$ ,  $\bigcap_{\lambda \in \Lambda} V(\mathfrak{a}_\lambda) = V(\sum_{\lambda \in \Lambda} \mathfrak{a}_\lambda) \in \mathcal{V}$  by Fact 1.36.
- (c) For  $n \geq 1$  and  $\mathfrak{a}_1, \dots, \mathfrak{a}_n \leq R$ ,  $\bigcup_{i=1}^n V(\mathfrak{a}_i) = V(\bigcap_{i=1}^n \mathfrak{a}_i) \in \mathcal{V}$  by Proposition 1.39(a).  $\square$

So by Proposition 2.12, the Zariski topology on  $\text{Spec}(R) = X$  is a topology.

**Definition 2.14.** A *basis* for the topology  $\mathcal{T}$  on a topological space  $X$  is a subset  $\mathcal{B} \subseteq \mathcal{T}$  such that for any open set  $U \subseteq X$  and any  $u \in U$ , there exists  $B \subseteq \mathcal{B}$  such that  $u \in B \subseteq U$ .

**Example 2.15.** In the Euclidean topology,  $\mathcal{B} = \{B_\epsilon(x) \mid x \in \mathbb{R}^n, \epsilon > 0\}$  is a basis.

**Theorem 2.16.** In  $X = \text{Spec}(R)$ ,  $\mathcal{B} = \{X_f \mid f \in R\}$  is a basis for the Zariski topology.

*Proof.* It suffices to show  $X \setminus V(S) = \bigcup_{s \in S} X_s$  for  $S \subseteq R$ . Note  $\mathfrak{p} \in X \setminus V(S)$  if and only if  $S \not\subseteq \mathfrak{p}$  if and only if there exists  $s \in S$  such that  $s \notin \mathfrak{p}$  if and only if there exists  $s \in S$  such that  $\mathfrak{p} \in X_s$  if and only if  $\mathfrak{p} \in \bigcup_{s \in S} X_s$ .  $\square$

**Proposition 2.17.** If  $R$  is noetherian, then for any open subset  $U \subseteq X = \text{Spec}(R)$ , there exist  $s_1, \dots, s_n \in R$  such that  $U = X_{s_1} \cup \dots \cup X_{s_n}$ , i.e., open sets are the finite union of the basis open sets.

*Proof.* Write  $U = X \setminus V(\mathfrak{a})$  for some  $\mathfrak{a} \leq R$ . Since  $R$  is noetherian,  $\mathfrak{a} = \langle s_1, \dots, s_n \rangle$  for some  $n \geq 1$  and  $s_1, \dots, s_n \in \mathfrak{a}$ . Then  $U = X \setminus V(\langle s_1, \dots, s_n \rangle) = X \setminus V(s_1, \dots, s_n) = \bigcup_{i=1}^n X_{s_i}$  by the proof of Theorem 2.16.  $\square$

**Definition 2.18.** A topological space  $X$  is *quasi-compact* if “every open cover of  $X$  has a finite sub-cover”, i.e., for any  $\{U_\lambda\}_{\lambda \in \Lambda} \subseteq \mathcal{T}$ , if  $X = \bigcup_{\lambda \in \Lambda} U_\lambda$ , then there exist  $n \geq 1$  and  $\lambda_1, \dots, \lambda_n \in \Lambda$  such that  $X = \bigcup_{i=1}^n U_{\lambda_i}$ .

**Theorem 2.19.**  $\text{Spec}(R)$  is quasi-compact.

*Proof.* Since each open set  $U_\lambda$  can be written as a union of  $X_f$ ’s with  $f \in R$ , without loss of generality, assume  $X = \bigcup_{\lambda \in \Lambda} X_{f_\lambda} = X \setminus V(\bigcup_{\lambda \in \Lambda} f_\lambda)$  by the proof of Theorem 2.16. Then  $\emptyset = V(\bigcup_{\lambda \in \Lambda} f_\lambda) = V(\langle \bigcup_{\lambda \in \Lambda} f_\lambda \rangle)$ . So by Proposition 1.32(b),  $\langle \bigcup_{\lambda \in \Lambda} f_\lambda \rangle = R \ni 1$ . Then  $1 = g_{\lambda_1} f_{\lambda_1} + \dots + g_{\lambda_n} f_{\lambda_n}$  for some  $n \geq 1$ ,  $\lambda_1, \dots, \lambda_n \in \Lambda$  and  $g_{\lambda_1}, \dots, g_{\lambda_n} \in R$ . So  $\langle f_{\lambda_1}, \dots, f_{\lambda_n} \rangle = R$ . Then  $V(f_{\lambda_1}, \dots, f_{\lambda_n}) = V(\langle f_{\lambda_1}, \dots, f_{\lambda_n} \rangle) = V(R) = \emptyset$ . Thus,  $X = X \setminus \emptyset = X \setminus V(f_{\lambda_1}, \dots, f_{\lambda_n}) = X_{f_{\lambda_1}} \cup \dots \cup X_{f_{\lambda_n}}$ .  $\square$

**Question.** What do the  $X_f$  look like? Answer:  $\text{Spec}(R)$ .

**Construction** (Classical algebraic geometry). Geometry: Let  $k$  be a field, usually  $k = \mathbb{R}$  or  $\mathbb{C}$ . Define *d-dimensional affine space*:  $\mathbb{A}_k^d = \mathbb{A}^d = k^d$ .

Let  $\underline{a} = (a_1, \dots, a_d) \in \mathbb{A}^d$  and  $S \subseteq k[\underline{X}] = k[X_1, \dots, X_d]$ . Define

$$V(S) := \{\underline{a} \in \mathbb{A}^d \mid f(\underline{a}) = 0, \forall f \in S\} =: \text{“zero locus of } S\text{”} \subseteq \mathbb{A}^d.$$

e.g.,  $V(X^2 + Y^2 + Z^2 - 1) = \text{“unit sphere”} \subseteq \mathbb{A}_{\mathbb{R}}^3 = \mathbb{R}^3$ .

Zariski topology on  $\mathbb{A}^d$ . Closed sets:  $V(S) = V(\langle S \rangle) \subseteq \mathbb{A}^d$  with  $S \subseteq k[\underline{X}]$ . Open sets:  $\mathbb{A}^d \setminus V(S)$  with  $S \subseteq k[\underline{X}]$ . Basic open sets:  $\mathbb{A}^d \setminus V(f)$  with  $f \in k[\underline{X}]$ .

Let  $T \subseteq k[\underline{X}]$  be fixed. Zariski topology on  $V(T)$ . Closed sets:  $V(S) \cap V(T)$  with  $S \subseteq k[\underline{X}]$ . Open sets:  $\underbrace{(\mathbb{A}^d \setminus V(S)) \cap V(T)}_{\text{open in } \mathbb{A}^d}$  with  $S \subseteq k[\underline{X}]$ . Basic open sets:  $(\mathbb{A}^d \setminus V(f)) \cap V(T)$  with  $f \in k[\underline{X}]$ .

We have

$$\begin{aligned} \varphi : \mathbb{A}^d &\hookrightarrow \text{m-Spec}(k[\underline{X}]) \subseteq \text{Spec}(k[\underline{X}]) \\ \underline{a} &\mapsto (X_1 - a_1, \dots, X_d - a_d) = \text{Ker}(\Phi_{\underline{a}}), \end{aligned}$$

where  $\Phi_{\underline{a}} : k[\underline{X}] \rightarrow k$  is given by  $f \mapsto f(\underline{a})$ .

Hilbert’s Nullstellensatz: If  $k = \bar{k}$ , then  $V(\mathfrak{b}) \neq \emptyset$  for  $\mathfrak{b} \leq k[\underline{X}]$ . Let  $\mathfrak{m} \in \text{m-Spec}(k[\underline{X}])$ . Then  $V(\mathfrak{m}) \neq \emptyset$  and so there exists  $\underline{a} \in V(\mathfrak{m})$  such that  $f(\underline{a}) = 0$  for all  $f \in \mathfrak{m} \subseteq k[\underline{X}]$ . Hence  $\mathfrak{m} \subseteq \text{Ker}(\Phi_{\underline{a}}) = (X_1 - a_1, \dots, X_d - a_d) \leq k[\underline{X}]$ . Also, since  $\mathfrak{m} \leq k[\underline{X}]$  is maximal,  $\mathfrak{m} = (X_1 - a_1, \dots, X_d - a_d) = \varphi(\underline{a})$ . So  $\varphi$  is onto. Thus,  $\varphi : \mathbb{A}^d \xrightarrow{\cong} \text{m-Spec}(k[\underline{X}])$ .

Grothendieck: there exists more geometric data in  $\text{Spec}(k[\underline{X}])$ .

Let  $V = V(T) = V(\mathfrak{b})$ , where  $\mathfrak{b} = \langle T \rangle \leq k[\underline{X}]$ . Then

$$\text{rad}(\mathfrak{b}) \leq I(V) := \{f \in k[\underline{X}] \mid f(\underline{a}) = 0, \forall \underline{a} \in V\} = \text{“vanishing ideal of } V\text{”} \leq k[\underline{X}].$$

Hilbert’s Nullstellensatz: If  $k = \bar{k}$ , then since  $\underline{a} \in V(\mathfrak{b})$  if and only if  $I(\underline{a}) \supseteq I(V(\mathfrak{b})) = \text{rad}(\mathfrak{b}) \supseteq \mathfrak{b}$ ,

$$\begin{aligned} \text{rad}(\mathfrak{b}) &= I(V) = I(V(\mathfrak{b})) = I\left(\bigcup_{\underline{a} \in V(\mathfrak{b})} \underline{a}\right) = \bigcap_{\underline{a} \in V(\mathfrak{b})} I(\underline{a}) = \bigcap_{\underline{a} \in V(\mathfrak{b})} \text{Ker}(\Phi_{\underline{a}}) \\ &= \bigcap_{\underline{a} \in V(\mathfrak{b})} (X_1 - a_1, \dots, X_d - a_d) = \bigcap_{\mathfrak{b} \subseteq \mathfrak{m} \in \mathfrak{m}\text{-Spec}(k[\underline{X}])} \mathfrak{m}. \end{aligned}$$

*Coordinate ring of  $V$ :*  $\Gamma(V) = k[\underline{X}]/I(V)$ , also known as *ring of regular functions on  $V$* .

Let  $\mathcal{F}(V, k)$  be the set of all functions from  $V$  to  $k$ . Define

$$\begin{aligned} \phi : \Gamma(V) &\rightarrow \mathcal{F}(V, k) \\ \bar{f} &\mapsto f \end{aligned}$$

Let  $\bar{f} = \bar{g} \in \Gamma(V)$ . Then  $f - g \in I(V)$ . So for all  $\underline{a} \in V$ , we have  $f(\underline{a}) - g(\underline{a}) = (f - g)(\underline{a}) = 0$ , i.e.,  $f(\underline{a}) = g(\underline{a})$ . Hence  $\phi$  is well-defined. It is straightforward to show  $\phi$  is a ring monomorphism. Define  $k[V]$  to be the set of *restrictions* of at least one polynomial  $f|_V : V \rightarrow k$ , where  $f \in k[\underline{X}]$ . Note  $\text{Im}(\phi) = k[V]$ . So  $\Gamma(V) \cong k[V]$ . Thus, it is very common to write  $k[V] = \Gamma(V)$ .

Let  $x := \bar{X} \in \Gamma(V)$ . Let  $x_i := \bar{X}_i \in \Gamma(V)$  be the  $i^{\text{th}}$  coordinate function with  $x_i(\underline{a}) = a_i$  for  $i = 1, \dots, d$ . Note  $f(X_1, \dots, X_n) = f(x_1, \dots, x_n)$  for  $f \in k[\underline{X}]$ . So  $x_i$ ’s generate  $\Gamma(V)$  as a  $k$ -algebra, i.e., every element of  $\Gamma(V)$  can be written as a polynomial in the  $x_i$ ’s with coefficients from  $k$ . Hence we denote  $k[V] = k[\underline{x}] = k[x_1, \dots, x_d]$ . Unlike in  $k[\underline{X}]$ , there may be nontrivial relations between the  $x_i$ ’s in  $k[\underline{x}]$ . For example, in  $\mathbb{Q}[x] = \mathbb{Q}[X]/\langle X^2 - 2 \rangle$ , we have  $0 = \overline{X^2 - 2} = x^2 - 2$  in  $\mathbb{Q}[x]$ , i.e.,  $x^2 = 2$  in  $\mathbb{Q}[x]$ .

We have

$$\begin{aligned} \bar{\varphi} : V &\hookrightarrow \mathfrak{m}\text{-Spec}(k[V]) \subseteq \text{Spec}(k[V]) \\ \underline{a} &\mapsto \frac{(X_1 - a_1, \dots, X_d - a_d)}{I(V)} = (x_1 - a_1, \dots, x_d - a_d). \end{aligned}$$

Hilbert’s Nullstellensatz: If  $k = \bar{k}$ , then similarly,  $\bar{\varphi}$  is onto.

Grothendieck: there exists more geometric data in  $\text{Spec}(k[V])$ .

Set up:  $R \ni f$ ,  $X = \text{Spec}(R) \supseteq X_f = X \setminus V(f) = \{\mathfrak{p} \in \text{Spec}(R) \mid f \notin \mathfrak{p}\}$ .

**Recall.** Let  $S = \{1, f, f^2, \dots\}$ . We have  $R_f = S^{-1}R = \{\frac{r}{f^n} \mid r \in R, n \geq 0\} = R[1/f]$ .

**Proposition 2.20.** Define  $\varphi : R \rightarrow R_f$  by  $\varphi(g) = \frac{g}{1}$  and  $\varphi^* : \text{Spec}(R_f) \rightarrow \text{Spec}(R) = X$  by  $\varphi^*(\mathfrak{q}) = \varphi^{-1}(\mathfrak{q})$ .

(a)  $\varphi^*(\mathfrak{q}) \in X_f$  for  $\mathfrak{q} \in \text{Spec}(R_f)$ .

(b) Restrict codomain, the induced map  $\varphi_f^* : \text{Spec}(R_f) \rightarrow X_f$  is 1-1 and onto.

Slogan:  $\text{Spec}(R_f) = X_f$  “open affine subsets”.

*Proof.* (a) Let  $\mathfrak{q} \in \text{Spec}(R_f)$ . Then  $\varphi^*(\mathfrak{q}) = \varphi^{-1}(\mathfrak{q}) \in \text{Spec}(R)$  by Fact 1.16. Note  $f \notin \varphi^*(\mathfrak{q}) = \varphi^{-1}(\mathfrak{q})$ , otherwise,  $R_f^\times \ni \frac{f}{1} = \varphi(f) \in \varphi(\varphi^{-1}(\mathfrak{q})) \subseteq \mathfrak{q} \in \text{Spec}(R_f)$ , a contradiction.

(b) Let  $\mathfrak{p} \in X_f$ , then  $\mathfrak{p} \in \text{Spec}(R)$  and so

$$\begin{aligned} \mathfrak{p}_f &:= \mathfrak{p}R_f = \left\{ \sum_i^{\text{finite}} \varphi(p_i) \cdot y_i \mid p_i \in \mathfrak{p}, y_i \in R_f, \forall i \right\} = \left\{ \sum_i^{\text{finite}} \frac{p_i}{1} \cdot \frac{r_i}{f^{n_i}} \mid p_i \in \mathfrak{p}, r_i \in R, n_i \geq 0, \forall i \right\} \\ &= \left\{ \frac{\sum_{i=1}^{\text{finite}} p_i \cdot r_i \cdot f^{\sum_{j \neq i}^{\text{finite}} n_j}}{f^{\sum_{i=1}^{\text{finite}} n_i}} \mid p_i \in \mathfrak{p}, r_i \in R, n_i \geq 0, \forall i \right\} = \left\{ \frac{p}{f^n} \mid p \in \mathfrak{p}, n \geq 0 \right\} \leq R_f. \end{aligned}$$

Since  $f^n \notin \mathfrak{p}$  for  $n \geq 0$ ,  $\frac{1}{f} \notin \mathfrak{p}_f$ . So  $\mathfrak{p}_f \leq R_f$ . Let  $\frac{x}{f^n}, \frac{y}{f^m} \in R_f$  with  $x, y \in R$  and  $n, m \geq 0$  such that  $\frac{xy}{f^{n+m}} = \frac{x}{f^n} \cdot \frac{y}{f^m} \in \mathfrak{p}_f$  and so  $xy \in \mathfrak{p}$ . Since  $\mathfrak{p} \in \text{Spec}(R)$ ,  $x \in \mathfrak{p}$  or  $y \in \mathfrak{p}$ . So  $\frac{x}{f^n} \in \mathfrak{p}_f$  or  $\frac{y}{f^m} \in \mathfrak{p}_f$ . Hence  $\mathfrak{p}_f \in \text{Spec}(R_f)$ .

On the other hand, by (a),  $\varphi^*(\mathfrak{q}) \in X_f$  for  $\mathfrak{q} \in \text{Spec}(R_f)$ . Thus, we have the 1-1 correspondence:

$$\begin{aligned} X_f &= \{\mathfrak{p} \in \text{Spec}(R) \mid f \notin \mathfrak{p}\} \rightleftharpoons \text{Spec}(R_f) \\ \mathfrak{p} &\mapsto \mathfrak{p}_f \\ \varphi^*(\mathfrak{q}) &= \varphi^{-1}(\mathfrak{q}) = “\mathfrak{q} \cap R” \leftarrow \mathfrak{q}. \end{aligned}$$

□

## Subspaces

**Proposition 2.21.** Let  $X$  be a topological space with a topology  $\mathcal{T}$  and  $Y \subseteq X$ . Define  $\mathcal{T}_Y = \{U \cap Y \mid U \in \mathcal{T}\}$ . Then  $\mathcal{T}_Y$  is a topology on  $Y$ , called the *subspace topology*.

*Proof.*  $Y = X \cap Y \in \mathcal{T}_Y$  since  $X \in \mathcal{T}$ .  $\emptyset = \emptyset \cap Y \in \mathcal{T}_Y$  since  $\emptyset \in \mathcal{T}$ . Let  $\{U_\lambda \cap Y \mid U_\lambda \in \mathcal{T}\}_{\lambda \in \Lambda} \subseteq \mathcal{T}_Y$ . Since  $\mathcal{T}$  is a topology on  $X$ ,  $\bigcup_{\lambda \in \Lambda} U_\lambda \in \mathcal{T}$ . So  $\bigcup_{\lambda \in \Lambda} (U_\lambda \cap Y) = (\bigcup_{\lambda \in \Lambda} U_\lambda) \cap Y \in \mathcal{T}_Y$ . Let  $U_1 \cap Y, \dots, U_n \cap Y \in \mathcal{T}_Y$ . Similarly, we have  $\bigcap_{i=1}^n (U_i \cap Y) \in \mathcal{T}_Y$ . □

**Remark.** The closed subsets of  $Y$  are  $\{V \cap Y \mid V \subseteq X \text{ is closed}\}$  since

$$\begin{aligned} \{Y \setminus (U \cap Y) \mid U \in \mathcal{T}\} &= \{Y \cap (U \cap Y)^c \mid U \in \mathcal{T}\} = \{(U^c \cup Y^c) \cap Y \mid U \in \mathcal{T}\} \\ &= \{(U^c \cap Y) \cup (Y^c \cap Y) \mid U \in \mathcal{T}\} = \{U^c \cap Y \mid U \in \mathcal{T}\}. \end{aligned}$$

**Proposition 2.22.** If  $\mathcal{B}$  is a basis for  $\mathcal{T}$ , then  $\mathcal{B}_Y = \{\mathcal{B} \cap Y \mid \mathcal{B} \in \mathcal{B}\}$  is a basis for  $\mathcal{T}_Y$ .

*Proof.* Let  $U \cap Y \in \mathcal{T}_Y$  with  $U \in \mathcal{T}$ . Since  $\mathcal{B}$  is a basis of  $\mathcal{T}$ ,  $U = \bigcup_{\lambda \in \Lambda_U} B_\lambda$  for some  $\{B_\lambda\}_{\lambda \in \Lambda_U} \subseteq \mathcal{B}$ . So  $U \cap Y = \bigcup_{\lambda \in \Lambda_U} (B_\lambda \cap Y)$ . □

**Corollary 2.23.** Let  $f \in R$ . Subspace topology on  $X_f \subseteq X = \text{Spec}(R)$  has

- (a) closed sets:  $V(\mathfrak{a}) \cap X_f = \{\mathfrak{p} \in \text{Spec}(R) \mid \mathfrak{a} \subseteq \mathfrak{p} \not\ni f\}$ , where  $\mathfrak{a} \leq R$ ;
- (b) open sets:  $(X \setminus V(\mathfrak{a})) \cap X_f = \{\mathfrak{p} \in \text{Spec}(R) \mid \mathfrak{a} \not\subseteq \mathfrak{p} \not\ni f\}$ , where  $\mathfrak{a} \leq R$ ;
- (c) basic open sets:  $X_g \cap X_f = X_{fg}$ , where  $g \in R$ .

**Remark.** Let  $\mathfrak{a} \leq R$ . Subspace topology on  $V(\mathfrak{a}) \subseteq X = \text{Spec}(R)$  has

- (a) closed sets:  $V(\mathfrak{b}) \cap V(\mathfrak{a}) = \{\mathfrak{p} \in \text{Spec}(R) \mid \mathfrak{b} + \mathfrak{a} \subseteq \mathfrak{p}\}$ , where  $\mathfrak{b} \leq R$ ;
- (b) open sets:  $(X \setminus V(\mathfrak{b})) \cap V(\mathfrak{a}) = \{\mathfrak{p} \in \text{Spec}(R) \mid \mathfrak{b} \not\subseteq \mathfrak{p} \supseteq \mathfrak{a}\}$ , where  $\mathfrak{b} \leq R$ ;
- (c) basic open sets:  $X_g \cap V(\mathfrak{a})$ , where  $g \in R$ .

**Proposition 2.24.** Let  $\mathfrak{a} \leq R$ ,  $\varphi : R \rightarrow R_f$  and  $\varphi_f^* : \text{Spec}(R_f) \rightarrow \text{Spec}(R)$  as in Proposition 2.20.

- (a)  $(\varphi_f^*)^{-1}(V(\mathfrak{a}) \cap X_f) = V(\mathfrak{a}_f)$ .
- (b)  $(\varphi_f^*)^{-1}((X \setminus V(\mathfrak{a})) \cap X_f) = \text{Spec}(R_f) \setminus V(\mathfrak{a}_f)$ .
- (c)  $(\varphi_f^*)^{-1}(X_g \cap X_f) = Z_{g|1}$  for  $g \in R$ .

*Proof.* (a) Let  $\mathfrak{p} \in \text{Spec}(R_f)$ .  $\mathfrak{p} \in (\varphi_f^*)^{-1}(V(\mathfrak{a}) \cap X_f)$  if and only if  $\varphi^{-1}(\mathfrak{p}) = \varphi_f^*(\mathfrak{p}) \in V(\mathfrak{a}) \cap X_f$  if and only if  $\varphi^{-1}(\mathfrak{p}) \in V(\mathfrak{a})$  if and only if  $\mathfrak{a} \subseteq \varphi^{-1}(\mathfrak{p})$  if and only if  $\mathfrak{a}_f = \mathfrak{a}R_f \subseteq \varphi^{-1}(\mathfrak{p})R_f = \mathfrak{p}^\dagger$  if and only if  $\mathfrak{p} \in V(\mathfrak{a}_f)$ .

(b) Let  $\mathfrak{p} \in \text{Spec}(R_f)$ .  $\mathfrak{p} \in (\varphi_f^*)^{-1}((X \setminus V(\mathfrak{a})) \cap X_f)$  if and only if  $\varphi^{-1}(\mathfrak{p}) = \varphi_f^*(\mathfrak{p}) \in (X \setminus V(\mathfrak{a})) \cap X_f$  if and only if  $\varphi^{-1}(\mathfrak{p}) \in X \setminus V(\mathfrak{a})$  if and only if  $\mathfrak{p} \in \text{Spec}(R_f) \setminus V(\mathfrak{a}_f)$  by the proof of (a).

(c) Method 1. By (a), we have  $(\varphi_f^*)^{-1}(X_g \cap X_f) = (\varphi_f^*)^{-1}((X \setminus V(g)) \cap X_f) = \text{Spec}(R_f) \setminus V((g)_f) = \{\mathfrak{p}_f \mid \mathfrak{p} \in \text{Spec}(R), \mathfrak{p}_f \not\supseteq (g)_f\} = \{\mathfrak{p}_f \mid g \notin \mathfrak{p} \in \text{Spec}(R)\} = \{\mathfrak{p}_f \mid \mathfrak{p} \in X_g\}$ .

Method 2. Let  $\mathfrak{p} \in \text{Spec}(R_f)$ . Then  $\mathfrak{p} \in (\varphi_f^*)^{-1}(X_g \cap X_f)$  if and only if  $\varphi_f^*(\mathfrak{p}) \in X_g \cap X_f$  if and only if  $\varphi_f^*(\mathfrak{p}) \in X_g$  if and only if  $\mathfrak{p} \in \{\mathfrak{q}_f \mid \mathfrak{q} \in X_g\}$ .  $\square$

## Continuous Functions and Homeomorphisms

Let  $X \neq \emptyset$  be a topological space.

**Definition 2.25.** Let  $f : X \rightarrow Y$  be a function between topological spaces. Then  $f$  is *continuous* if  $f^{-1}(U) \in \mathcal{T}_X$  for  $U \in \mathcal{T}_Y$ . “Inverse image of arbitrary open set in  $Y$  is open in  $X$ ”.

**Remark.** Let  $Y \subseteq X$ . The subspace topology  $\mathcal{T}_Y$  is the smallest topology on  $Y$  such that  $Y \xhookrightarrow{\subseteq} X$  is continuous.

**Fact 2.26.** To show  $f$  is continuous, it is equivalent to showing  $f^{-1}(\text{arbitrary closed sets of } Y)$  is closed in  $X$ , equivalent to showing  $f^{-1}(\text{basic open subsets of } Y)$  is open in  $X$ .

**Theorem 2.27.** Let  $\varphi : R \rightarrow S$  be a ring homomorphism, then  $\varphi^* : \text{Spec}(S) \rightarrow \text{Spec}(R)$  is continuous.

*Proof.* Let  $\mathfrak{a} \leq R$  and  $\mathfrak{p} \in \text{Spec}(S)$ . Then  $\mathfrak{p} \in (\varphi^*)^{-1}(V(\mathfrak{a}))$  if and only if  $\varphi^*(\mathfrak{p}) \in V(\mathfrak{a})$  if and only if  $\varphi^{-1}(\mathfrak{p}) = \varphi^*(\mathfrak{p}) \supseteq \mathfrak{a}$  if and only if  $\mathfrak{p} \supseteq \varphi(\varphi^{-1}(\mathfrak{p})) \supseteq \varphi(\mathfrak{a})$  if and only if  $\mathfrak{p} \in V(\mathfrak{a}S)$ .  $\square$

<sup>†</sup>Method 1: Let  $\varphi_f^*(\mathfrak{p}) = \varphi^{-1}(\mathfrak{p}) =: \mathfrak{q} \in X_f$ . By the proof of Proposition 2.20(a),  $\varphi_f^*(\mathfrak{q}_f) = \mathfrak{q}$ . Also, since  $\varphi_f^*$  is 1-1,  $\varphi^{-1}(\mathfrak{p})R_f = \mathfrak{q}R_f = \mathfrak{q}_f = \mathfrak{p}$ .

Method 2: Claim.  $\varphi^{-1}(I)R_f = I$  for  $I \leq R_f$ . “ $\subseteq$ ”. By 1.63(a). “ $\supseteq$ ”. Let  $i \in I$ . Then  $i = \frac{r}{f^n} \in I$  for some  $r \in R$  and  $n \geq 0$ . So  $\varphi(r) = \frac{r}{1} = \frac{f^n}{1} \cdot \frac{r}{f^n} \in I$ . Then  $r \in \varphi^{-1}(I)$ . So  $i = \frac{r}{f^n} = \varphi(r) \cdot \frac{1}{f^n} \in \varphi^{-1}(I)R_f$ .

**Theorem 2.28.** Let  $f \in R$ ,  $\varphi : R \rightarrow R_f$  and  $\varphi^* : \text{Spec}(R_f) \rightarrow \text{Spec}(R)$ . Then  $\varphi^*(\text{Spec}(R_f)) = X_f$  “principal open set”. Restrict codomain,  $\varphi_f^* : \text{Spec}(R_f) \rightarrow X_f$  is 1-1 and onto. Moreover, give the codomain subspace topology,  $\varphi_f^*$  and  $(\varphi_f^*)^{-1}$  are continuous. “homeomorphism”.

*Proof.* By Proposition 2.24, we have  $\varphi_f^*$  is continuous or by Theorem 2.27 and Lemma 2.30.

Let  $I \leq R_f$ . Then  $I = \varphi^{-1}(I)R_f$  by the proof of Proposition 2.24(a). Since  $\varphi_f^*$  is a bijection,  $((\varphi_f^*)^{-1})^{-1}(V(I)) = \varphi_f^*(V(I)) = \varphi_f^*(V(\varphi^{-1}(I)R_f)) = V(\varphi^{-1}(I)) \cap X_f$  by Proposition 2.24(a).  $\square$

**Example.** Let  $k$  be a field and  $R = k[[X]]$ . Claim.  $\text{Spec}(R) = \{0, \langle X \rangle\}$ . Let  $0 \neq f \in [[X]]$ . Then  $f = \sum_{i=0}^{\infty} a_i X^i$  for some  $a_i \in k$  for  $i \geq 0$ . Let  $m = \min\{i \geq 0 \mid a_i \neq 0\}$ . Then  $f(X) = X^m(\sum_{i=0}^{\infty} a_{m+i} X^i)$ . Since  $a_m \in k^\times$ , we have  $\sum_{i=0}^{\infty} a_{m+i} X^i \in R^\times$ . So every  $0 \neq f \in R$  is of the form  $uX^l$  for some  $l \geq 0$  and  $u \in R^\times$ . Hence if  $0 \neq I \leq R$ ,  $I = \langle X^m \rangle$ , where  $m = \min\{j \geq 0 \mid X^j \in I\}$ . Thus,  $\mathfrak{p} = \langle X \rangle$  for  $0 \neq \mathfrak{p} \in \text{Spec}(R)$ .

Define  $\varphi : R \rightarrow S = k \times Q(R)$  by  $\sum_{i=1}^{\text{finite}} a_i X^i \mapsto (a_0, \frac{\sum_{i=1}^{\text{finite}} a_i X^i}{1})$ . Note  $\varphi$  is a ring homomorphism and  $\text{Spec}(S) = \{k \times 0, 0 \times Q(R)\}$ . So the continuous function  $\varphi^* : \text{Spec}(S) \rightarrow \text{Spec}(R)$  sending  $k \times 0$  to  $0$  and  $0 \times Q(R)$  to  $\langle X \rangle$  is 1-1 and onto.

Closed sets of  $\text{Spec}(S)$  are  $V(1, 1) = \emptyset$ ,  $V(0, 0) = \text{Spec}(S)$ ,  $V(0, 1) = \{0 \times Q(R)\}$  and  $V(1, 0) = \{k \times 0\}$ . Closed sets of  $\text{Spec}(R)$  are  $V(1) = \emptyset$ ,  $V(0) = \text{Spec}(R)$  and  $V(X) = \{\langle X \rangle\}$ . Since  $\varphi^*$  is a bijection, we have  $((\varphi^*)^{-1})^{-1}(\{k \times 0\}) = \varphi^*(\{k \times 0\}) = \{0\}$  is not closed in  $\text{Spec}(R)$ . So  $(\varphi^*)^{-1}$  is not continuous.

**Corollary 2.29.**  $X_f$  is quasi-compact.

*Proof.* It follows from  $X_f$  is homeomorphic to  $\text{Spec}(R_f)$  and  $\text{Spec}(R_f)$  is quasi-compact.  $\square$

**Example.**  $U \subseteq \text{Spec}(R) = X$  may not be quasi-compact. Let  $R = k[X_1, X_2, X_3, \dots]$ . Let  $U = X \setminus V(X_1, X_2, X_3, \dots) = X \setminus \bigcap_{i=1}^{\infty} V(X_i) = \bigcup_{i=1}^{\infty} (X \setminus V(X_i))$  by Fact 1.36(a). Let  $n \geq 1$ . Claim.  $V(X_1, X_2, X_3, \dots) \neq V(X_1, X_2, \dots, X_n)$ . “ $\subseteq$ ”. It is straightforward. “ $\not\subseteq$ ”. Let  $\mathfrak{p} = \langle X_1, \dots, X_n \rangle \in V(X_1, X_2, \dots, X_n)$ . Then  $\mathfrak{p} \notin V(X_1, X_2, \dots)$  since  $\langle X_1, X_2, \dots \rangle \ni X_{n+1} \notin \mathfrak{p}$ . So  $U = X \setminus V(X_1, X_2, X_3, \dots) \neq X \setminus V(X_1, \dots, X_n) = X \setminus \bigcap_{i=1}^n V(X_i) = \bigcup_{i=1}^n (X \setminus V(X_i))$  for  $n \geq 1$ .

**Fact.** If  $R$  is noetherian and  $U \subseteq X = \text{Spec}(R)$  is open, then  $U$  is quasi-compact.

*Proof.* Let  $U = \bigcup_{\lambda \in \Lambda} U_\lambda$  be an open cover with  $U_\lambda$  open in  $X$  for  $\lambda \in \Lambda$ . Use the fact that  $X_f$ ’s form a basis to assume without loss of generality  $U_\lambda = X_{f_\lambda}$  for some  $f_\lambda \in R$  for  $\lambda \in \Lambda$ . Then  $U = \bigcup_{\lambda \in \Lambda} X_{f_\lambda} = \bigcup_{\lambda \in \Lambda} (X \setminus V(f_\lambda)) = X \setminus V(\langle f_\lambda \mid \lambda \in \Lambda \rangle)$ . Since  $R$  is noetherian, there exist  $f_{\lambda_1}, \dots, f_{\lambda_n} \in R$  such that  $\langle f_\lambda \mid \lambda \in \Lambda \rangle = \langle f_{\lambda_1}, \dots, f_{\lambda_n} \rangle$ . So  $U = X \setminus V(\langle f_{\lambda_1}, \dots, f_{\lambda_n} \rangle) = \bigcup_{i=1}^n X_{f_{\lambda_i}}$ .  $\square$

**Lemma 2.30.** Let  $f : X \rightarrow Y$  be a continuous function between two topological spaces. If  $f(X) \subseteq Z \subseteq Y$ , then consider the natural map  $f_Z : X \rightarrow Z$  and give  $Z$  the subspace topology, we have  $f_Z$  is continuous.

*Proof.* Let  $U \subseteq Z$  be open. Since  $Z$  has the subspace topology,  $U = Z \cap \tilde{U}$  for some  $\tilde{U} \subseteq Y$  open. Since  $f(X) \subseteq Z$ ,  $f_Z^{-1}(U) = f^{-1}(Z \cap \tilde{U}) = f^{-1}(Z) \cap f^{-1}(\tilde{U}) = f^{-1}(\tilde{U})$  is open in  $X$  since  $f$  is continuous.  $\square$

**Theorem 2.31.** Let  $\mathfrak{b} \leq R$ ,  $\pi : R \rightarrow R/\mathfrak{b}$  be the natural surjection and consider  $\pi^* : \text{Spec}(R/\mathfrak{b}) \rightarrow \text{Spec}(R)$ .

(a)  $\pi^*(\text{Spec}(R/\mathfrak{b})) = V(\mathfrak{b})$ .

(b) Give the codomain subspace topology and restrict the codomain, then  $\pi_{\mathfrak{b}}^* : \text{Spec}(R/\mathfrak{b}) \rightarrow V(\mathfrak{b})$  is continuous, 1-1 and onto, and  $(\pi_{\mathfrak{b}}^*)^{-1}$  is continuous. “homeomorphism”.

*Proof.* By prime correspondence,

$$\begin{aligned} \text{Spec}(R/\mathfrak{b}) &\xrightarrow{\sim} V(\mathfrak{b}) \\ \mathfrak{p}/\mathfrak{b} &\leftrightarrow \mathfrak{p} \supseteq \mathfrak{b} \\ \mathfrak{p} &\mapsto \pi^{-1}(\mathfrak{p}) = \pi^*(\mathfrak{p}). \end{aligned}$$

So  $\pi^*(\text{Spec}(R/\mathfrak{b})) = V(\mathfrak{b})$ , and  $\pi_{\mathfrak{b}}^*$  is 1-1 and onto. By Theorem 2.27 and Lemma 2.30,  $\pi_{\mathfrak{b}}^*$  is continuous. Let  $\mathfrak{b} \subseteq \mathfrak{a} \leq R$ . Then by prime correspondence,  $((\pi_{\mathfrak{b}}^*)^{-1})^{-1}(V(\mathfrak{a}/\mathfrak{b})) = \pi_{\mathfrak{b}}^*(V(\mathfrak{a}/\mathfrak{b})) = V(\mathfrak{a}) \cap V(\mathfrak{b}) = V(\mathfrak{a})$ . So  $(\pi_{\mathfrak{b}}^*)^{-1}$  is continuous.  $\square$

**Corollary 2.32.**  $V(\mathfrak{b})$  is quasi-compact for  $\mathfrak{b} \leq R$ .

**Definition 2.33.**  $X$  is *irreducible* if for  $\emptyset \neq U_1, U_2 \subseteq X$  open,  $U_1 \cap U_2 \neq \emptyset$ .

$X$  is *reducible* if it is not irreducible, i.e., if and only if there exist  $\emptyset \neq U_1, U_2 \subseteq X$  open such that  $U_1 \cap U_2 = \emptyset$ .

**Example 2.34.** If  $R$  is an integral domain, then  $X = \text{Spec}(R)$  is irreducible.

*Proof.* Let  $\emptyset \neq U \subseteq X$  be open. Then  $\emptyset \neq U = X \setminus V(\mathfrak{a})$  for some  $\mathfrak{a} \leq R$ . So  $V(\mathfrak{a}) \neq X = \text{Spec}(R)$ . Hence  $\mathfrak{a} \neq \langle 0 \rangle$  and so  $\langle 0 \rangle \notin V(\mathfrak{a})$ . Also, since  $R$  is an integral domain,  $\langle 0 \rangle \in X$ . So  $\langle 0 \rangle \in U$ .  $\square$

**Definition 2.33+.** A subset  $\emptyset \neq Y \subseteq X$  with subspace topology is an *irreducible subset* if it is irreducible as topological space. Equivalently,  $\emptyset \neq Y \subseteq X$  with subspace topology is *irreducible* if  $Y = V \cup W$  for  $V, W \subseteq Y$  closed, then  $Y = V$  or  $Y = W$ .

**Corollary 2.35.** If  $\mathfrak{q} \in \text{Spec}(R)$ , then  $V(\mathfrak{q}) \subseteq \text{Spec}(R)$  with subspace topology is irreducible.

*Proof.* Let  $\mathfrak{q} \in \text{Spec}(R)$ . Then  $R/\mathfrak{q}$  is an integral domain. So  $\text{Spec}(R/\mathfrak{q})$  is irreducible by Example 2.34. Since  $V(\mathfrak{q})$  is homeomorphic to  $\text{Spec}(R/\mathfrak{q})$  by Theorem 2.31, we have  $\emptyset \neq V(\mathfrak{q})$  is irreducible.  $\square$

**Definition 2.36.** Let  $Y \subseteq X$ . The *closure* of  $Y$  in  $X$  is

$$\bar{Y} = \bigcap_{\substack{Y \subseteq V \subseteq X \\ V \text{ closed}}} V.$$

**Fact 2.37.** If  $Y \subseteq X$ , then  $\bar{Y}$  is the (unique) smallest closed subset of  $X$  containing  $Y$ .

If  $V \subseteq X$  is closed, then  $\bar{Y} \subseteq V$  if and only if  $Y \subseteq V$ .

**Example.** In  $X = \text{Spec}(\mathbb{Z})$ , Zariski topology is almost the “cofinite topology”, open sets are  $X, \emptyset$  and  $\{X \setminus \{p_1\mathbb{Z}, \dots, p_n\mathbb{Z}\} \mid n \geq 1, 0 \neq p_i \text{ is prime, } \forall i = 1, \dots, n\}$ .

**Lemma 2.38.** The followings are equivalent.

(i)  $X$  is irreducible.

(ii) For  $V_1, V_2 \subsetneq X$  closed,  $V_1 \cup V_2 \subsetneq X$ .

(iii) For  $\emptyset \neq U \subseteq X$  open,  $\bar{U} = X$ .

“Non-empty open sets are dense”.

*Proof.* “(i) $\Leftrightarrow$ (ii)”. By Definition 2.33.

“(ii) $\Rightarrow$ (iii)”. Assume (b). Let  $\emptyset \neq U \subseteq X$  be open. Suppose  $V_1 := \bar{U} \neq X$ . Let  $V_2 := X \setminus U$ . Then  $V_1, V_2 \subseteq X$  are closed. So  $X = U \cup (X \setminus U) \subseteq \bar{U} \cup (X \setminus U) = V_1 \cup V_2 \subsetneq X$  by assumption, a contradiction.

“(iii) $\Rightarrow$ (i)”. By contrapositive. Assume  $X$  is reducible. Then there exist  $\emptyset \neq U_1, U_2 \subseteq X$  open such that  $U_1 \cap U_2 = \emptyset$ . So  $U_1 \subseteq X \setminus U_2 \subsetneq X$ . Also, since  $X \setminus U_2$  is closed,  $\bar{U}_1 \subseteq X \setminus U_2 \subsetneq X$   $\square$

**Definition 2.33++.**  $X$  is *irreducible* if and only if for  $V_1, V_2 \subsetneq X$  closed,  $V_1 \cup V_2 \neq X$ .

**Proposition 2.39.**  $X = \text{Spec}(R)$  is irreducible if and only if  $\text{Nil}(R) \in \text{Spec}(R)$ .

*Proof.* “ $\Leftarrow$ ”. Assume  $\text{Nil}(R) \in \text{Spec}(R)$ . By Proposition 1.32(c),  $V(\text{Nil}(R)) = \text{Spec}(R)$ . Then by Corollary 2.35,  $\text{Spec}(R) = V(\text{Nil}(R))$  is irreducible.

“ $\Rightarrow$ ”. Assume  $X = \text{Spec}(R)$  is irreducible. Since  $R \neq 0$ ,  $\text{Nil}(R) \neq R$  by Proposition 1.26(b). Let  $a, b \in R$  such that  $ab \in \text{Nil}(R)$ . Then  $V(a) \cup V(b) = V(ab) = \text{Spec}(R)$ . Since  $\text{Spec}(R)$  is irreducible,  $V(a) = \text{Spec}(R)$  or  $V(b) = \text{Spec}(R)$ . So  $a \in \text{Nil}(R)$  or  $b \in \text{Nil}(R)$ .  $\square$

**Proposition 2.40.** We have the following.

- (a) If  $Y \subseteq X$  is irreducible, then  $\bar{Y} \subseteq X$  with subspace topology is irreducible.
- (b) If  $\mathcal{C}$  is a chain of irreducible subsets of  $X$ , then  $\bigcup_{Y \in \mathcal{C}} Y$  with subspace topology is irreducible.
- (c) For irreducible  $Y \subseteq X$ , there exists a maximal irreducible subset  $Z \subseteq X$  such that  $Y \subseteq Z$ .
- (d)  $X$  is the union of its maximal irreducible subsets which are all closed.

*Proof.* (a) Assume  $Y \subseteq X$  is irreducible. Let  $\bar{Y} = V_1 \cup V_2$  with  $V_1, V_2 \subseteq \bar{Y}$  closed. Let  $i \in \{1, 2\}$ . Since  $V_i$  is closed in  $\bar{Y}$  and  $\bar{Y}$  has subspace topology, there exists  $\tilde{V}_i \subseteq X$  closed in  $X$  such that  $V_i = \tilde{V}_i \cap \bar{Y}$ . Set  $V'_i = \tilde{V}_i \cap Y = (\tilde{V}_i \cap \bar{Y}) \cap Y = V_i \cap Y$ . Since  $V_i$  is closed in  $\bar{Y}$ ,  $V'_i = V_i \cap Y$  is closed in  $Y^\dagger$ . Then  $\bar{Y} = V_1 \cup V_2 = (\tilde{V}_1 \cap \bar{Y}) \cup (\tilde{V}_2 \cap \bar{Y}) = (\tilde{V}_1 \cup \tilde{V}_2) \cap \bar{Y}$ . So  $Y \subseteq \bar{Y} \subseteq \tilde{V}_1 \cup \tilde{V}_2$ . Hence  $Y = (\tilde{V}_1 \cup \tilde{V}_2) \cap Y = (\tilde{V}_1 \cap Y) \cup (\tilde{V}_2 \cap Y) = V'_1 \cup V'_2$ . Since  $Y$  is irreducible,  $Y = V'_1$  or  $V'_2$ . Say  $Y = V'_1 = V_1 \cap Y$ . Then  $Y \subseteq V_1 \subseteq \tilde{V}_1$ . Since  $\tilde{V}_1 \subseteq X$  is closed,  $\bar{Y} \subseteq \tilde{V}_1$ . Thus,  $\bar{Y} = \tilde{V}_1 \cap \bar{Y} = V_1$ .

(b) Let  $\mathcal{C}$  be a chain of irreducible subsets of  $X$  and  $Z := \bigcup_{Y \in \mathcal{C}} Y$ . Let  $V_1, V_2 \subsetneq Z$  be closed. Then there exist  $x_1 \in Z \setminus V_1$  and  $x_2 \in Z \setminus V_2$ . So there exist  $Y_1, Y_2 \in \mathcal{C}$  such that  $x_1 \in Y_1$  and  $x_2 \in Y_2$ . Since  $\mathcal{C}$  is a chain,  $Y_1 \subseteq Y_2$  or  $Y_2 \subseteq Y_1$ . Say  $Y_2 \subseteq Y_1$ , then  $x_1 \in Y_1 \setminus V_1$  and  $x_2 \in Y_1 \setminus V_2$ . So  $V_1 \cap Y_1 \subsetneq Y_1$  and  $V_2 \cap Y_1 \subsetneq Y_1$ . Since  $V_1, V_2$  are closed in  $Z$ ,  $V_1 \cap Y_1$  and  $V_2 \cap Y_1$  are closed in  $Y_1$  similar to (a). Also, since  $Y_1$  is irreducible, we have  $(V_1 \cap Y_1) \cup (V_2 \cap Y_1) \subsetneq Y_1$ . So  $Y_1 \not\subseteq V_1 \cup V_2$ . Also, since  $Y_1 \subseteq Z$ ,  $Z \not\subseteq V_1 \cup V_2$ . Thus,  $V_1 \cup V_2 \subsetneq Z$ .

(c) Let  $Y \subseteq X$  be irreducible. Set  $\Sigma = \{\text{irreducible subsets } Z \subseteq X \mid Y \subseteq Z\}$ . Since  $Y \in \Sigma$ ,  $\Sigma \neq \emptyset$ . From (b), Zorn' lemma applies. So  $\Sigma$  has a maximal element.

<sup>†</sup>Let  $Z \subseteq X$  have a subspace topology. If  $Y \subseteq Z$ , then the topology that  $Y$  inherits as a subspace of  $Z$  is the same as the topology that  $Y$  inherits as a subspace of  $X$



(d) Let  $\mathcal{M}$  be the union of the maximal irreducible subsets of  $X$ . Claim.  $X = \mathcal{M}$ . “ $\supseteq$ ”. It is straightforward. “ $\subseteq$ ”. Let  $x \in X$ , then  $\{x\} \subseteq X$  is irreducible. By (c), there exists a maximal irreducible subset  $Z \subseteq X$  such that  $\{x\} \subseteq Z$ . By (a),  $\bar{Z}$  is irreducible. Also, since  $Z \subseteq \bar{Z}$  and  $Z$  is maximal irreducible, we have  $Z = \bar{Z}$ , i.e.,  $Z$  is closed.  $\square$

**Definition 2.41.** The maximal irreducible subsets of  $X$  are the *irreducible components* of  $X$ .

**Proposition 2.42.** <sup>†</sup> Let  $X = \text{Spec}(R)$ .

(a)  $V \subseteq X$  with subspace topology is closed and irreducible if and only if  $V = V(\mathfrak{p})$  for some  $\mathfrak{p} \in \text{Spec}(R)$ .

(b) The irreducible components of  $X$  are  $V(\mathfrak{p})$ , where  $\mathfrak{p} \in \text{Min}(\text{Spec}(R)) = \text{Min}(R)$ .

*Proof.* (a) “ $\Leftarrow$ ”. Let  $\mathfrak{p} \in \text{Spec}(R)$ . Let  $V, W \subseteq V(\mathfrak{p})$  be closed such that  $V(\mathfrak{p}) = V \cup W$ . Then  $V = V(\mathfrak{a}) \cap V(\mathfrak{p})$  and  $W = V(\mathfrak{b}) \cap V(\mathfrak{p})$  for some  $\mathfrak{a}, \mathfrak{b} \leq R$ . Since  $\mathfrak{p} \in \text{Spec}(R)$ ,  $\mathfrak{p} \in V(\mathfrak{p}) = V \cup W = (V(\mathfrak{a}) \cap V(\mathfrak{p})) \cup (V(\mathfrak{b}) \cap V(\mathfrak{p})) = V(\mathfrak{a} + \mathfrak{p}) \cup V(\mathfrak{b} + \mathfrak{p}) = V(\mathfrak{a} + \mathfrak{p})(\mathfrak{b} + \mathfrak{p})$ . So  $\mathfrak{p} \supseteq (\mathfrak{a} + \mathfrak{p})(\mathfrak{b} + \mathfrak{p})$ . Since  $\mathfrak{p} \in \text{Spec}(R)$ ,  $\mathfrak{p} \supseteq \mathfrak{a} + \mathfrak{p} \supseteq \mathfrak{a}$  or  $\mathfrak{p} \supseteq \mathfrak{b} + \mathfrak{p} \supseteq \mathfrak{b}$ . So  $V(\mathfrak{p}) \subseteq V(\mathfrak{a})$  or  $V(\mathfrak{p}) \subseteq V(\mathfrak{b})$ . Hence  $V(\mathfrak{p}) = V(\mathfrak{a}) \cap V(\mathfrak{p}) = V$  or  $V(\mathfrak{p}) = V(\mathfrak{b}) \cap V(\mathfrak{p}) = W$ .

“ $\Rightarrow$ ”. Assume  $V \subseteq X$  is closed and irreducible. Then  $\emptyset \neq V = V(\mathfrak{a}) = V(\text{rad}(\mathfrak{a}))$  for some  $\mathfrak{a} \leq R$ . So it suffices to show  $\text{rad}(\mathfrak{a}) \in \text{Spec}(R)$ . Note  $\mathfrak{r} := \text{rad}(\mathfrak{a}) \leq R$ .

Method 1. Let  $x, y \in R$  such that  $xy \in \mathfrak{r}$ . Then  $\mathfrak{r}^2 \subseteq (xR + \mathfrak{r})(yR + \mathfrak{r}) \subseteq \mathfrak{r}$ . So  $V(\mathfrak{r}) = V(\mathfrak{r}^2) \supseteq V((xR + \mathfrak{r})(yR + \mathfrak{r})) \supseteq V(\mathfrak{r})$ . Hence  $V = V(\mathfrak{r}) = V((xR + \mathfrak{r})(yR + \mathfrak{r})) = (V(xR) \cap V(\mathfrak{r})) \cup (V(yR) \cap V(\mathfrak{r})) = (V(xR) \cap V) \cup (V(yR) \cap V)$ . Also, since  $V(xR) \cap V$  and  $V(yR) \cap V$  are closed in  $V$  and  $V$  is irreducible, we have  $V(\mathfrak{r}) = V(xR) \cap V \subseteq V(xR)$  or  $V(\mathfrak{r}) = V(yR) \cap V \subseteq V(yR)$ . Then  $x \in xR \subseteq \text{rad}(xR) = \bigcap_{\mathfrak{p} \in V(xR)} \mathfrak{p} \subseteq \bigcap_{\mathfrak{p} \in V(\mathfrak{r})} \mathfrak{p} = \text{rad}(\mathfrak{r}) = \mathfrak{r}$  by Fact 1.58(c) and (g), or  $y \in \mathfrak{r}$  similarly. So  $\text{rad}(\mathfrak{a}) = \mathfrak{r} \in \text{Spec}(R)$ .

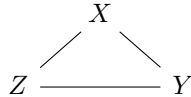
Method 2. Assume  $\text{rad}(\mathfrak{a}) \supseteq IJ$  for some  $I, J \leq R$ . Then  $V(I) \cup V(J) = V(IJ) \supseteq V(\text{rad}(\mathfrak{a})) = V(\mathfrak{a})$ . Since  $V(\mathfrak{a}) = V$  is irreducible and  $V(\mathfrak{a}) = (V(\mathfrak{a}) \cap V(I)) \cup (V(\mathfrak{a}) \cap V(J)) = V(\mathfrak{a}I) \cup V(\mathfrak{a}J)$ ,  $V(I) \supseteq V(\mathfrak{a})$  or  $V(J) \supseteq V(\mathfrak{a})$ . So by Proposition 1.32(d),  $\text{rad}(\mathfrak{a}) \supseteq \text{rad}(I) \supseteq I$  or  $\text{rad}(\mathfrak{a}) \supseteq \text{rad}(J) \supseteq J$ .

(b) Let  $V$  be an irreducible component of  $X = \text{Spec}(R)$ . Then  $V$  is closed by Proposition 2.40(c) and maximal irreducible. So by (a),  $V = V(\mathfrak{p})$  for some  $\mathfrak{p} \in \text{Spec}(R)$ . Let  $\mathfrak{q} \in \text{Spec}(R)$  such that  $\mathfrak{q} \subseteq \mathfrak{p}$ . Then  $V(\mathfrak{q}) \supseteq V(\mathfrak{p}) = V$ . By (a),  $V(\mathfrak{q})$  is closed and irreducible. So by the maximality of  $V$ ,  $V(\mathfrak{q}) = V(\mathfrak{p})$ . So  $\mathfrak{q} = \mathfrak{p}$  by Proposition 1.32(d).  $\square$

**Example 2.43.** Let  $R = \frac{k[X,Y,Z]}{(XY, YZ, XZ)}$ , where  $k$  is a field. Then

$$\begin{aligned} \langle XY, YZ, XZ \rangle &= \langle X, YZ, XZ \rangle \cap \langle Y, YZ, XZ \rangle = \langle X, YZ \rangle \cap \langle Y, XZ \rangle \\ &= \langle X, Y \rangle \cap \langle X, Z \rangle \cap \langle Y, X \rangle \cap \langle Y, Z \rangle = \langle X, Y \rangle \cap \langle X, Z \rangle \cap \langle Y, Z \rangle. \end{aligned}$$

Or let  $G$  be the following graph:



<sup>†</sup>This proposition also holds for  $V(\mathfrak{a})$  with subspace topology and with  $\text{Min}(V(\mathfrak{a}))$ .

Then the edge ideal of  $G$  is  $I_G = \langle XY, YZ, XZ \rangle$ . Let  $P_V = \langle X \mid X \in V \rangle$  for  $V \subseteq V(G)$ . Then we have  $I_G = \bigcap_{V \text{ min. v.cover}} P_V = P_{\{X,Y\}} \cap P_{\{Y,Z\}} \cap P_{\{X,Z\}} = \langle X, Y \rangle \cap \langle Y, Z \rangle \cap \langle X, Z \rangle$ . So  $\text{Min}(k[X, Y, Z]) = \{P_V \mid V \text{ min. v.cover}\} = \{\langle X, Y \rangle, \langle Y, Z \rangle, \langle X, Z \rangle\}$ . By Fact 1.15,  $\text{Min}(R) = \{\langle \bar{X}, \bar{Y} \rangle, \langle \bar{Y}, \bar{Z} \rangle, \langle \bar{X}, \bar{Z} \rangle\}$ . So the irreducible components of  $\text{Spec}(R)$  are  $V(\langle \bar{X}, \bar{Y} \rangle)$ ,  $V(\langle \bar{X}, \bar{Z} \rangle)$  and  $V(\langle \bar{Y}, \bar{Z} \rangle)$ .

**Corollary 2.44.** (a)  $\text{Min}(R) \neq \emptyset$ .

(b) For  $\mathfrak{q} \in \text{Spec}(R)$ , there exists  $\mathfrak{p} \in \text{Min}(R)$  such that  $\mathfrak{p} \subseteq \mathfrak{q}$ .

*Proof.* (a) Since  $\text{Spec}(R) \neq \emptyset$ , by Proposition 2.42(b),  $\text{Min}(R) \neq \emptyset$ .

(b) Let  $\mathfrak{q} \in \text{Spec}(R)$ . Then  $V(\mathfrak{q}) \subseteq \text{Spec}(R)$  are closed and irreducible by Proposition 2.42(a). So there exists a (closed) maximal irreducible subset  $Z \subseteq \text{Spec}(R)$  such that  $V(\mathfrak{q}) \subseteq Z$  by Proposition 2.40(c). Then  $V(\mathfrak{q}) \subseteq Z = V(\mathfrak{p})$  for some  $\mathfrak{p} \in \text{Min}(R)$  by Proposition 2.42(b). So  $\mathfrak{p} \subseteq \mathfrak{q}$  by Proposition 1.32(d).  $\square$

**Proposition 2.45.** Let  $\mathfrak{p} \in \text{Spec}(R)$ .

(a)  $\overline{\{\mathfrak{p}\}} = V(\mathfrak{p})$ .

(b)  $\overline{\{\mathfrak{p}\}} = \{\mathfrak{p}\}$  if and only if  $\mathfrak{p} \in \text{m-Spec}(R)$ . “closed points are maximal”.

(c) If  $R$  is an integral domain, then  $\overline{\{0\}} = V(0) = \text{Spec}(R)$ . 0 is the “the generic point”.

*Proof.* (a) One point set  $\{\mathfrak{p}\}$  is clearly irreducible. Then  $\overline{\{\mathfrak{p}\}}$  is also irreducible by Proposition 2.40(a). Also, since  $\overline{\{\mathfrak{p}\}}$  is closed,  $\overline{\{\mathfrak{p}\}} = V(\mathfrak{a})$  for some  $\mathfrak{a} \leq R$  by Proposition 2.42(a). So  $\mathfrak{a} \subseteq \mathfrak{p}$ . Hence  $V(\mathfrak{p}) \subseteq V(\mathfrak{a}) = \overline{\{\mathfrak{p}\}}$ . Since  $\{\mathfrak{p}\}$  is the smallest closed subset containing  $\mathfrak{p}$ , we have  $\overline{\{\mathfrak{p}\}} = V(\mathfrak{p})$ .

(b) “ $\Rightarrow$ ”. Assume  $\overline{\{\mathfrak{p}\}} = \{\mathfrak{p}\}$ . Since  $\mathfrak{p} \neq R$ , there exists  $\mathfrak{m} \in \text{m-Spec}(R)$  such that  $\mathfrak{m} \supseteq \mathfrak{p}$ . Then  $\mathfrak{m} \subseteq V(\mathfrak{m}) \subseteq V(\mathfrak{p}) = \overline{\{\mathfrak{p}\}} = \{\mathfrak{p}\}$  by (a). So by the maximality of  $\mathfrak{m}$ , we have  $\mathfrak{p} = \mathfrak{m}$ .

“ $\Leftarrow$ ”. Assume  $\mathfrak{p} \in \text{m-Spec}(R)$ . Then by (a),  $\overline{\{\mathfrak{p}\}} = V(\mathfrak{p}) = \{\mathfrak{p}\}$ .

(c) It follows from (a).  $\square$



# Chapter 3

## Localization

Let  $R$  be a commutative ring with identity but not a field.

**Recall 3.1.** A subset  $U \subseteq R$  is *multiplicatively closed* if  $1 \in U$  and for  $u, v \in U$ ,  $uv \in U$ ,

**Example 3.2.** (a)  $\{1, f, f^2, \dots\} \subseteq R$  is multiplicatively closed for  $f \in R$ .

(b)  $R^\times \subseteq R$  is multiplicatively closed.

(c)  $R \setminus \mathfrak{p} \subseteq R$  is multiplicatively closed for  $\mathfrak{p} \in \text{Spec}(R)$ .

(d)  $1 + \mathfrak{a} \subseteq R$  is multiplicatively closed for  $\mathfrak{a} \leq R$ .

Let  $U \subseteq R$  be multiplicatively closed.

**Recall 3.3.**  $U^{-1}R = \{\frac{r}{u} \mid r \in R, u \in U\}$ , where  $\frac{r}{u} = \frac{r'}{u'}$  if and only if there exists  $u'' \in U$  such that  $u''(ru' - r'u) = 0$ , i.e.,  $\frac{u''r}{u''u} = \frac{r'}{u'}$ , formally,  $\frac{r}{u}$  is the equivalence class under an equivalence relation.

$U^{-1}R$  is a commutative ring with identity with  $\frac{r}{u} + \frac{s}{v} = \frac{rv+su}{uv}$  and  $\frac{r}{u} \frac{s}{v} = \frac{rs}{uv}$  for  $\frac{r}{u}, \frac{s}{v} \in U^{-1}R$ .

$0_{U^{-1}R} = \frac{0_R}{1_R} = \frac{0}{1}$  and  $1_{U^{-1}R} = \frac{1_R}{1_R} = \frac{1}{1}$  for all  $u \in U$ .

$\frac{r}{u} = 0$  if and only if there exists  $u'' \in U$  such that  $u''r = 0$ .

$\psi : R \rightarrow U^{-1}R$  given by  $\psi(r) = \frac{r}{1}$  is a well-defined ring homomorphism.  $\psi$  is 1-1 if and only if  $U \subseteq \text{NZD}(R)$ .

**Notation 3.4.** (a) If  $U = \{1, f, f^2, \dots\}$ , write  $U^{-1}R = R_f$ . ( $R_f = 0$  for  $f \in \text{Nil}(R)$ ).

(b) If  $U = R \setminus \mathfrak{p}$  for some  $\mathfrak{p} \in \text{Spec}(R)$ , write  $U^{-1}R = R_{\mathfrak{p}}$ .

(c) If  $U \subseteq R$  is multiplicatively closed, write  $U^{-1}R = R_U = R[U^{-1}]$ .

Let  $\psi : R \rightarrow U^{-1}R$  be the natural ring homomorphism.

**Recall 3.3+ε.**  $\psi(U) \subseteq (U^{-1}R)^\times$  since  $\frac{1}{u} = (\frac{u}{1})^{-1} = (\psi(u))^{-1}$  for  $u \in U$ . So localization makes more elements invertible.

Let  $\varphi : R \rightarrow S$  be a ring homomorphism.

**Proposition 3.5** (UMP for  $\psi$ ). Let  $\varphi(U) \subseteq S^\times$ . Then there exists a unique ring homomorphism  $\Phi : U^{-1}R \rightarrow S$  such that  $\Phi \circ \psi = \varphi$ . In fact,  $\Phi(\frac{r}{u}) = \varphi(r)\varphi(u)^{-1}$  for  $\frac{r}{u} \in U^{-1}R$ .

$$\begin{array}{ccc}
R & \xrightarrow{\psi} & U^{-1}R \\
& \searrow \varphi & \downarrow \exists! \Phi \\
& & S
\end{array}
\qquad
\begin{array}{ccc}
R & \xrightarrow{\psi} & U^{-1}R \\
& \searrow \varphi & \downarrow \Lambda \\
& & S
\end{array}$$

*Proof.* Let  $\frac{r}{u} = \frac{r'}{u'}$ . Then there exists  $u'' \in U$  such that  $u''(ru' - r'u) = 0$ . Since  $\varphi$  is a ring homomorphism, we have  $\varphi(u'')(\varphi(r)\varphi(u') - \varphi(r')\varphi(u)) = 0$ . Also, since  $\varphi(u'') \in S^\times$ , we have  $\varphi(r)\varphi(u') = \varphi(r')\varphi(u)$ , i.e.,  $\varphi(r)\varphi(u)^{-1} = \varphi(r')\varphi(u')^{-1}$  since  $\varphi(u), \varphi(u') \in S^\times$ . So  $\phi$  is well-defined. Since  $\Phi(\frac{r}{u} + \frac{s}{v}) = \Phi(\frac{rv+su}{uv}) = \varphi(rv+su)\varphi(uv)^{-1} = (\varphi(r)\varphi(v) + \varphi(s)\varphi(u))\varphi(u)^{-1}\varphi(v)^{-1} = \varphi(r)\varphi(u)^{-1} + \varphi(s)\varphi(v)^{-1} = \Phi(\frac{r}{u}) + \Phi(\frac{s}{v})$  and similarly,  $\Phi(\frac{r}{u} \cdot \frac{s}{v}) = \Phi(\frac{r}{u})\Phi(\frac{s}{v})$  for  $\frac{r}{u}, \frac{s}{v} \in U^{-1}R$ , we have  $\Phi$  is a ring homomorphism.

Suppose there is another ring homomorphism  $\Lambda : U^{-1}R \rightarrow S$  such that  $\Lambda \circ \psi = \varphi$ . Then  $\varphi(r) = \Lambda(\psi(r)) = \Lambda(\frac{r}{1})$  for  $r \in R$ . So  $\Lambda(\frac{r}{u}) = \Lambda(\frac{r}{1}\frac{1}{u}) = \Lambda(\frac{r}{1})\Lambda(\frac{1}{u})^{-1} = \varphi(r)\varphi(u)^{-1} = \Phi(\frac{r}{u})$  for  $\frac{r}{u} \in U^{-1}R$ . Thus,  $\Lambda = \Phi$ .  $\square$

**Proposition 3.6.** We have the following.

- (a)  $\varphi(U) \subseteq S$  is multiplicatively closed and  $\varphi(U)^{-1}S =: U^{-1}S$ .
- (b) There is a unique ring homomorphism  $U^{-1}\varphi : U^{-1}R \rightarrow U^{-1}S$  given by  $U^{-1}\varphi(r/u) = \varphi(r)/\varphi(u)$ .

$$\begin{array}{ccc}
R & \xrightarrow{\psi} & U^{-1}R \\
\downarrow \varphi & \begin{array}{ccc} r & \mapsto & \frac{r}{1} \\ \downarrow & & \downarrow \\ \varphi(r) & \mapsto & \frac{\varphi(r)}{1} \end{array} & \downarrow U^{-1}\varphi \\
S & \xrightarrow{\rho} & U^{-1}S
\end{array}$$

- (c) If  $\varphi$  is onto,  $U^{-1}\varphi$  is onto.
- (d) If  $\varphi$  is 1-1,  $U^{-1}\varphi$  is 1-1.
- (e) If  $\alpha : S \rightarrow T$  is a ring homomorphism, then  $U^{-1}(\alpha \circ \varphi) = (\varphi(U)^{-1}\alpha) \circ (U^{-1}\varphi)$ .

$$\begin{array}{ccccc}
R & \xrightarrow{\psi} & U^{-1}R & & \\
\downarrow \alpha \circ \varphi & \searrow \varphi & \downarrow & \searrow U^{-1}\varphi & \\
& & S & \xrightarrow{\quad} & U^{-1}S \\
& \swarrow \alpha & \downarrow & \swarrow \varphi(U)^{-1}\alpha & \\
T & \xrightarrow{\quad} & \varphi(U)^{-1}T := \alpha(\varphi(U))^{-1}T & & 
\end{array}$$

*Proof.* (b) Let  $\frac{r}{u} = \frac{r'}{u'} \in U^{-1}R$ . Then there exists  $u'' \in U$  such that  $u''(ru' - r'u) = 0$ . So there exists  $\varphi(u'') \in \varphi(U)$  such that  $\varphi(u'')(\varphi(r)\varphi(u') - \varphi(r')\varphi(u)) = 0$ . Hence  $\frac{\varphi(r)}{\varphi(u)} = \frac{\varphi(r')}{\varphi(u')}$  in  $U^{-1}S$ . So  $U^{-1}\varphi$  is well-defined. Since  $U^{-1}\varphi(\frac{r}{u} + \frac{s}{v}) = U^{-1}\varphi(\frac{rv+su}{uv}) = \frac{\varphi(rv+su)}{\varphi(uv)} = \frac{\varphi(r)\varphi(v) + \varphi(s)\varphi(u)}{\varphi(u)\varphi(v)} = \frac{\varphi(r)}{\varphi(u)} + \frac{\varphi(s)}{\varphi(v)} = U^{-1}\varphi(\frac{r}{u}) + U^{-1}\varphi(\frac{s}{v})$  and similarly,  $U^{-1}\varphi(\frac{r}{u} \cdot \frac{s}{v}) = U^{-1}\varphi(\frac{r}{u})U^{-1}\varphi(\frac{s}{v})$  for  $\frac{r}{u}, \frac{s}{v} \in U^{-1}R$ .

Since  $\varphi(U) \subseteq S$  is multiplicatively closed, by Recall 3.3+ $\epsilon$ ,  $\rho(\varphi(U)) \subseteq ((\varphi(U))^{-1}S)^\times = (U^{-1}S)^\times$ . Then the uniqueness follows from Proposition 3.5.

(c) Assume  $\varphi$  is onto. Let  $\frac{s}{\varphi(u)} \in U^{-1}S$  with  $s \in S$  and  $u \in U$ . Since  $\varphi : R \rightarrow S$  is onto, there exists  $r \in R$  such that  $\varphi(r) = s$ . Then  $U^{-1}\varphi(\frac{r}{u}) = \frac{\varphi(r)}{\varphi(u)} = \frac{s}{\varphi(u)}$ .

(d) Assume  $\varphi$  is 1-1. Let  $\frac{r}{u} \in U^{-1}R$  with  $r \in R$  and  $u \in U$ . Then  $\frac{r}{u} \in \text{Ker}(U^{-1}\varphi)$  if and only if  $0 = U^{-1}\varphi(\frac{r}{u}) = \frac{\varphi(r)}{\varphi(u)}$  if and only if there exists  $u'' \in U$  such that  $0 = \varphi(u'')\varphi(r) = \varphi(u''r)$  if and only if there exists  $u'' \in U$  such that  $u''r = 0$  since  $\varphi$  is 1-1 if and only if  $\frac{r}{u} = 0$  in  $U^{-1}R$ .

(e) Since  $\varphi : R \rightarrow S$  and  $\alpha : S \rightarrow T$  are ring homomorphisms,  $\alpha \circ \varphi$  is a ring homomorphism. Since  $(\alpha \circ \varphi)(U) = \alpha(\varphi(U)) \subseteq T$  is multiplicatively closed by (a), we have  $U^{-1}(\alpha \circ \varphi)$  and  $\varphi(U)^{-1}\alpha$  are well-defined.

$$\begin{array}{ccc}
 U^{-1}R & & \\
 \downarrow & \searrow & \\
 & \frac{r}{u} & \searrow \frac{\varphi(r)}{\varphi(u)} \\
 & \downarrow & \swarrow \frac{\varphi(r)}{\varphi(u)} \\
 & \frac{(\alpha \circ \varphi)(r)}{(\alpha \circ \varphi)(u)} = \frac{\alpha(\varphi(r))}{\alpha(\varphi(u))} & \swarrow \frac{\varphi(r)}{\varphi(u)} \\
 (\alpha \circ \varphi)(U)^{-1}T & & \alpha(\varphi(U))^{-1}T
 \end{array}$$

Then by the commutative diagram,  $U^{-1}(\alpha \circ \varphi) = (\varphi(U)^{-1}\alpha) \circ (U^{-1}\varphi)$ .  $\square$

**Proposition 3.7.** Let  $\varphi(U) \subseteq S$  be multiplicatively closed. Then  $\text{Im}(U^{-1}\varphi) \cong U^{-1}\text{Im}(\varphi)$  given by  $\frac{\varphi(r)}{\varphi(u)} \mapsto \frac{i(\pi(r))}{i(\pi(u))} = \frac{\varphi(r)}{\varphi(u)}$ .

*Proof.* We have

$$\begin{array}{ccccc}
 R & \xrightarrow{\psi} & U^{-1}R & & \\
 \downarrow \varphi & \searrow \pi & \downarrow U^{-1}\varphi & \searrow U^{-1}\pi & \\
 & \text{Im}(\varphi) & \xrightarrow{\quad} & U^{-1}\text{Im}(\varphi) & \\
 & \swarrow i & \downarrow & \swarrow \pi(U)^{-1}i & \\
 S & \xrightarrow{\quad} & U^{-1}S & & 
 \end{array}$$

By Proposition 3.6(e),  $\text{Im}(U^{-1}\varphi) = \text{Im}(i \circ \pi) = \text{Im}((\pi(U)^{-1}i) \circ U^{-1}\pi)$ . Since  $\pi$  is onto,  $U^{-1}(\pi)$  is onto by Proposition 3.6(c). So  $\text{Im}(U^{-1}\varphi) = \text{Im}(\pi(U)^{-1}i)$ . Since  $i$  is 1-1,  $\pi(U)^{-1}i$  is 1-1 by Proposition 3.6(d). Hence by the first isomorphism theorem,  $U^{-1}\text{Im}(\varphi) \cong \text{Im}(\pi(U)^{-1}i) = \text{Im}(U^{-1}\varphi)$ .  $\square$

Let  $\mathfrak{a}, \mathfrak{b} \leq R$ .

**Definition 3.8.** Define a relation “ $\sim$ ” on  $U \times \mathfrak{a}$  by  $(u, a) \sim (u', a')$  if and only if there exists  $u'' \in U$  such that  $u''(u'a - ua') = 0$ .

**Fact 3.9.** This is an equivalence relation.

**Notation 3.10.**  $U^{-1}\mathfrak{a} = \{\text{equivalence classes from } U \times \mathfrak{a} \text{ under } \sim\}$ , and  $a/u$  or  $\frac{a}{u}$  with  $a \in \mathfrak{a}$  and  $u \in U$  are its elements, i.e.,  $U^{-1}\mathfrak{a} = \{a/u \mid a \in \mathfrak{a}, u \in U\}$ .

**Proposition 3.11.** We have the following.

(a) The map  $i : U^{-1}\mathfrak{a} \rightarrow U^{-1}R$  given by  $i(a/u) = a/u$  is a well-defined ring monomorphism. Identify  $U^{-1}\mathfrak{a}$  with  $\text{Im}(i) \subseteq U^{-1}R$ , so write  $U^{-1}\mathfrak{a} \subseteq U^{-1}R$ .

**Warning.**  $\frac{r}{u} \in U^{-1}R$  such that  $\frac{r}{u} \in U^{-1}\mathfrak{a}$  may have  $r \notin \mathfrak{a}$ .

(b) If  $\frac{r}{u} \in U^{-1}R$ , then  $\frac{r}{u} \in U^{-1}\mathfrak{a}$  if and only if there exists  $v \in U$  such that  $vr \in \mathfrak{a}$ , in this case, we have  $\frac{r}{u} = \frac{vr}{vu} \in U^{-1}\mathfrak{a}$  with  $ur \in \mathfrak{a}$  and  $vu \in U$ .

(c) Let  $\pi : R \rightarrow \frac{R}{\mathfrak{a}}$  be the natural surjection. Then  $U^{-1}\mathfrak{a} = \text{Ker}(U^{-1}\pi) \leq U^{-1}R$  and  $\frac{U^{-1}R}{U^{-1}\mathfrak{a}} \cong U^{-1}\frac{R}{\mathfrak{a}} := \pi(U^{-1}\frac{R}{\mathfrak{a}})$ .

(d) More generally, if  $\varphi : R \rightarrow S$  is a ring homomorphism, then  $U^{-1}\text{Ker}(\varphi) = \text{Ker}(U^{-1}\varphi) \leq U^{-1}R$  such that  $\text{Im}(U^{-1}\varphi) \cong \frac{U^{-1}R}{U^{-1}\text{Ker}(\varphi)}$ .

(e)  $U^{-1}\mathfrak{a} = \mathfrak{a} \cdot U^{-1}R$ , extension of  $\mathfrak{a}$  along  $\psi : R \rightarrow U^{-1}R$ .

*Proof.* (a) By the definition of “ $\sim$ ”,  $i$  is a well-defined ring monomorphism. Let  $\frac{a}{u} \in U^{-1}\mathfrak{a}$  with  $a \in R$  and  $u \in U$ . Then  $\frac{a}{u} \in \text{Ker}(i)$  if and only if  $0 = i(\frac{a}{u}) = \frac{a}{u}$  in  $U^{-1}R$  if and only if there exists  $v \in U$  such that  $va = 0 \in \mathfrak{a} \subseteq R$  if and only if  $\frac{a}{u} = \frac{va}{vu} = \frac{0}{vu} = 0$  in  $U^{-1}\mathfrak{a}$  by (b). Also, since  $i$  is a ring homomorphism,  $i$  is 1-1.

(b) Method 1. “ $\Rightarrow$ ”. Assume  $\frac{r}{u} \in U^{-1}\mathfrak{a}$ . Then  $\frac{r}{u} = \frac{a}{u'}$  for some  $a \in \mathfrak{a}$  and  $u' \in U$ . So there exists  $u'' \in U$  such that  $u''u'r = u''ua \in \mathfrak{a}$  since  $a \in \mathfrak{a}$ . Let  $v = u''u'$ . Then  $vr = u''u'r \in \mathfrak{a}$ .

“ $\Leftarrow$ ”. Assume  $vr \in \mathfrak{a}$  for some  $v \in U$ . Then  $\frac{r}{u} = \frac{vr}{vu} \in U^{-1}\mathfrak{a}$ .

Method 2. Note  $\frac{r}{u} \in U^{-1}\mathfrak{a}$  if and only if  $\frac{r}{u} = \frac{a}{u'}$  for some  $a \in \mathfrak{a}$  and  $u' \in U$  if and only if  $u''u'r - u''ua = 0$  for some  $a \in \mathfrak{a}$  and  $u', u'' \in U$  if and only if  $1 \cdot v \cdot r - 1 \cdot 1 \cdot a = 0$  for some  $a \in \mathfrak{a}$  and  $v \in U$  if and only if there exists  $v \in U$  such that  $vr \in \mathfrak{a}$ .

(c) Note by Proposition 3.7,  $\text{Im}(U^{-1}\pi) \cong U^{-1}\text{Im}(\pi) = U^{-1}\frac{R}{\mathfrak{a}}$  given by  $\frac{\bar{r}}{\bar{u}} \mapsto \frac{\bar{r}}{\bar{u}}$ . Then by (d),  $U^{-1}\frac{R}{\mathfrak{a}} \cong \frac{U^{-1}R}{U^{-1}\text{Ker}(\pi)} = \frac{U^{-1}R}{U^{-1}\mathfrak{a}}$  given by  $\frac{\bar{r}}{\bar{u}} \mapsto \frac{\bar{r}}{\bar{u}}$ .

(d) Let  $\frac{r}{u} \in U^{-1}R$  with  $r \in R$  and  $u \in U$ . Then  $\frac{r}{u} \in U^{-1}\text{Ker}(\varphi)$  if and only if there exists  $v \in U$  such that  $vr \in \text{Ker}(\varphi)$  by (b) if and only if there exists  $\varphi(v) \in \varphi(U)$  such that  $0 = \varphi(vr) = \varphi(v)\varphi(r)$  if and only if  $U^{-1}\varphi(\frac{r}{u}) = \frac{\varphi(r)}{\varphi(u)} = 0$  in  $U^{-1}S = \varphi(U)^{-1}S$  if and only if  $\frac{r}{u} \in \text{Ker}(U^{-1}\varphi)$ .

By the first isomorphism theorem,  $\text{Im}(U^{-1}\varphi) \cong \frac{U^{-1}R}{\text{Ker}(U^{-1}\varphi)} = \frac{U^{-1}R}{U^{-1}\text{Ker}(\varphi)}$  given by  $\frac{\varphi(r)}{\varphi(u)} \mapsto \frac{\bar{r}}{\bar{u}}$ .

$$\begin{array}{ccc} U^{-1}R & \longrightarrow & \frac{U^{-1}R}{\text{Ker}(U^{-1}\varphi)} \\ & \searrow U^{-1}\varphi & \downarrow \\ & & \text{Im}(U^{-1}\varphi) \end{array}$$

(e) “ $\supseteq$ ”. It follows from  $\mathfrak{a} \cdot U^{-1}R$  is generated by  $\{\psi(a) = \frac{a}{1} \mid a \in \mathfrak{a}\} \subseteq U^{-1}\mathfrak{a}$ .

“ $\subseteq$ ”. Let  $\frac{a}{u} \in U^{-1}\mathfrak{a}$  with  $a \in \mathfrak{a}$  and  $u \in U$ . Then  $\frac{a}{u} = \frac{a}{1} \cdot \frac{1}{u} = \psi(a) \frac{1}{u} \in \mathfrak{a} \cdot U^{-1}R$ . □

**Proposition 3.12.** We have the following.

- (a)  $U^{-1}(\mathfrak{a} + \mathfrak{b}) = (U^{-1}\mathfrak{a}) + (U^{-1}\mathfrak{b})$ .
- (b)  $U^{-1}(\mathfrak{a} \cap \mathfrak{b}) = (U^{-1}\mathfrak{a}) \cap (U^{-1}\mathfrak{b})$ .
- (c)  $U^{-1}(\mathfrak{a}\mathfrak{b}) = (U^{-1}\mathfrak{a})(U^{-1}\mathfrak{b})$ .
- (d)  $U^{-1}\text{rad}(\mathfrak{a}) = \text{rad}(U^{-1}\mathfrak{a})$ .
- (e)  $U^{-1}\text{Nil}(R) = \text{Nil}(U^{-1}R)$ .
- (f)  $U^{-1}(\mathfrak{b} : \mathfrak{a}) = (U^{-1}\mathfrak{b} : U^{-1}\mathfrak{a})$  if  $\mathfrak{a}$  is finitely generated.

*Proof.* (a) By Proposition 3.11(e) and 1.63(c), we have  $U^{-1}(\mathfrak{a} + \mathfrak{b}) = (\mathfrak{a} + \mathfrak{b}) \cdot U^{-1}R = (\mathfrak{a} \cdot U^{-1}R) + (\mathfrak{b} \cdot U^{-1}R) = (U^{-1}\mathfrak{a}) + (U^{-1}\mathfrak{b})$ .

(b) “ $\subseteq$ ”. By Proposition 3.11(e) and 1.63(d),  $U^{-1}(\mathfrak{a} \cap \mathfrak{b}) = (\mathfrak{a} \cap \mathfrak{b}) \cdot U^{-1}R \subseteq (\mathfrak{a} \cdot U^{-1}R) \cap (\mathfrak{b} \cdot U^{-1}R) = (U^{-1}\mathfrak{a}) \cap (U^{-1}\mathfrak{b})$ .

“ $\supseteq$ ”. Let  $\frac{r}{u} \in U^{-1}R$  with  $r \in R, u \in U$  such that  $\frac{r}{u} \in (U^{-1}\mathfrak{a}) \cap (U^{-1}\mathfrak{b})$ . Then there exist  $v, w \in U$  such that  $vr \in \mathfrak{a}$  and  $wr \in \mathfrak{b}$  by Proposition 3.11(b). So  $(vw)r \in \mathfrak{a} \cap \mathfrak{b}$ . Also, since  $vw \in U$ ,  $\frac{r}{u} \in U^{-1}(\mathfrak{a} \cap \mathfrak{b})$  by Proposition 3.11(b).

(c) By Proposition 3.11(e) and 1.63(e), we have  $U^{-1}(\mathfrak{a}\mathfrak{b}) = (\mathfrak{a}\mathfrak{b}) \cdot U^{-1}R = (\mathfrak{a} \cdot U^{-1}R)(\mathfrak{b} \cdot U^{-1}R) = (U^{-1}\mathfrak{a})(U^{-1}\mathfrak{b})$ .

(d) “ $\subseteq$ ”. By Proposition 3.11(e) and 1.63(g),  $U^{-1}\text{rad}(\mathfrak{a}) = \text{rad}(\mathfrak{a}) \cdot U^{-1}R \subseteq \text{rad}(\mathfrak{a} \cdot U^{-1}R) = \text{rad}(U^{-1}\mathfrak{a})$ .

“ $\supseteq$ ”. Let  $\frac{r}{u} \in \text{rad}(U^{-1}\mathfrak{a})$  with  $r \in R$  and  $u \in U$ . Then  $\frac{r^n}{u^n} = (\frac{r}{u})^n \in U^{-1}\mathfrak{a}$  for some  $n \geq 1$ . So there exists  $v \in U$  such that  $vr^n \in \mathfrak{a}$  by Proposition 3.11(b). Hence  $(vr)^n = v^{n-1} \cdot vr^n \in \mathfrak{a}$ . So  $vr \in \text{rad}(\mathfrak{a})$ . Thus,  $\frac{r}{u} \in U^{-1}\text{rad}(\mathfrak{a})$  by Proposition 3.11(b).

(e) Special case of (d) with  $\mathfrak{a} = 0$ .

(f) “ $\subseteq$ ”. By Proposition 3.11(e) and 1.63(f),  $U^{-1}(\mathfrak{b} : \mathfrak{a}) = (\mathfrak{b} : \mathfrak{a}) \cdot U^{-1}R \subseteq (\mathfrak{b} \cdot U^{-1}R : \mathfrak{a} \cdot U^{-1}R) = (U^{-1}\mathfrak{b} : U^{-1}\mathfrak{a})$ .

“ $\supseteq$ ”. Let  $\frac{r}{u} \in U^{-1}R$  with  $r \in R, u \in U$  such that  $\frac{r}{u} \in (U^{-1}\mathfrak{b} : U^{-1}\mathfrak{a})$ . Since  $\mathfrak{a}$  is finitely generated,  $\mathfrak{a} = \langle a_1, \dots, a_n \rangle R$  for some  $n \geq 1$  and  $a_1, \dots, a_n \in R$ . Then  $U^{-1}\mathfrak{a} = \langle \frac{a_1}{1}, \dots, \frac{a_n}{1} \rangle U^{-1}R$ . Since  $\frac{r}{u} \in (U^{-1}\mathfrak{b} : U^{-1}\mathfrak{a})$ ,  $\frac{ra_i}{u} = \frac{r}{u} \frac{a_i}{1} \in U^{-1}\mathfrak{b}$  for  $i = 1, \dots, n$ . So by Proposition 3.11(b), there exists  $v_i \in U$  such that  $v_i ra_i \in \mathfrak{b}$  for  $i = 1, \dots, n$ . Let  $v = v_1 \cdots v_n \in U$ . Then  $(vr)a_i \in \mathfrak{b}$  for  $i = 1, \dots, n$ . So  $vr \in (\mathfrak{b} : \mathfrak{a})$ . Thus,  $\frac{r}{u} \in U^{-1}(\mathfrak{b} : \mathfrak{a})$  by Proposition 3.11(b).  $\square$

**Proposition 3.13.** We have the following.

- (a) For  $I \leq U^{-1}R$ , there exists  $\mathfrak{a} \leq R$  such that  $I = U^{-1}\mathfrak{a}$ , i.e., every ideal of  $U^{-1}R$  is an extension of an ideal of  $R$  along  $\psi$ .
- (b) If  $\mathfrak{a} \leq R$ , then  $\psi^{-1}(U^{-1}\mathfrak{a}) = \{r \in R \mid \exists v \in U \text{ s.t. } vr \in \mathfrak{a}\} = \bigcup_{v \in U} (\mathfrak{a} : v)$ .
- (c)  $U^{-1}\frac{R}{\mathfrak{a}} = 0$  if and only if  $\frac{U^{-1}R}{U^{-1}\mathfrak{a}} = 0$  if and only if  $U^{-1}\mathfrak{a} = U^{-1}R$  if and only if  $U \cap \mathfrak{a} \neq \emptyset$ .



*Proof.* (a) Since  $I \leq U^{-1}R$ , we have  $\psi^{-1}(I) \leq R$ . Claim.  $I = U^{-1}(\psi^{-1}(I))$ .

“ $\supseteq$ ”. By Proposition 1.63(a),  $I \supseteq \psi^{-1}(I) \cdot U^{-1}R = U^{-1}(\psi^{-1}(I))$ .

“ $\subseteq$ ”. Let  $i \in I$ . Then  $i = \frac{r}{u}$  for some  $r \in R$  and  $u \in U$ . Also, since  $\frac{u}{1} \in R$ ,  $\psi(r) = \frac{r}{1} = \frac{r}{u} \cdot \frac{u}{1} \in I$ , i.e.,  $r \in \psi^{-1}(I)$ . So  $i = \frac{r}{u} \in U^{-1}(\psi^{-1}(I))$ .

(b) Let  $r \in R$ . Then  $r \in \psi^{-1}(U^{-1}\mathfrak{a})$  if and only if  $\frac{r}{1} = \psi(r) \in U^{-1}\mathfrak{a}$  if and only if  $vr \in \mathfrak{a}$  for some  $v \in U$  by Proposition 3.11(b) if and only if  $r \in (\mathfrak{a} : v)$  for some  $v \in U$  if and only if  $r \in \bigcup_{v \in U} (\mathfrak{a} : v)$ .

(c) By Proposition 3.11(c),  $U^{-1}\frac{R}{\mathfrak{a}} = 0$  if and only if  $\frac{U^{-1}R}{U^{-1}\mathfrak{a}} = 0$ . Note  $U^{-1}\mathfrak{a} = U^{-1}R$  if and only if  $\frac{1}{1} \in U^{-1}\mathfrak{a}$  if and only if  $1 \in \psi^{-1}(U^{-1}\mathfrak{a}) = \bigcup_{v \in U} (\mathfrak{a} : v)$  if and only if  $U \cap \mathfrak{a} \neq \emptyset$  by (b).  $\square$

**Corollary 3.14.** Let  $\mathfrak{p} \in \text{Spec}(R)$  and  $Q(R/\mathfrak{p})$  be the field of fraction. Then  $R_{\mathfrak{p}} = U^{-1}R$  is local with maximal ideal  $\mathfrak{p}_{\mathfrak{p}} := \mathfrak{p}R_{\mathfrak{p}} = U^{-1}\mathfrak{p}$  and  $Q(R/\mathfrak{p}) \xleftarrow{\cong} R_{\mathfrak{p}}/\mathfrak{p}_{\mathfrak{p}}$  given by  $\bar{r}/\bar{u} \mapsto \bar{r}/\bar{u}$ .

*Proof.* Note  $I \leq U^{-1}R$  if and only if there exists  $\mathfrak{a} \leq R$  with  $U \cap \mathfrak{a} = \emptyset$  such that  $I = U^{-1}\mathfrak{a}$  by Proposition 3.13(a) and (c). Since  $\max\{\mathfrak{a} \leq R \mid U \cap \mathfrak{a} = \emptyset\} = \mathfrak{p}$ ,  $\text{m-Spec}(R_{\mathfrak{p}}) = \{U^{-1}\mathfrak{p}\}$ .

Let  $\tau : R \rightarrow R/\mathfrak{p}$  be the natural projection. Then by Proposition 3.11(c),  $R_{\mathfrak{p}}/\mathfrak{p}_{\mathfrak{p}} = \frac{U^{-1}R}{U^{-1}\mathfrak{p}} \cong U^{-1}\frac{R}{\mathfrak{p}}^{\dagger} := \tau(U)^{-1}\frac{R}{\mathfrak{p}} = Q(R/\mathfrak{p})$ .  $\square$

**Corollary 3.15.** If  $\mathfrak{m} \in \text{m-Spec}(R)$ , then  $R_{\mathfrak{m}}/\mathfrak{m}_{\mathfrak{m}} \cong R/\mathfrak{m}$ .

*Proof.* Since  $\mathfrak{m} \in \text{m-Spec}(R)$ ,  $R/\mathfrak{m}$  is a field. So by Corollary 3.14,  $R_{\mathfrak{m}}/\mathfrak{m}_{\mathfrak{m}} \cong Q(R/\mathfrak{m}) = R/\mathfrak{m}$ .  $\square$

**Example.** (a) Let  $p \in \mathbb{Z}$  be prime. Then  $\langle p \rangle \in \text{m-Spec}(\mathbb{Z})$ . So  $\mathbb{Z}_{(p)}/(p)_{(p)} \cong \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ .

(b) Let  $a_1, \dots, a_d \in k$ . Then, similarly,

$$\frac{k[X_1, \dots, X_d]_{(X_1 - a_1, \dots, X_d - a_d)}}{(X_1 - a_1, \dots, X_d - a_d)_{(X_1 - a_1, \dots, X_d - a_d)}} \cong Q\left(\frac{k[X_1, \dots, X_d]}{(X_1 - a_1, \dots, X_d - a_d)}\right) \cong Q(k) = k.$$

Let  $\mathfrak{p} \in \text{Spec}(R)$ .

**Question.**  $U \cap \mathfrak{p} = \emptyset$  if and only if  $U^{-1}\mathfrak{p} \in \text{Spec}(U^{-1}R)$  by prime correspondence for localization. What does  $(U^{-1}R)_{U^{-1}\mathfrak{p}}$  look like?

**Lemma 3.16.** Let  $U \cap \mathfrak{p} = \emptyset$ . Let  $\frac{r}{u} \in U^{-1}R$ . Then  $\frac{r}{u} \in U^{-1}\mathfrak{p}$  if and only if  $r \in \mathfrak{p}$ .

*Proof.* “ $\Leftarrow$ ”. By definition.

“ $\Rightarrow$ ”. Assume  $\frac{r}{u} \in U^{-1}\mathfrak{p}$ . Then there exists  $v \in U$  such that  $vr \in \mathfrak{p} \in \text{Spec}(R)$ . So  $v \in \mathfrak{p}$  or  $r \in \mathfrak{p}$ . Since  $v \in U$  and  $U \cap \mathfrak{p} = \emptyset$ , we have  $v \notin \mathfrak{p}$ . So  $r \in \mathfrak{p}$ .  $\square$

**Proposition 3.17.** Let  $U \cap \mathfrak{p} = \emptyset$ . Then  $U^{-1}\mathfrak{p} \in \text{Spec}(U^{-1}R)$  and

$$(U^{-1}R)_{U^{-1}\mathfrak{p}} \xrightarrow{\cong} R_{\mathfrak{p}} \\ \frac{r/1}{s/1} \mapsto r/s \quad s \in R \setminus \mathfrak{p}$$

*Proof.* We have

---

<sup>†</sup>In this case, some textbook denotes it  $(R/\mathfrak{p})_{\mathfrak{p}}$ .

$$\begin{array}{ccc}
r & \xrightarrow{\quad} & \frac{r}{1} \\
\downarrow & \begin{array}{ccc} R & \xrightarrow{\quad} & R_{\mathfrak{p}} \\ & \searrow \beta & \downarrow \exists \varphi \\ U^{-1}R & \xrightarrow{\alpha} & (U^{-1}R)_{U^{-1}\mathfrak{p}} \end{array} & \downarrow \\
r/1 & \xrightarrow{\quad} & \frac{r/1}{1/1}
\end{array}$$

Let  $\beta = \alpha \circ \psi$ . By proposition 3.5, to show  $\varphi$  is a well-defined ring homomorphism, it suffices to show  $\beta(R \setminus \mathfrak{p}) \subseteq ((U^{-1}R)_{U^{-1}\mathfrak{p}})^{\times}$  since  $U \subseteq R \setminus \mathfrak{p}$ . Let  $x \in R \setminus \mathfrak{p}$ . Then  $\beta(x) = \frac{x/1}{1/1}$ . Since  $x/1 \in U^{-1}R$  and  $x \notin \mathfrak{p}$ , we have  $x/1 \notin U^{-1}\mathfrak{p}$  by Lemma 3.16. So  $\frac{x}{1}$  is an allowable denominator in  $(U^{-1}R)_{U^{-1}\mathfrak{p}}$ . Hence  $\frac{1/1}{x/1} \in (U^{-1}R)_{U^{-1}\mathfrak{p}}$ . Thus,  $\frac{x/1}{1/1} \in ((U^{-1}R)_{U^{-1}\mathfrak{p}})^{\times}$  with  $(\frac{x/1}{1/1})^{-1} = \frac{1/1}{x/1}$ . Besides, by Proposition 3.5, we have  $\varphi(r/s) = \beta(r)/\beta(s) = \frac{r/1}{s/1}$  for  $\frac{r}{s} \in R_{\mathfrak{p}}$ .

Let  $\frac{r}{s} \in R_{\mathfrak{p}}$ . Then  $\frac{r}{s} \in \text{Ker}(\varphi)$  if and only if  $0 = \varphi(\frac{r}{s}) = \frac{r/1}{s/1} \in (U^{-1}R)_{U^{-1}\mathfrak{p}}$  if and only if there exists  $\frac{t}{v} \in U^{-1}R \setminus U^{-1}\mathfrak{p}$  with  $t \in R \setminus \mathfrak{p}$  such that  $\frac{tr}{v} = \frac{t}{v} \cdot \frac{r}{1} = 0$  in  $U^{-1}R$  by Proposition 3.11(b) and Lemma 3.16 if and only if there exist  $t \in R \setminus \mathfrak{p}$  and  $w \in U \subseteq R \setminus \mathfrak{p}$  such that  $wtr = 0$  in  $R$  by Proposition 3.11(b) if and only if there exists  $v' \in U \subseteq R \setminus \mathfrak{p}$  such that  $v'r = 0$  in  $R$  since  $R \setminus \mathfrak{p}$  is multiplicatively closed if and only if  $\frac{r}{s} = 0$  in  $R_{\mathfrak{p}}$  by Proposition 3.11(b). So  $\varphi$  is 1-1.

Let  $\frac{r/u}{s/v} \in (U^{-1}R)_{U^{-1}\mathfrak{p}}$  with  $r \in R$ ,  $u, v \in U \subseteq R \setminus \mathfrak{p}$  and  $s \in R \setminus \mathfrak{p}$ . Then  $us \in R \setminus \mathfrak{p}$  since  $R \setminus \mathfrak{p}$  is multiplicatively closed. So  $\frac{vr}{us} \in R_{\mathfrak{p}}$ . Also, since  $\varphi(\frac{vr}{us}) = \frac{\beta(vr)}{\beta(us)} = \frac{vr/1}{us/1} = \frac{uv/1 \cdot r/u}{uv/1 \cdot s/v} = \frac{r/u}{s/v}$ , we have  $\varphi$  is onto.  $\square$

**Corollary 3.18.** If  $\mathfrak{q} \in \text{Spec}(R)$  with  $\mathfrak{p} \subseteq \mathfrak{q}$ , then  $\mathfrak{p}_{\mathfrak{q}} \in \text{Spec}(R_{\mathfrak{q}})$  and  $(R_{\mathfrak{q}})_{\mathfrak{p}_{\mathfrak{q}}} \xleftarrow{\cong} R_{\mathfrak{p}}$  given by  $\frac{r/1}{s/1} \mapsto r/s$ .

*Proof.* Take  $U = R \setminus \mathfrak{q}$  in Proposition 3.17.  $\square$

**Example.** (a) Let  $0 \neq p \in \mathbb{Z}$  be prime. Then  $(0) \subseteq (p) \subsetneq \mathbb{Z}$  and  $\mathbb{Z}_{(p)} = \{\frac{m}{n} \in \mathbb{Q} \mid (n, p) = 1\}$  is a domain. So by Corollary 3.18,  $Q(\mathbb{Z}_{(p)}) = (\mathbb{Z}_{(p)})_{(0)_{(p)}} \cong \mathbb{Z}_{(0)} = Q(\mathbb{Z}) = \mathbb{Q}$ .

(b) Let  $R$  be a domain and  $0 \notin U$ . Then  $U^{-1}R$  is a domain and  $\mathfrak{p} := (0) \in \text{Spec}(R)$ . So  $Q(U^{-1}R) = (U^{-1}R)_{U^{-1}(0)} \cong R_{(0)} = Q(R)$  by Proposition 3.17. In fact, the map  $Q(U^{-1}R) \xleftarrow{\cong} Q(R)$  is given by  $\frac{r/1}{s/1} \mapsto r/s$ .

**Proposition 3.19.** Let  $R \neq 0$ . Then  $\text{NZD}(R) \subseteq R$  is multiplicatively closed. Moreover, it is *saturated*: if  $r, s \in R$  such that  $rs \in \text{NZD}(R)$ , then  $r, s \in \text{NZD}(R)$ .

*Proof.* Since  $R \neq 0$ ,  $1 \in \text{NZD}$ . Let  $r, s \in \text{NZD}(R)$ . Assume  $(rs)t = 0$  for some  $t \in R$ . Then  $r(st) = 0$ . Since  $r \in \text{NZD}(R)$ ,  $st = 0$ . Also, since  $s \in \text{NZD}(R)$ ,  $t = 0$ . So  $rs \in \text{NZD}(R)$ .

Let  $x, y \in R$  such that  $xy \in \text{NZD}(R)$ . By symmetry, we need to show  $x \in \text{NZD}(R)$ . Assume  $xz = 0$  for some  $z \in R$ . Then  $(xy)z = y(xz) = 0$ . Since  $xy \in \text{NZD}(R)$ ,  $z = 0$ .  $\square$

**Definition 3.20.** The *total ring of fractions of  $R$*  (or *total quotient ring of  $R$* ) is

$$Q(R) = \text{NZD}(R)^{-1}R.$$

**Example.** (a) If  $R$  is an integral domain, then  $\text{NZD}(R) = R \setminus \{0\}$  and  $\text{Q}(R) = \text{NZD}(R)^{-1}(R) = (R \setminus 0)^{-1}(R) = \text{Q}(R)$ . So the total ring of fractions of a domain is equal to the field of fraction.

(b) Let  $R = \frac{k[X,Y,Z,W]}{\langle XY,YZ,ZW,XW \rangle}$ , not an integral domain. Let  $x = \bar{X}$ ,  $y = \bar{Y}$ ,  $z = \bar{Z}$  and  $w = \bar{W}$ . Since  $\langle 0 \rangle R = \langle x, z \rangle \cap \langle y, w \rangle$  is a minimal primary decomposition,  $\text{Ass}_R(0) = \{\langle x, z \rangle, \langle y, w \rangle\}$ . So  $\text{ZD}(R) = \bigcup_{\mathfrak{p} \in \text{Ass}_R(0)} \mathfrak{p} = \langle x, z \rangle \cup \langle y, w \rangle$  by Corollary 4.34. Then  $U := \text{NZD}(R) = R \setminus \{\langle x, z \rangle \cup \langle y, w \rangle\}$ .

By prime correspondence for localization,  $\text{Spec}(\text{Q}(R)) = \{U^{-1}\mathfrak{p} \mid \mathfrak{p} \in \text{Spec}(R), \mathfrak{p} \cap U = \emptyset\} = \{U^{-1}\langle x, z \rangle, U^{-1}\langle y, w \rangle\}$ . Let  $\mathfrak{p}_1 = U^{-1}\langle x, z \rangle$  and  $\mathfrak{p}_2 = U^{-1}\langle y, w \rangle$ . Then by Proposition 3.12(b),  $\mathfrak{p}_1 \cap \mathfrak{p}_2 = U^{-1}(\langle x, z \rangle \cap \langle y, w \rangle) = U^{-1}\langle xy, yz, zw, xw \rangle = 0$ . So  $\text{m-Spec}(U^{-1}R) = \{\mathfrak{p}_1, \mathfrak{p}_2\}$ . Hence  $\mathfrak{p}_1 + \mathfrak{p}_2 = U^{-1}R = \text{Q}(R)$ . Let  $\pi_1 : R \rightarrow R/\langle x, z \rangle$  and  $\pi_2 : R \rightarrow R/\langle y, w \rangle$  be natural surjections. Then by Chinese Remainder Theorem and Proposition 3.17 with  $0 \notin \pi_1(R \setminus \langle x, z \rangle \cup \langle y, w \rangle) = \pi_1(U)$  and  $0 \notin \pi_2(U)$ ,

$$\begin{aligned} \text{Q}(R) &\cong \frac{U^{-1}R}{\mathfrak{p}_1} \times \frac{U^{-1}R}{\mathfrak{p}_2} = \text{Q}\left(\frac{U^{-1}R}{\mathfrak{p}_1}\right) \times \text{Q}\left(\frac{U^{-1}R}{\mathfrak{p}_2}\right) \cong \text{Q}\left(U^{-1}\frac{R}{\langle x, z \rangle}\right) \times \text{Q}\left(U^{-1}\frac{R}{\langle y, w \rangle}\right) \\ &\cong \left(U^{-1}\frac{R}{\langle x, z \rangle}\right)_{U^{-1}(0)} \times \left(U^{-1}\frac{R}{\langle y, w \rangle}\right)_{U^{-1}(0)} \cong \left(\frac{R}{\langle x, z \rangle}\right)_{(0)} \times \left(\frac{R}{\langle y, w \rangle}\right)_{(0)} \\ &\cong \text{Q}\left(\frac{R}{\langle x, z \rangle}\right) \times \text{Q}\left(\frac{R}{\langle y, w \rangle}\right) \cong \text{Q}(k[Y, W]) \times \text{Q}(k[X, Z]) = k(Y, W) \times k(X, Z). \end{aligned}$$

**Proposition 3.21.** The natural ring homomorphism  $\psi : R \rightarrow \text{Q}(R)$  is 1-1. Moreover,  $\text{NZD}(R)$  is the unique largest multiplicatively closed subset of  $R$  with this property.

*Proof.* Let  $r \in R$ . Then  $r \in \text{Ker}(\psi)$  if and only if  $\psi(r) = 0 = \frac{r}{1}$  in  $\text{Q}(R)$  if and only if there exists  $v \in \text{NZD}(R)$  such that  $vr = 0$  by Proposition 3.11(b)(b) if and only if  $r = 0$ . So  $\psi$  is 1-1.

Assume  $U \subseteq R$  is multiplicatively closed such that the natural ring homomorphism  $\phi : R \rightarrow U^{-1}R$  is 1-1. Let  $u \in U$ . Let  $r \in R$  such that  $ur = 0$ . Then  $\phi(r) = \frac{r}{1} = \frac{ur}{u} = \frac{0}{u} = 0$ . Also, since  $\phi$  is 1-1,  $r = 0$ . So  $u \in \text{NZD}(R)$ .  $\square$

**Question 3.22.** Let  $\varphi^* : \text{Spec}(S) \rightarrow \text{Spec}(R)$ .

(a) When is  $\mathfrak{p} \in \text{Im}(\varphi^*)$ ?, i.e., when does there exist  $\mathfrak{q} \in \text{Spec}(S)$  such that  $\mathfrak{p} = \varphi^{-1}(\mathfrak{q})$ .

(b) What does  $(\varphi^*)^{-1}(\mathfrak{p}) = \{\mathfrak{q} \in \text{Spec}(S) \mid \varphi^*(\mathfrak{q}) = \mathfrak{p}\}$  look like? In general, if  $f : Y \rightarrow X$  is a (continuous) function and  $x \in X$ , then  $f^{-1}(x) = \{y \in Y \mid f(y) = x\}$  = fibre over  $x$  w.r.t.  $f$ .

**Construction 3.23.** Let  $U = R \setminus \mathfrak{p}$ .

$$\begin{array}{ccc} R & \xrightarrow{\varphi} & S \\ \downarrow \psi & & \downarrow \rho \\ U^{-1}R & \xrightarrow{U^{-1}\varphi} & U^{-1}S \\ \downarrow \tau & & \downarrow \pi \\ \text{Q}(R/\mathfrak{p}) \cong \frac{R_{\mathfrak{p}}}{\mathfrak{p}_{\mathfrak{p}}} = \frac{U^{-1}R}{U^{-1}\mathfrak{p}U^{-1}R} & \xrightarrow{\overline{\pi \circ U^{-1}\varphi}} & \frac{U^{-1}S}{\mathfrak{p} \cdot U^{-1}S} := \frac{U^{-1}S}{\mathfrak{p}S \cdot U^{-1}S} := \frac{U^{-1}S}{U^{-1}\mathfrak{p} \cdot U^{-1}S} \\ & & \parallel \\ & & \mathcal{F}(\mathfrak{p}) = \frac{S_{\mathfrak{p}}}{\mathfrak{p} \cdot S_{\mathfrak{p}}} := \frac{\varphi(U)^{-1}S}{\varphi(U)^{-1}(\mathfrak{p}S)} \end{array}$$

Note  $\mathfrak{p} \cdot U^{-1}S$  is the extension of  $\mathfrak{p}$  along  $\rho \circ \varphi$ ,  $\mathfrak{p}S \cdot U^{-1}S$  is the extension of  $\mathfrak{p}S$  along  $\rho$ , and  $U^{-1}\mathfrak{p} \cdot U^{-1}S$  is the extension of  $U^{-1}\mathfrak{p}$  along  $U^{-1}\varphi$ .  $\mathcal{F}(\mathfrak{p})$  is fibre over  $\mathfrak{p}$  w.r.t.  $\varphi$ .

Let  $\frac{p}{u} \in U^{-1}\mathfrak{p}$  with  $p \in \mathfrak{p}$  and  $u \in U$ . Then  $\pi \circ (U^{-1}\varphi)(\frac{p}{u}) = \pi(\frac{\varphi(p)}{\varphi(u)}) = 0$  in  $\frac{\varphi(U)^{-1}S}{\varphi(U)^{-1}(\mathfrak{p}S)}$  since  $\varphi(p) \in \mathfrak{p}S$ . So by Construction 1.13,  $\overline{\pi \circ (U^{-1}\varphi)}$  is a well-defined ring homomorphism.

$$\begin{array}{ccc}
 U^{-1}R & \xrightarrow{\quad} & \frac{U^{-1}R}{U^{-1}\mathfrak{p}} \\
 \searrow \pi \circ (U^{-1}\varphi) & & \downarrow \overline{\pi \circ (U^{-1}\varphi)} \\
 & & \mathcal{F}(\mathfrak{p}) = \frac{\varphi(U)^{-1}S}{\varphi(U)^{-1}(\mathfrak{p}S)}
 \end{array}$$
  

$$\begin{array}{ccccc}
 & R & \xrightarrow{\quad \varphi \quad} & S & \\
 \psi \swarrow & & & & \searrow \epsilon \\
 U^{-1}R & \xrightarrow{\quad U^{-1}\varphi \quad} & U^{-1}S & & \\
 \tau \searrow & & \swarrow \pi & & \\
 & \frac{R}{\mathfrak{p}} & \xrightarrow{\quad \overline{\epsilon \circ \varphi} \quad} & \frac{S}{\mathfrak{p}S} & \\
 \swarrow \overline{\pi \circ \psi} & & \searrow \overline{\pi \circ \rho} & & \\
 \frac{U^{-1}R}{U^{-1}\mathfrak{p}} & \xrightarrow{\quad \overline{\pi \circ (U^{-1}\varphi)} \quad} & \frac{\varphi(U)^{-1}S}{\varphi(U)^{-1}(\mathfrak{p}S)} & & 
 \end{array}$$

Let  $\bar{r} \in \frac{R}{\mathfrak{p}}$  with  $r \in R$ . Then  $\overline{\pi \circ (U^{-1}\varphi)} \circ (\overline{\tau \circ \psi})(\bar{r}) = \overline{\pi \circ (U^{-1}\varphi)}(\overline{\tau \circ \psi}(r)) = \overline{\pi \circ (U^{-1}\varphi)}(\frac{r}{1}) = \pi \circ (U^{-1}\varphi)(\frac{r}{1}) = \frac{\varphi(r)}{\varphi(1)} = \frac{\varphi(r)}{1}$  and  $\overline{\pi \circ \rho} \circ \overline{\epsilon \circ \varphi}(\bar{r}) = \overline{\pi \circ \rho}(\overline{\epsilon \circ \varphi}(r)) = \overline{\pi \circ \rho}(\overline{\phi(r)}) = \pi \circ \rho(\phi(r)) = \frac{\varphi(1)}{1}$ . So the diagram on the bottom also commutes.

**Theorem 3.24.** Let  $\varphi^* : \text{Spec}(S) \rightarrow \text{Spec}(R)$  and  $U = R \setminus \mathfrak{p}$ . Then the following are equivalent.

- (i)  $\mathfrak{p} \in \text{Im}(\varphi^*)$ , i.e.,  $(\varphi^*)^{-1}(\mathfrak{p}) \neq \emptyset$ .
- (ii)  $\mathfrak{p} = \varphi^{-1}(\mathfrak{p}S)$ , where  $\mathfrak{p}S$  is not necessarily prime.
- (iii)  $\mathfrak{p} \cdot U^{-1}S \neq U^{-1}S$ , i.e.,  $\mathcal{F}(\mathfrak{p}) = \frac{U^{-1}S}{\mathfrak{p} \cdot U^{-1}S} \neq 0$ .

Moreover, the map  $\theta : \text{Spec}(\mathcal{F}(\mathfrak{p})) \rightarrow (\varphi^*)^{-1}(\mathfrak{p}) \subseteq \text{Spec}(S)$  given by  $\theta(Q) = \rho^{-1}(\pi^{-1}(Q))$  is a well-defined bijection, where  $(\varphi^*)^{-1}(\mathfrak{p})$  is the fibre over  $\mathfrak{p}$  w.r.t.  $\varphi^* : \text{Spec}(S) \rightarrow \text{Spec}(R)$ .

$$\begin{array}{ccc}
 R & \xrightarrow{\quad \varphi \quad} & S \\
 \downarrow \psi & & \downarrow \rho \\
 U^{-1}R & \xrightarrow{\quad} & U^{-1}S \\
 \downarrow \tau & & \downarrow \pi \\
 \frac{U^{-1}R}{\mathfrak{p} \cdot U^{-1}R} & \xrightarrow{\quad} & \frac{U^{-1}S}{\mathfrak{p} \cdot U^{-1}S}
 \end{array}$$

*Proof.* “(i) $\Rightarrow$ (ii)”. Assume there is  $\mathfrak{q} \in \text{Spec}(S)$  such that  $\mathfrak{p} = \varphi^{-1}(\mathfrak{q})$ . Then by Proposition 1.63(b),  $\mathfrak{p} = \varphi^{-1}(\mathfrak{q}) = \varphi^{-1}(\varphi^{-1}(\mathfrak{q})S) = \varphi^{-1}(\mathfrak{p}S)$ .

“(ii) $\Rightarrow$ (iii)”. Assume  $\mathfrak{p} = \varphi^{-1}(\mathfrak{p}S)$ . Note  $\mathfrak{p} \cdot U^{-1}S = \mathfrak{p}S \cdot U^{-1}S = \mathfrak{p}S \cdot \varphi(U)^{-1}S = \varphi(U)^{-1}(\mathfrak{p}S)$ . To show  $\varphi(U)^{-1}(\mathfrak{p}S) \neq \varphi(U)^{-1}S$ , it is equivalent to show  $\mathfrak{p}S \cap \varphi(U) = \emptyset$  by Proposition 3.13(c). Suppose  $\varphi(u) \in \mathfrak{p}S \cap \varphi(U)$  for some  $u \in U$ . Then  $u \in \varphi^{-1}(\mathfrak{p}S) = \mathfrak{p} = R \setminus U$ , a contradiction.

“(iii) $\Rightarrow$ (i) and well-definedness of  $\theta$ ”. It suffices to show  $\varphi^*(\theta(Q)) = \mathfrak{p}$ , i.e.,  $\varphi^{-1}(\rho^{-1}(\pi^{-1}(Q))) = \mathfrak{p}$  for  $Q \in \text{Spec}(\frac{U^{-1}S}{\mathfrak{p} \cdot U^{-1}S})$ . Let  $\mathfrak{q} := \pi^{-1}(Q) \in \text{Spec}(U^{-1}S)$ . Then by prime correspondence for quotients, we have  $\mathfrak{p} \cdot U^{-1}S \subseteq \pi^{-1}(Q) = \mathfrak{q}$  and  $Q = \frac{\mathfrak{q}}{\mathfrak{p} \cdot U^{-1}S}$ . Since  $\mathfrak{q} \in \text{Spec}(U^{-1}S)$ , by prime correspondence for localization  $\text{Spec}(U^{-1}S) \xrightarrow{\rho^{-1}} \text{Spec}(S)$ , for  $\mathfrak{r} := \rho^{-1}(\mathfrak{q}) = \rho^{-1}(\pi^{-1}(Q)) \in \text{Spec}(S)$  with  $\mathfrak{r} \cap \varphi(U) = \emptyset$ , we have  $\mathfrak{q} = \mathfrak{r} \cdot U^{-1}S = \mathfrak{r} \cdot \varphi(U)^{-1}S = \varphi(U)^{-1}\mathfrak{r}$ . So by Proposition 1.63(a),  $\mathfrak{p} \subseteq \varphi^{-1} \circ \rho^{-1}(\mathfrak{p} \cdot U^{-1}S) \subseteq \varphi^{-1}(\rho^{-1}(\pi^{-1}(Q))) = \varphi^{-1}(\mathfrak{r})$ . Suppose  $\mathfrak{p} \subsetneq \varphi^{-1}(\mathfrak{r})$ . Then there exists  $x \in \varphi^{-1}(\mathfrak{r})$  such that  $x \in R \setminus \mathfrak{p} = U$ . So  $\varphi(x) \in \mathfrak{r} \cap \varphi(U) = \emptyset$ , a contradiction. Thus,  $\mathfrak{p} = \varphi^{-1}(\mathfrak{r}) = \varphi^{-1}(\rho^{-1}(\pi^{-1}(Q)))$ .

By prime correspondence for quotients,  $\pi^*$  is 1-1 and by prime correspondence for localization,  $\rho^*$  is 1-1. Since  $\theta : \text{Spec}(\mathcal{F}(\mathfrak{p})) \xrightarrow{\pi^*} \mathbf{V}(\mathfrak{p} \cdot U^{-1}S) \xrightarrow{\rho^*|_{\text{restriction}}} (\varphi^*)^{-1}(\mathfrak{p})$ , we have  $\theta$  is the restriction of  $\rho^* \circ \pi^*$ . So  $\theta$  is 1-1.

Let  $\mathfrak{q} \in (\varphi^*)^{-1}(\mathfrak{p})$ . Then  $\mathfrak{q} \in \text{Spec}(S)$  such that  $\varphi^{-1}(\mathfrak{q}) = \mathfrak{p} \in \text{Spec}(R)$ . Since,  $\mathfrak{p} \cup U = \emptyset$ ,  $\mathfrak{q} \cap \varphi(U) = \emptyset$ . So  $\mathfrak{q} \cdot U^{-1}S = \mathfrak{q} \cdot \varphi(U)^{-1}S = \varphi(U)^{-1}\mathfrak{q} \in \text{Spec}(U^{-1}S)$  such that  $\rho^{-1}(\mathfrak{q} \cdot U^{-1}S) = \mathfrak{q}$ . Since  $\varphi^{-1}(\mathfrak{q}) = \mathfrak{p}$ , we have  $\mathfrak{p}S = \varphi^{-1}(\mathfrak{q})S \subseteq \mathfrak{q}$  by Proposition 1.63(a). So  $\mathfrak{p} \cdot U^{-1}S = \mathfrak{p}S \cdot U^{-1}S \subseteq \mathfrak{q} \cdot U^{-1}S$ . Hence by prime correspondence for quotients,  $\frac{\mathfrak{q} \cdot U^{-1}S}{\mathfrak{p} \cdot U^{-1}S} \in \text{Spec}(\frac{U^{-1}S}{\mathfrak{p} \cdot U^{-1}S})$  such that  $\pi^{-1}(\frac{\mathfrak{q} \cdot U^{-1}S}{\mathfrak{p} \cdot U^{-1}S}) = \mathfrak{q} \cdot U^{-1}S$ . So  $\theta(\frac{\mathfrak{q} \cdot U^{-1}S}{\mathfrak{p} \cdot U^{-1}S}) = \rho^{-1}(\pi^{-1}(\frac{\mathfrak{q} \cdot U^{-1}S}{\mathfrak{p} \cdot U^{-1}S})) = \rho^{-1}(\mathfrak{q} \cdot U^{-1}S) = \mathfrak{q}$ . Thus,  $\theta$  is onto.  $\square$

**Proposition 3.25.** If  $(R, \mathfrak{m})$  is local, then  $\mathcal{F}(\mathfrak{m}) \cong \frac{S}{\mathfrak{m} \cdot S}$ .

*Proof.* Since  $(R, \mathfrak{m})$  is local, we have  $U := R \setminus \mathfrak{m} = R^\times$  by Proposition 1.22. So  $U^{-1}(-) \cong -$ , e.g.,  $\mathcal{F}(\mathfrak{m}) = \frac{U^{-1}S}{\mathfrak{m} \cdot U^{-1}S} \cong \frac{S}{\mathfrak{m} \cdot S}$ .  $\square$

**Definition 3.26.** (a) If  $(R, \mathfrak{m})$  is local, then  $\mathcal{F}(\mathfrak{m}) \cong S/\mathfrak{m}S$  is the *closed fibre* of  $\varphi$  (fibre over unique closed point of  $\text{Spec}(R)$ ).

(b) If  $R$  is an integral domain, then  $\mathcal{F}(0)$  is the *generic fibre* of  $\varphi$  (fibre over the generic point of  $R$ ).

**Example 3.27.** (a) Let  $\varphi : R \xrightarrow{\subseteq} R[X_1, \dots, X_d]$ .

(1) If  $(R, \mathfrak{m})$  is local, then  $\mathcal{F}(\mathfrak{m}) \cong \frac{R[X_1, \dots, X_d]}{\mathfrak{m} \cdot R[X_1, \dots, X_d]} = \frac{R[X_1, \dots, X_d]}{\mathfrak{m}[X_1, \dots, X_d]} \cong \frac{R}{\mathfrak{m}}[X_1, \dots, X_d]$ .

(2) If  $\mathfrak{p} \in \text{Spec}(R)$ , then with  $U = R \setminus \mathfrak{p}$ , we have

$$\mathcal{F}(\mathfrak{p}) = \frac{U^{-1}(R[X_1, \dots, X_d])}{\mathfrak{p} \cdot U^{-1}(R[X_1, \dots, X_d])} \cong \frac{(U^{-1}R)[X_1, \dots, X_n]}{(\mathfrak{p}U^{-1}R)[X_1, \dots, X_n]} \cong \frac{R_{\mathfrak{p}}}{\mathfrak{p}_{\mathfrak{p}}}[X_1, \dots, X_n] \cong Q\left(\frac{R}{\mathfrak{p}}\right)[X_1, \dots, X_d]$$

since  $U^{-1}(R[X]) \cong (U^{-1}R)[X]$  defined by  $\frac{\sum_{i=1}^{\text{finite}} r_i x^i}{u} \mapsto \sum_{i=1}^{\text{finite}} \frac{r_i}{u} x^i$ .

(b) Let  $R \xrightarrow{\subseteq} R[[X_1, \dots, X_d]]$ .

(1) If  $(R, \mathfrak{m})$  is local, then  $\mathcal{F}(\mathfrak{m}) \cong \frac{R}{\mathfrak{m}}[[X_1, \dots, X_d]]$  similarly.

(c) Let  $k$  be a field and  $\varphi : k[X_1, \dots, X_d] \xrightarrow{\subseteq} k[[X_1, \dots, X_d]]$ .

(1) Let  $\mathfrak{m} = \langle X_1, \dots, X_d \rangle = k[X_1, \dots, X_d]$  be maximal. Then  $\mathfrak{m} \cdot k[[X_1, \dots, X_d]] = \langle X_1, \dots, X_d \rangle \leq k[[X_1, \dots, X_d]]$ . So with  $U = k[X_1, \dots, X_d] \setminus \mathfrak{m}$ ,  $\mathcal{F}(\mathfrak{m}) = \frac{U^{-1}(k[[X_1, \dots, X_d]])}{\mathfrak{m} \cdot U^{-1}(k[[X_1, \dots, X_d]])} \cong \frac{k[[X_1, \dots, X_d]]}{\mathfrak{m} \cdot k[[X_1, \dots, X_d]]} \cong \frac{k[[X_1, \dots, X_d]]}{\langle X_1, \dots, X_d \rangle} \cong k$  since  $U^{-1}(R[[X]]) \cong (U^{-1}R)[[X]]$  given by  $\frac{\sum_{i=1}^{\infty} r_i x^i}{u} \mapsto \sum_{i=1}^{\infty} \frac{r_i}{u} x^i$ .

(2)  $\mathcal{F}(0)$  is weird, which has chains of prime ideals of length  $d - 1$ .



# Chapter 4

## Primary Decomposition

Let  $R$  be a nonzero commutative ring with identity.

**Discussion 4.1.** UFD's have prime factorization. In fact, it is “if and only if”.

Alternative versions for non-UFD's.

(a) Irreducible factorizations:

<u>Pros</u>	<u>Cons</u>
familiar	don't necessarily exist

(b) Primary decompositions:

<u>Pros</u>	<u>Cons</u>
exist, e.g., if $R$ is noetherian, there exists more general form than just for principal ideal	replace factorizations of elements with intersections of nice ideals

**Theorem 4.2.** Let  $R$  be a noetherian integral domain and  $a \in R \setminus \{R^\times \cup 0\}$ .

(a)  $a$  has an irreducible factor in  $R$ .

(b) There exist irreducible  $b_1, \dots, b_n \in R$  such that  $a = b_1 \cdots b_n$ .

*Proof.* (a) Let  $\Sigma = \{\langle b \rangle \neq R : b \mid a\}$ . Since  $\langle a \rangle \in \Sigma$ ,  $\Sigma \neq \emptyset$ . Since  $R$  is noetherian,  $\Sigma$  has a maximal element, say  $\langle b \rangle$ . Claim.  $\langle b \rangle$  is irreducible. Since  $a \neq 0$  and  $b \mid a$ , we have  $b \neq 0$ . Since  $\langle b \rangle \neq R$ ,  $b \notin R^\times$ . Suppose  $b = cd$  for some  $c \in R \setminus R^\times$  and  $d \in R$ . Since  $c \mid b \mid a$ , we have  $c \mid a$ . Also, since  $c \notin R^\times$ ,  $\langle c \rangle \in \Sigma$ . Since  $\langle b \rangle \subseteq \langle c \rangle \subsetneq R$  and  $\langle b \rangle$  is maximal in  $\Sigma$ , we have  $\langle cd \rangle = \langle b \rangle = \langle c \rangle$ . Also, since  $R$  is an integral domain,  $d \in R^\times$ . So  $b$  is irreducible in  $R$ .

(b) If  $a$  is irreducible, then done. Else by (a) there exists  $b_1 \in R$  irreducible such that  $b_1 \mid a$  and  $a = b_1 a_1$  for some  $a_1 \in R$ . If  $a_1$  is irreducible, then done. Else by (a) there exists irreducible  $b_2 \in R$  such that  $b_2 \mid a_1$  and  $a_1 = b_2 a_2$  for some  $a_2 \in R$ . If  $a_2$  is irreducible, then done and we have  $\langle a \rangle \subsetneq \langle a_1 \rangle \subsetneq \langle a_2 \rangle$ . Since  $R$  is noetherian, by the ascending chain condition, the process will terminate in finite number of steps.  $\square$



**Example 4.3.** (a) Let  $k$  be a field and  $A = k[X^{\mathbb{R}_{\geq 0}}] := \{\sum_{i \in \mathbb{R}_{\geq 0}}^{\text{finite}} a_i X^i \mid a_i \in k\}$ . Let  $\mathfrak{m} = \langle X^{\mathbb{R}_{>0}} \rangle \leq A$ . Then  $\mathfrak{m} \in \text{m-Spec}(R)$  and  $A/\mathfrak{m} \cong k$ . Let  $R = A_{\mathfrak{m}}$ . Then  $A \setminus \mathfrak{m} \subseteq R^\times$ . Since  $X$  has no irreducible factors in  $R$ ,  $X$  has no irreducible factorization. Let  $r \in R \setminus \{R^\times \cup 0\}$ . Then  $r = X^\epsilon \cdot f$  for some  $\epsilon > 0$  and  $f \in R \setminus \{0\}$ . Since  $X^\epsilon \cdot f = X^{\frac{\epsilon}{2}} \cdot X^{\frac{\epsilon}{2}} \cdot f$ . So  $r$  is not irreducible in  $R$ . Thus,  $R$  has no irreducible elements.

(b) In  $\mathbb{Z}_6$ , we have  $3^2 = 3$ ,  $2^2 = 4$ ,  $2^3 = 2$ .

**Definition 4.4.** If  $R$  satisfies the condition of Theorem 4.2(b), then  $R$  is *atomic*.

**Lemma 4.5** (Nakayama's Lemma). Let  $I, J \leq R$  such that  $I \subseteq \text{Jac}(R)$  and  $J$  is finitely generated. If  $J = IJ$ , then  $J = 0$ .

*Proof.* Let  $n$  be the minimum number of generators of  $J$ . Suppose  $n \geq 2$ . Since  $J$  is finitely generated,  $IJ = J = \langle x_1, \dots, x_n \rangle$  for some  $x_1, \dots, x_n \in J$ . So  $x_n \in IJ$  and then  $x_n = \sum_{i=1}^n a_i x_i$  for some  $a_1, \dots, a_n \in I$ , i.e.,  $x_n(1 - a_n) = \sum_{i=1}^{n-1} a_i x_i$ . Since  $a_n \in I \subseteq \text{Jac}(R)$ ,  $1 - a_n \in R^\times$  by Proposition 1.29. So  $x_n \in \langle x_1, \dots, x_{n-1} \rangle$ , contradicting minimality of  $n$ . Hence  $n = 1$  or  $0$ . If  $n = 1$ , similarly, we have  $x_1(1 - a_1) = 0$  for some  $a_1 \in I$  with  $1 - a_1 \in R^\times$ , so  $x_1 = 0$ , a contradiction. Thus,  $n = 0$ .  $\square$

**Lemma 4.6.** Let  $(R, \mathfrak{m})$  be local and  $0 \neq b = cd$  with  $b, c, d \in R$  such that  $\langle b \rangle = \langle c \rangle$ . Then  $d \in R^\times$ .

*Proof.* Since  $b = cd$  and  $\langle b \rangle = \langle c \rangle$ , we have  $\langle c \rangle = \langle b \rangle = \langle cd \rangle = \langle d \rangle \langle c \rangle$ . Suppose  $d \notin R^\times$ . Then  $\langle d \rangle \subseteq \mathfrak{m} = \text{Jac}(R)$ . So by Lemma 4.5,  $c = 0$ . Hence  $b = cd = 0$ , a contradiction. Thus,  $d \in R^\times$ .  $\square$

**Theorem 4.7.** Let  $(R, \mathfrak{m})$  be local and noetherian. Let  $a \in R \setminus \{R^\times \cup 0\}$ .

(a)  $a$  has an irreducible factor in  $R$ .

(b)  $a = b_1 \cdots b_n$  for some irreducible elements  $b_1, \dots, b_n \in R$ .

*Proof.* It is similar to the proof of Theorem 4.2.  $\square$

**Discussion 4.8.** Let  $R$  be noetherian and (local or a domain). Let  $a \in R \setminus \{R^\times \cup 0\}$  with irreducible factorization  $a = b_1 \cdots b_n$ . Then  $V(a) = V(b_1 \cdots b_n) = V(b_1) \cup \cdots \cup V(b_n)$ , which are not necessarily an irreducible decomposition.

**Example 4.9.** Let  $R = \frac{k[X, Y, Z]_{(X, Y, Z)}}{(X^2 - YZ)} \cong \frac{k[X, Y, Z]_{(X, Y, Z)}}{(X^2 - YZ)} \cong \left( \frac{k[X, Y, Z]}{(X^2 - YZ)} \right)_{(X, Y, Z)}$  or  $R = \frac{k[X, Y, Z]}{(X^2 - YZ)}$ . Since  $X^2 - YZ \in k[Y, Z][X]$  and  $Y$  is prime (irreducible) in  $k[Y, Z][X]$ , by Eisenstein's Criterion,  $X^2 - YZ$  is irreducible in  $k[X, Y, Z]$ . Since  $(k[X, Y, Z], \langle X, Y, Z \rangle)$  is local,  $\frac{k[X, Y, Z]}{(X^2 - YZ)}$  is local. So  $R$  is a local, noetherian and integral domain. Let  $x = \bar{X} \in R$ , which is irreducible. Let  $y = \bar{Y}, z = \bar{Z} \in R$ . Since  $(x, z) \in V(x) \setminus V(y)$  and  $(x, y) \in V(x) \setminus V(z)$ ,  $V(x) \neq V(y)$  and  $V(x) \neq V(z)$ . Also, since  $V(x) = V(x^2) = V(yz) = V(y) \cup V(z)$ , we have  $V(x)$  is not irreducible in  $\text{Spec}(R)$ .

Primary decomposition does the job.

**Definition 4.10.** An ideal  $\mathfrak{q} \leq R$  is *primary* if  $xy \in \mathfrak{q}$  with  $x, y \in R$ , then  $x \in \mathfrak{q}$  or  $y \in \text{rad}(\mathfrak{q})$ , i.e., if  $\bar{x}\bar{y} = 0$  with  $\bar{x}, \bar{y} \in R/\mathfrak{q}$ , then  $\bar{x} = 0$  or  $\bar{y} \in \text{Nil}(R/\mathfrak{q})$ , i.e., if  $xy \in \mathfrak{q}$  with  $x, y \in R$ , then  $x \in \mathfrak{q}$  or  $y \in \mathfrak{q}$  or  $x, y \in \text{rad}(\mathfrak{q})$ , i.e., if  $\text{Nil}(A/\mathfrak{q}) = \text{ZD}(A/\mathfrak{q})$ .

**Example 4.11.** We have the following examples.

(a) If  $\mathfrak{p} \in \text{Spec}(R)$ , then  $\mathfrak{p}$  is primary since  $\text{rad}(\mathfrak{p}) = \mathfrak{p}$ .

(b) If  $\mathfrak{m} \in \text{Spec}(R)$  and  $\mathfrak{q} \leq R$  such that  $\mathfrak{m}^n \subseteq \mathfrak{q} \subseteq \mathfrak{m}$  for some  $n \geq 1$ , then  $\mathfrak{q}$  is primary. In particular,  $\mathfrak{m}^n$  is primary for  $n \geq 1$ .

*Proof.* Let  $xy \in \mathfrak{q} \subseteq \mathfrak{m}$  with  $x, y \in R$ . Assume  $y \notin \text{rad}(\mathfrak{q})$ . Since  $\text{rad}(\mathfrak{m}) = \text{rad}(\mathfrak{m}^n) \subseteq \text{rad}(\mathfrak{q}) \subseteq \text{rad}(\mathfrak{m})$ , we have  $\text{rad}(\mathfrak{q}) = \text{rad}(\mathfrak{m}) = \mathfrak{m} \in \text{m-Spec}(R)$ . So  $\langle y, \mathfrak{m} \rangle = R$ . As in Proposition 1.46(b), we can show  $\langle y, \mathfrak{m}^n \rangle = R$  by Proposition 1.39(a). So  $1 = zy + \alpha$  for some  $z \in R$  and  $\alpha \in \mathfrak{m}^n \subseteq \mathfrak{q}$ . Also, since  $xy \in \mathfrak{q}$ ,  $x = x(zy + \alpha) = (xy)z + x\alpha \in \mathfrak{q}$ .  $\square$

(c) Proof of (b) shows that if  $\mathfrak{q} \leq R$  such that  $\text{rad}(\mathfrak{q}) = \mathfrak{m} \in \text{m-Spec}(R)$ , then  $\mathfrak{q}$  is primary.

Alternating proof of (b). Let  $\bar{x}, \bar{y} \in \bar{R} := R/\mathfrak{q}$  such that  $\bar{x}\bar{y} = 0$ . Let  $\mathfrak{p}/\mathfrak{q} \in \text{Spec}(\bar{R})$  with  $\mathfrak{p} \in \text{Spec}(R)$  such that  $\mathfrak{p} \supseteq \mathfrak{q} \supseteq \mathfrak{m}^n$ . Then  $R \supsetneq \mathfrak{p} = \text{rad}(\mathfrak{p}) \supseteq \text{rad}(\mathfrak{q}) \supseteq \text{rad}(\mathfrak{m}^n) = \mathfrak{m} \in \text{Spec}(R)$ . So  $\mathfrak{p} = \mathfrak{m}$ . Hence  $\text{Spec}(\bar{R}) = \{\mathfrak{m}/\mathfrak{q}\}$ . So  $(\bar{R}, \mathfrak{m}/\mathfrak{q})$  is local. If  $\bar{y} \in \mathfrak{m}/\mathfrak{q} = \text{Nil}(R/\mathfrak{q})$  by Proposition 1.26(d), done. Assume now  $\bar{y} \notin \text{Nil}(R/\mathfrak{q}) = \mathfrak{m}/\mathfrak{q}$ . Then  $\bar{y} \in \bar{R}^\times$  by Proposition 1.22. Also, since  $\bar{x}\bar{y} = 0$  in  $\bar{R}$ ,  $\bar{x} = 0$ .

(d) Let  $p \in \mathbb{Z}$  be prime. Then  $\langle p \rangle$  is maximal and so  $\langle p^n \rangle$  is primary by (b).

**Example 4.12.** We have the following examples.

(a) If  $R$  is a UFD and  $p \in R$  is prime, then  $\langle p^n \rangle$  is primary.

(b) Let  $R = \frac{k[X, Y, Z]}{\langle X^2 - YZ \rangle}$  and  $x = \bar{X} \in R$ . Then  $x$  is irreducible. Note  $R/\langle x \rangle = \frac{k[X, Y, Z]}{\langle X^2 - YZ \rangle} / \langle x \rangle \cong \frac{k[X, Y, Z]}{\langle X, X^2 - YZ \rangle} = \frac{k[X, Y, Z]}{\langle X, YZ \rangle} \cong \frac{k[Y, Z]}{\langle YZ \rangle}$ . Let  $y = \bar{Y}, z = \bar{Z} \in \frac{k[Y, Z]}{\langle YZ \rangle}$ . Then  $yz = 0$  with  $y, z \neq 0$ . So  $y, z \notin (0) = \text{rad}(0) = \text{Nil}(R/\langle x \rangle)$ . Thus,  $\langle x \rangle$  is not primary.

(c) Let  $R = k[X_1, \dots, X_d]$ . Then  $I = \langle X_1^{e_1}, \dots, X_n^{e_n} \rangle$  with  $e_1, \dots, e_n \geq 1$  is primary.

Let  $J = \langle X_1^{e_1}, \dots, X_d^{e_d}, f_1, \dots, f_n \rangle \leq R$  with  $e_1, \dots, e_d \geq 1$  and  $f_1, \dots, f_n \in R \setminus R^\times$ . Since  $\text{rad}(J) = \langle X_1, \dots, X_d \rangle \in \text{m-Spec}(R)$ , by Example 4.11(c), we have  $J$  is primary.

(d) Let  $R = k[X, Y, Z]$  and  $I = \langle X^2, XY \rangle$ . Then  $\text{rad}(I) = \langle X \rangle$ . Since  $XY \in I$  with  $X \notin I$  and  $Y \notin \text{rad}(I)$ ,  $I$  is not primary.

Let  $J = \langle X, YZ \rangle$ . Then  $R/J = \frac{k[X, Y, Z]}{\langle X, YZ \rangle} \cong \frac{k[Y, Z]}{\langle YZ \rangle}$ . So similar to (b), we have  $J$  is not primary.

*Proof.* (a) Let  $xy \in \langle p^n \rangle$  with  $x, y \in R$ . If  $y \in \text{rad}(\langle p^n \rangle) = \langle p \rangle$ , then done. Assume  $y \notin \langle p \rangle$ . Then  $p \nmid y$ . Since  $xy \in \langle p^n \rangle$ ,  $p^n \mid xy$ . Since  $xy$  has a unique factorization and  $p \nmid y$ ,  $p^n \mid x$ , i.e.,  $x \in \langle p^n \rangle$ .

(c) Assume by symmetry  $I = \langle X_1^{e_1}, \dots, X_n^{e_n} \rangle$ . Let  $f, g \in R$  such that  $fg \in I$ . If  $f \in I$ , then done. Assume  $f \notin I$ . Let  $f = \sum_{i=1}^s a_i f_i$  for some  $s \geq 1$ ,  $a_i \in R \setminus \{0\}$  and  $f_i \in R$  monomial for  $i = 1, \dots, s$  and  $g = \sum_{i=1}^t b_i g_i$  for some  $t \geq 1$ ,  $b_i \in R \setminus \{0\}$  and  $g_i \in R$  monomial for  $i = 1, \dots, t$ . Since  $f \notin I$ ,  $f_i \notin I$  for some  $i \in \{1, \dots, s\}$ . Let  $f = \tilde{f} + \hat{f}$ , where  $\hat{f}$  are all monomials in  $I$  and  $\tilde{f}$  are all monomials not in  $I$ . Since  $\tilde{f}g + \hat{f}g \in I = fg \in I$  and  $\hat{f}g \in I$ ,  $\tilde{f}g \in I$ . Use a monomial ordering, e.g. lexicographical order, assume  $f_s$  is the largest monomial occurring in  $\tilde{f}$  and  $g_t$  is the largest monomial occurring in  $g$ . Then  $f_s g_t$  is the largest monomial occurring in  $\tilde{f}g \in I$ . So  $f_s g_t \in I$ . Since the monomial  $f_s \notin I$ ,  $X_i^{e_i} \nmid f_s$  for  $i = 1, \dots, n$ . So  $g_t$  is not a constant in  $R$  and hence  $X_j \mid g_t$  for some  $j \in \{1, \dots, n\}$ . Then  $g_t \in \langle X_1, \dots, X_n \rangle = \text{rad}(\langle X_1^{e_1}, \dots, X_n^{e_n} \rangle) = \text{rad}(I)$ . So  $g = \sum_{i=1}^{t-1} b_i g_i + b_t g_t$  with  $b_t g_t \in \text{rad}(I)$ . Induct on  $t$ , we have  $b_i g_i \in \text{rad}(I)$  for all  $i = 1, \dots, t$ . Thus,  $g \in \text{rad}(I)$ .  $\square$

Let  $\mathfrak{a} \leq R$ .

**Definition 4.13.**  $\mathfrak{a}$  is *reducible* if  $\mathfrak{a} = I \cap J$  for some  $I, J \leq R$  with  $I \neq \mathfrak{a}$  and  $J \neq \mathfrak{a}$ .

$\mathfrak{a}$  is *irreducible* if it is not reducible, i.e., if  $\mathfrak{a} = I \cap J$  for some  $I, J \leq R$ , then  $I = \mathfrak{a}$  or  $J = \mathfrak{a}$ .

**Example 4.14.** (a) If  $\mathfrak{p} \in \text{Spec}(R)$ , then  $\mathfrak{p}$  is irreducible.

(b) If  $\mathfrak{a}$  is primary in  $R$ , then  $\mathfrak{a}$  may not be irreducible.

*Proof.* (a) Assume  $\mathfrak{p} = I \cap J$  for some  $I, J \leq R$ . Then  $\mathfrak{p} = I \cap J \supseteq IJ$  by Fact 1.38(f). Since  $\mathfrak{p} \in \text{Spec}(R)$ ,  $\mathfrak{p} \supseteq I$  or  $\mathfrak{p} \supseteq J$ . So  $I \supseteq I \cap J = \mathfrak{p} \supseteq I$  or  $J \supseteq I \cap J = \mathfrak{p} \supseteq J$ . Hence  $\mathfrak{p} = I$  or  $\mathfrak{p} = J$ .

(b) Counterexample. In  $R = k[X, Y]$ , let  $\mathfrak{a} = \langle X^2, XY, Y^2 \rangle$ , then by Example 4.11(c),  $\mathfrak{a}$  is primary since  $\text{rad}(\mathfrak{a}) = \langle X, Y \rangle \in \text{m-Spec}(R)$ , but  $\mathfrak{a}$  is not irreducible since  $\mathfrak{a} = \langle X, Y^2 \rangle \cap \langle X^2, Y \rangle$ .  $\square$

**Proposition 4.15.** Let  $R$  be noetherian. If  $\mathfrak{a}$  is irreducible, then  $\mathfrak{a}$  is primary.

*Proof.* Case 1. Assume  $\mathfrak{a} = 0$ . Let  $x, y \in R$  such that  $xy = 0$ . If  $x = 0$ , then done. Assume  $x \neq 0$ . Note  $(0 : y) \subseteq (0 : y^2) \subseteq (0 : y^3) \subseteq \dots$ . Since  $R$  is noetherian,  $(0 : y^n) = (0 : y^{n+1})$  for some  $n \geq 1$ . Let  $z \in \langle x \rangle \cap \langle y^n \rangle$ . Then  $xs = z = y^nt$  for some  $s \in R$  and  $t \in R$ . So  $y^{n+1}t = xys = 0$ , i.e.,  $t \in (0 : y^{n+1}) = (0 : y^n)$ . Hence  $z = y^nt = 0$ . So  $\langle x \rangle \cap \langle y^n \rangle = 0 = \mathfrak{a}$ . Also, since  $\mathfrak{a}$  is irreducible and  $\langle x \rangle \neq 0$ , we have  $\langle y^n \rangle = 0$ , i.e.,  $y^n = 0$ . So  $y \in \text{rad}(0) = \text{rad}(\mathfrak{a})$ . Thus,  $\mathfrak{a}$  is primary.

Case 2. Assume  $\mathfrak{a}$  is arbitrary. To show  $\mathfrak{a}$  is primary, by Case 1 it suffices to show  $(0) \leq R/\mathfrak{a}$  is irreducible. Let  $I, J \leq R/\mathfrak{a}$  such that  $0 = I \cap J = \frac{\tilde{I}}{\mathfrak{a}} \cap \frac{\tilde{J}}{\mathfrak{a}} = \frac{\tilde{I} \cap \tilde{J}}{\mathfrak{a}}$  for some  $\tilde{I}, \tilde{J} \leq R$  ( $\mathfrak{a} \leq \tilde{I} \cap \tilde{J}$ ). So  $\tilde{I} \cap \tilde{J} = \mathfrak{a}$ . Also, since  $\mathfrak{a}$  is irreducible,  $\tilde{I} = \mathfrak{a}$  or  $\tilde{J} = \mathfrak{a}$ . So  $I = \frac{\tilde{I}}{\mathfrak{a}} = 0$  or  $J = \frac{\tilde{J}}{\mathfrak{a}} = 0$ .  $\square$

**Definition 4.16.** A *primary decomposition* of  $\mathfrak{a}$  is  $\mathfrak{a} = \bigcap_{i=1}^n J_i$  such that  $J_1, \dots, J_n$  are primary.

**Theorem 4.17** (Noether). Assume  $R$  is noetherian. Then  $\mathfrak{a}$  has a primary decomposition.

*Proof.* It suffices to show  $\mathfrak{a} = \bigcap_{i=1}^n J_i$  for some  $n \geq 1$  such that  $J_i$  is irreducible for  $i = 1, \dots, n$ . Suppose not. Let  $\Sigma = \{\mathfrak{b} \leq R \mid \mathfrak{b} \text{ does not have a irreducible decomposition}\}$ . Since  $\mathfrak{a} \in \Sigma$ ,  $\Sigma \neq \emptyset$ . Since  $R$  is noetherian,  $\Sigma$  has a maximal element, say  $\mathfrak{q}$ . Then  $\mathfrak{q} = I \cap J$  for some  $\mathfrak{q} \subsetneq I, J \leq R$ . Since  $\mathfrak{q}$  is maximal, we have  $I, J \notin \Sigma$ . So there exists  $m \geq n \geq 1$  and irreducible  $J_1, \dots, J_m \leq R$  such that  $I = \bigcap_{i=1}^m J_i$  and  $J = \bigcap_{i=n+1}^m J_i$ . Thus,  $\mathfrak{q} = I \cap J = \bigcap_{i=1}^m J_i$ , contradicting  $\mathfrak{q} \in \Sigma$ .  $\square$

**Example 4.18.** We have the following examples.

(a) Let  $R$  be a UFD and  $a \in R \setminus \{R^\times \cup 0\}$  has a prime factorization  $a = up_1^{e_1} \dots p_n^{e_n}$  with  $u \in R^\times$ ,  $e_i \geq 1$  and  $p_i \nmid p_j$  for  $1 \leq i, j \leq n$  with  $i \neq j$ . Then  $\langle a \rangle = \bigcap_{i=1}^n \langle p_i^{e_i} \rangle$ , a primary decomposition by Example 4.12(a).

(b) Let  $R = k[X_1, \dots, X_d]$  and  $\mathfrak{a}$  be an monomial ideal with an m-irreducible decomposition  $\mathfrak{a} = \bigcap_{i=1}^n J_i$  with  $J_1, \dots, J_n$  generated by pure power of variables. So  $\mathfrak{a} = \bigcap_{i=1}^n J_i$  is a primary decomposition by Example 4.12(c). Moreover, it is an irreducible decomposition.

(c) Let  $R = k[X_1, \dots, X_d]$  and  $\mathfrak{a}$  be an monomial ideal with an m-irreducible decomposition  $\mathfrak{a} = \bigcap_{i=1}^n J_i$ . Then  $\mathfrak{a}$  is primary if and only if  $\text{rad}(J_i) = \text{rad}(J_j)$  for  $1 \leq i, j \leq n$ .

*Proof.* (c) “ $\Leftarrow$ ”. Assume  $\text{rad}(J_i) = \text{rad}(J_j)$  for  $1 \leq i, j \leq n$ . Let  $xy \in \mathfrak{a}$  with  $x, y \in R$ . If  $y \in \text{rad}(\mathfrak{a})$ , done. Assume  $y \notin \text{rad}(\mathfrak{a})^\dagger = \text{rad}(\bigcap_{i=1}^n J_i) = \bigcap_{i=1}^n \text{rad}(J_i) = \text{rad}(J_i)$  for  $i = 1, \dots, n$  by Fact 1.58(d). Since  $R$  is noetherian and  $J_i$  is irreducible,  $J_i$  is primary for  $i = 1, \dots, n$ . Also, since  $xy \in \mathfrak{a} \subseteq J_i$  for  $i = 1, \dots, n$ , we have  $x \in J_i$  for  $i = 1, \dots, n$ . So  $x \in \bigcap_{i=1}^n J_i = \mathfrak{a}$ .

“ $\Rightarrow$ ”. Assume  $\mathfrak{a}$  is primary. Induct on  $n$ . The base case  $n = 2$  is the important case. Suppose  $\text{rad}(J_1) \neq \text{rad}(J_2)$ . Then we have there exist  $a \in \text{rad}(J_1) \setminus \text{rad}(J_2)$  and  $b \in \text{rad}(J_2) \setminus \text{rad}(J_1)$ . So  $a, b \notin \text{rad}(J_1) \cap \text{rad}(J_2) = \text{rad}(J_1 \cap J_2) = \text{rad}(\mathfrak{a})$  and  $ab \in \text{rad}(J_1) \cap \text{rad}(J_2) = \text{rad}(\mathfrak{a})$ , contradicting  $\text{rad}(\mathfrak{a}) \in \text{Spec}(R)$  by Proposition 4.19.  $\square$

**Proposition 4.19.** If  $\mathfrak{q} \leq R$  is primary, then  $\text{rad}(\mathfrak{q}) \in \text{Spec}(R)$ . In particular,  $\text{rad}(\mathfrak{q})$  is the unique smallest prime ideal of  $R$  containing  $\mathfrak{q}$ .

*Proof.* Since  $\mathfrak{q} \leq R$ ,  $\text{rad}(\mathfrak{q}) \leq R$ . Let  $xy \in \text{rad}(\mathfrak{q})$  with  $x, y \in R$ . Then  $x^m y^m = (xy)^m \in \mathfrak{q}$  for some  $m \geq 1$ . Since  $\mathfrak{q}$  is primary,  $x^m \in \mathfrak{q}$  or  $y^m \in \text{rad}(\mathfrak{q})$ . So  $x \in \text{rad}(\mathfrak{q})$  or  $y \in \text{rad}(\text{rad}(\mathfrak{q})) = \text{rad}(\mathfrak{q})$  by Fact 1.58(c). Hence  $\text{rad}(\mathfrak{q}) \in \text{Spec}(R)$ . The minimality follows from the definition of prime ideal and equivalent definition of primary ideal.  $\square$

**Definition 4.20.** If  $\mathfrak{q} \leq R$  is primary and  $\mathfrak{p} = \text{rad}(\mathfrak{q})$ , then  $\mathfrak{q}$  is  $\mathfrak{p}$ -primary.

**Example 4.21.** (a) Let  $p \in \mathbb{Z}$  be prime. Then  $\mathfrak{q} = \langle p^n \rangle$  is primary with  $\text{rad}(\mathfrak{q}) = \langle p \rangle \in \text{Spec}(\mathbb{Z})$  for  $n \geq 1$ .

(b) Let  $\mathfrak{m} \in \text{m-Spec}(R)$  and  $\mathfrak{q} \leq R$  such that  $\mathfrak{m}^n \subseteq \mathfrak{q} \subseteq \mathfrak{m}$  for some  $n \geq 1$ . Then  $\mathfrak{q}$  is primary with  $\text{rad}(\mathfrak{q}) = \mathfrak{m} \in \text{Spec}(R)$  by the proof of Example 4.11(b).

(c) Let  $R = k[X_1, \dots, X_d]$  and  $\mathfrak{q} = \langle X_{i_1}^{e_1}, \dots, X_{i_n}^{e_n} \rangle$  with  $e_1, \dots, e_n \geq 1$ . Then  $\mathfrak{q}$  is primary with  $\text{rad}(\mathfrak{q}) = \langle X_{i_1}, \dots, X_{i_n} \rangle \in \text{Spec}(R)$ .

**Proposition 4.22.** Let  $\mathfrak{q}_1, \dots, \mathfrak{q}_n \leq R$  be  $\mathfrak{p}$ -primary. Then  $\bigcap_{i=1}^n \mathfrak{q}_i$  is  $\mathfrak{p}$ -primary.

*Proof.* It is similar to the proof of Example 4.18(c).  $\square$

**Definition 4.23.** A primary decomposition  $\mathfrak{a} = \bigcap_{i=1}^n \mathfrak{q}_i$  is *minimal* if

- (a)  $\text{rad}(\mathfrak{q}_i) \neq \text{rad}(\mathfrak{q}_j)$  for  $1 \leq i, j \leq n$  with  $i \neq j$ ,
- (b)  $\bigcap_{i=1, i \neq j}^n \mathfrak{q}_i \not\subseteq \mathfrak{q}_j$ , i.e.,  $\mathfrak{a} \subsetneq \bigcap_{i=1, i \neq j}^n \mathfrak{q}_i$  for  $j = 1, \dots, n$ .

**Example 4.24.** (a) Let  $n \in \mathbb{Z}$  and  $n = p_1^{e_1} \cdots p_m^{e_m}$  such that  $p_1, \dots, p_m$  are distinct primes and  $e_1, \dots, e_m \geq 1$ . Then the primary decomposition  $\langle n \rangle = \bigcap_{i=1}^m \langle p_i^{e_i} \rangle$  is minimal.

(b) Let  $R = k[X, Y]$ . Then  $\langle X^2, XY \rangle = \langle X^2, Y \rangle \cap \langle X \rangle = \langle X^2, XY, Y^2 \rangle \cap \langle X \rangle$  are two minimal primary decompositions.

**Notice:** minimal primary decomposition is not necessarily unique up to re-ordering.

**Definition 4.25.** Let  $\mathfrak{a} = \bigcap_{i=1}^n \mathfrak{q}_i$  be a minimal primary decomposition such that  $\text{rad}(\mathfrak{q}_i) = \mathfrak{p}_i$  for  $i = 1, \dots, n$ .

---

<sup>†</sup>Not try to assume  $x \notin \mathfrak{a}$ .

(a) The *associated primes* of  $\mathfrak{a}$  are  $\mathfrak{p}_1, \dots, \mathfrak{p}_n$ . Write it as

$$\text{Ass}_R(\mathfrak{a}) = \{\mathfrak{p}_1, \dots, \mathfrak{p}_n\}.$$

(b) The *minimal (associated) primes* of  $\mathfrak{a}$  are the minimal elements of  $\{\mathfrak{p}_1, \dots, \mathfrak{p}_n\}$  w.r.t.  $\subseteq$ . Write it as

$$\text{Min}(\mathfrak{a}) = \min\{\text{Ass}_R(\mathfrak{a})\} = \min\{\mathfrak{p}_1, \dots, \mathfrak{p}_n\}.$$

(c) The *embedded primes* of  $\mathfrak{a}$  are the non-minimal associated primes of  $\mathfrak{a}$ , i.e.,  $\text{Ass}_R(\mathfrak{a}) \setminus \text{Min}(\mathfrak{a})$ .

**Example 4.26.** Let  $R = k[X, Y]$  and  $\mathfrak{a} = \langle X^2, XY \rangle$ . Then  $\text{Ass}_R(\mathfrak{a}) = \{\langle X \rangle, \langle X, Y \rangle\}$ ,  $\text{Min}(\mathfrak{a}) = \{\langle X \rangle\}$  and the embedded prime(s) of  $\mathfrak{a}$  is  $\{\langle X, Y \rangle\}$ .

**Goals:**  $\text{Ass}_R(\mathfrak{a})$  is independent of the minimal primary decomposition, so  $\text{Min}(\mathfrak{a})$  is also independent of the minimal primary decomposition.  $\text{Ass}_R(\mathfrak{a}) = \text{Ass}_R(R/\mathfrak{a})^\dagger$  if  $R$  is noetherian.

**Proposition 4.27.** If  $\mathfrak{a}$  has a primary decomposition, then  $\mathfrak{a}$  has a minimal primary decomposition.

*Proof.* Let  $\mathfrak{a} = \bigcap_{i=1}^n \mathfrak{q}_i$  be a primary decomposition. If  $\text{rad}(\mathfrak{q}_i) = \text{rad}(\mathfrak{q}_j)$  for some  $i, j \in \{1, \dots, n\}$  with  $i \neq j$ , then  $\mathfrak{q}_i \cap \mathfrak{q}_j$  is  $\mathfrak{p}$ -primary where  $\mathfrak{p} := \text{rad}(\mathfrak{q}_i)$  by Proposition 4.22, so combine  $\mathfrak{q}_i$  and  $\mathfrak{q}_j$  to get a new shorter decomposition, this process terminates in at most  $n$  steps. Then without loss of generality, assume  $\mathfrak{p}_i = \text{rad}(\mathfrak{q}_i) \neq \text{rad}(\mathfrak{q}_j) = \mathfrak{p}_j$  for  $1 \leq i, j \leq n$  with  $i \neq j$ . If  $\bigcap_{i=1, i \neq j}^n \mathfrak{p}_i \subseteq \mathfrak{q}_j$  for some  $j \in \{1, \dots, n\}$ , then  $\mathfrak{a} = \bigcap_{i=1}^n \mathfrak{q}_i = \bigcap_{i=1, i \neq j}^n \mathfrak{q}_i$ , so  $\bigcap_{i=1, i \neq j}^n \mathfrak{q}_i$  is a shorter decomposition, the process terminates in at most  $n$  steps.  $\square$

Let  $\mathfrak{a} = \bigcap_{i=1}^n \mathfrak{q}_i$  be a minimal primary decomposition such that  $\text{rad}(\mathfrak{q}_i) = \mathfrak{p}_i$  for  $i = 1, \dots, n$ .

**Proposition 4.28.** Re-order the  $\mathfrak{q}_i$ 's if necessary to assume without loss of generality,  $\text{Min}(\mathfrak{a}) = \{\mathfrak{p}_1, \dots, \mathfrak{p}_m\}$ . Then the irreducible components of  $V(\mathfrak{a})$  with subspace topology are  $V(\mathfrak{p}_1), \dots, V(\mathfrak{p}_m)$ .

*Proof.* Claim.  $\text{Min}(V(\mathfrak{a})) = \{\mathfrak{p}_1, \dots, \mathfrak{p}_m\}$ . Then  $V(\mathfrak{p}_1), \dots, V(\mathfrak{p}_m)$  are all maximal irreducible subset of  $V(\mathfrak{a})$  by Proposition 2.42.

“ $\subseteq$ ”. Let  $\mathfrak{p} \in \text{Min}(V(\mathfrak{a}))$ . Then  $\mathfrak{p} \supseteq \mathfrak{a} = \bigcap_{i=1}^n \mathfrak{q}_i$ . So  $\mathfrak{p} \supseteq \text{rad}(\mathfrak{a}) = \text{rad}(\bigcap_{i=1}^n \mathfrak{q}_i) = \bigcap_{i=1}^n \text{rad}(\mathfrak{q}_i) = \bigcap_{i=1}^n \mathfrak{p}_i = \bigcap_{j=1}^m \mathfrak{p}_j$  since there exists  $j_i \in \{1, \dots, m\}$  such that  $\mathfrak{p}_{j_i} \subseteq \mathfrak{p}_i$  for  $i = m+1, \dots, n$ . Since  $\mathfrak{p} \in \text{Spec}(R)$ ,  $\mathfrak{p} \supseteq \mathfrak{p}_k \supseteq \bigcap_{j=1}^m \mathfrak{p}_j = \text{rad}(\mathfrak{a}) \supseteq \mathfrak{a}$  for some  $k \in \{1, \dots, m\}$ . Also, since  $\mathfrak{p}_k \in \text{Spec}(R)$  by Proposition 4.19 and  $\mathfrak{p} \in \text{Min}(V(\mathfrak{a}))$ , we have  $\mathfrak{p} = \mathfrak{p}_k$ .

“ $\supseteq$ ”. Fix  $j \in \{1, \dots, m\}$ . Suppose there exists  $\mathfrak{p} \in \text{Spec}(R)$  such that  $\mathfrak{a} \subseteq \mathfrak{p} \subsetneq \mathfrak{p}_j$ . Then  $\mathfrak{a}R_{\mathfrak{p}_j} \subseteq \mathfrak{p}R_{\mathfrak{p}_j} \subsetneq \mathfrak{p}_jR_{\mathfrak{p}_j}$  by prime correspondence for localization. For  $i = 1, \dots, m$  with  $i \neq j$ , since  $\mathfrak{p}_i \not\subseteq \mathfrak{p}_j$ , we have  $\mathfrak{p}_i \cap (R \setminus \mathfrak{p}_j) \neq \emptyset$  and then  $\mathfrak{p}_iR_{\mathfrak{p}_j} = R_{\mathfrak{p}_j}$  by Proposition 3.13(c). So we have  $\mathfrak{a}R_{\mathfrak{p}_j} = (R \setminus \mathfrak{p}_j)^{-1}\mathfrak{a} = (R \setminus \mathfrak{p}_j)^{-1}(\bigcap_{i=1}^m \mathfrak{p}_i) = \bigcap_{i=1}^m (R \setminus \mathfrak{p}_j)^{-1}\mathfrak{p}_i = \bigcap_{i=1}^m \mathfrak{p}_iR_{\mathfrak{p}_j} = (\bigcap_{i=1, i \neq j}^m R_{\mathfrak{p}_j}) \cap \mathfrak{p}_jR_{\mathfrak{p}_j} = \mathfrak{p}_jR_{\mathfrak{p}_j}$  by Proposition 3.12(a), a contradiction. Thus,  $\mathfrak{p}_j \in \text{Min}(V(\mathfrak{a}))$ .  $\square$

**Proposition 4.29.** Let  $\mathfrak{q} \leq R$  be  $\mathfrak{p}$ -primary and  $x \in R$ . Then

$$(\mathfrak{q} : x) = \begin{cases} R & \text{if } x \in \mathfrak{q} \\ \mathfrak{q} & \text{if } x \notin \mathfrak{p} \\ \mathfrak{p}\text{-primary} & \text{if } x \notin \mathfrak{q} \end{cases}.$$

<sup>†</sup>By definition of *associated prime* from module theory,  $\text{Ass}_R(R/\mathfrak{a}) = \text{Spec}(R) \cap \{\text{Ann}_R(\bar{x}) \mid \bar{x} \in R/\mathfrak{a}\}$ .

*Proof.* If  $x \in \mathfrak{q}$ , then  $1 \in (\mathfrak{q} : x)$ , so  $(\mathfrak{q} : x) = R$ .

Assume  $x \notin \mathfrak{p} = \text{rad}(\mathfrak{q})$ . Note  $(\mathfrak{q} : x) \supseteq \mathfrak{q}$  by definition of colon ideal. Let  $y \in (\mathfrak{q} : x)$ , then  $yx \in \mathfrak{q}$ . Since  $\mathfrak{q}$  is primary,  $y \in \mathfrak{q}$  or  $x \in \text{rad}(\mathfrak{q})$ . By assumption,  $y \in \mathfrak{q}$ . Hence  $(\mathfrak{q} : x) \subseteq \mathfrak{q}$ .

Assume  $x \notin \mathfrak{q}$ . Let  $y \in (\mathfrak{q} : x)$ . Then  $xy \in \mathfrak{q}$ . Since  $\mathfrak{q}$  is primary,  $x \in \mathfrak{q}$  or  $y \in \text{rad}(\mathfrak{q}) = \mathfrak{p}$ . So by assumption,  $y \in \mathfrak{p}$ . Then  $\mathfrak{q} \subseteq (\mathfrak{q} : x) \subseteq \mathfrak{p}$ . So  $\mathfrak{p} = \text{rad}(\mathfrak{q}) \subseteq \text{rad}(\mathfrak{q} : x) \subseteq \text{rad}(\mathfrak{p}) = \mathfrak{p}$ . Hence  $\text{rad}(\mathfrak{q} : x) = \mathfrak{p}$ . Next, let  $ab \in (\mathfrak{q} : x)$  with  $a, b \in R$ . If  $b \in \text{rad}(\mathfrak{q} : x)$ , then  $(\mathfrak{q} : x)$  is  $\mathfrak{p}$ -primary, done. Assume  $b \notin \text{rad}(\mathfrak{q} : x) = \mathfrak{p} = \text{rad}(\mathfrak{q})$ . Since  $ab \in (\mathfrak{q} : x)$ ,  $ax \cdot b = abx \in \mathfrak{q}$ . Also, since  $\mathfrak{q}$  is primary and  $b \notin \text{rad}(\mathfrak{q})$ ,  $ax \in \mathfrak{q}$ , i.e.,  $a \in (\mathfrak{q} : x)$ . Thus,  $(\mathfrak{q} : x)$  is  $\mathfrak{p}$ -primary.  $\square$

**Proposition 4.30.**

$$\text{Ass}_R(\mathfrak{a}) := \{\mathfrak{p}_1, \dots, \mathfrak{p}_n\} = \text{Spec}(R) \cap \{\text{rad}(\mathfrak{a} : x) \mid x \in R\}^\dagger.$$

So  $\text{Ass}_R(\mathfrak{a})$  is independent of the minimal primary decomposition.

*Proof.* Let  $x \in R$ . Then  $(\mathfrak{a} : x) = (\bigcap_{i=1}^n \mathfrak{q}_i : x) = \bigcap_{i=1}^n (\mathfrak{q}_i : x)$  by Fact 1.54(i). So  $\text{rad}(\mathfrak{a} : x) = \text{rad}(\bigcap_{i=1}^n (\mathfrak{q}_i : x)) = \bigcap_{i=1}^n \text{rad}(\mathfrak{q}_i : x) = \bigcap_{i=1, x \notin \mathfrak{q}_i}^n \mathfrak{p}_i$  by Proposition 4.29, where the intersection of empty ideals is the  $R$ .

“ $\supseteq$ ”. Let  $\mathfrak{p} \in \text{Spec}(R) \cap \{\text{rad}(\mathfrak{a} : x) \mid x \in R\}$ . Then  $\mathfrak{p} \in \text{Spec}(R)$  and there exists  $x \in R$  such that  $\mathfrak{p} = \text{rad}(\mathfrak{a} : x) = \bigcap_{i=1, x \notin \mathfrak{q}_i}^n \mathfrak{p}_i$  which is not an empty intersection since  $\mathfrak{p} \neq R$ . So by Proposition 1.47(b),  $\mathfrak{p} = \mathfrak{p}_i$  with  $x \notin \mathfrak{q}_i$  for some  $i \in \{1, \dots, n\}$ .

“ $\subseteq$ ”. Let  $j \in \{1, \dots, n\}$ . Since  $\mathfrak{a} = \bigcap_{i=1}^n \mathfrak{q}_i$  is a minimal primary decomposition,  $\bigcap_{i=1, i \neq j}^n \mathfrak{q}_i \not\subseteq \mathfrak{q}_j$ . So there exists  $x \in \bigcap_{i=1, i \neq j}^n \mathfrak{q}_i$  such that  $x \notin \mathfrak{q}_j$ , i.e.,  $x \in \mathfrak{q}_i$  for  $1 \leq i \leq n$  with  $i \neq j$  and  $x \notin \mathfrak{q}_j$ . So  $\text{rad}(\mathfrak{a} : x) = \bigcap_{i=1, x \notin \mathfrak{q}_i}^n \mathfrak{p}_i = \mathfrak{p}_j$ . Hence  $\mathfrak{p}_j \in \text{Spec}(R) \cap \{\text{rad}(\mathfrak{a} : x) \mid x \in R\}$ .  $\square$

**Theorem 4.31.** If  $R$  is noetherian, then

$$\begin{aligned} \text{Ass}_R(\mathfrak{a}) &:= \{\mathfrak{p}_1, \dots, \mathfrak{p}_n\} = \text{Spec}(R) \cap \{(\mathfrak{a} : x) \mid x \in R\} \\ &= \text{Spec}(R) \cap \{\text{Ann}_R(\bar{x}) \mid \bar{x} \in R/\mathfrak{a}\} =: \text{Ass}_R(R/\mathfrak{a}). \end{aligned}$$

*Proof.* Proof of the first equality. “ $\supseteq$ ”. Let  $\mathfrak{p} \in \text{Spec}(R)$  such that  $\mathfrak{p} = (\mathfrak{a} : x)$  for some  $x \in R$ . Then  $\mathfrak{p} = \text{rad}(\mathfrak{p}) = \text{rad}(\mathfrak{a} : x)$ . So by Proposition 4.30,  $\mathfrak{p} = \mathfrak{p}_i$  for some  $i \in \{1, \dots, n\}$ . “ $\subseteq$ ”. Let  $j \in \{1, \dots, n\}$ . Since  $\mathfrak{a} = \bigcap_{i=1}^n \mathfrak{q}_i$  is a minimal primary decomposition,  $\mathfrak{a} \subsetneq \bigcap_{i=1, i \neq j}^n \mathfrak{q}_i$ . Since  $R$  is noetherian,  $\mathfrak{p}_j$  is finitely generated. Also, since  $\text{rad}(\mathfrak{q}_j) = \mathfrak{p}_j$ , there exists  $m \geq 1$  such that  $\mathfrak{p}_j^m \subseteq \mathfrak{q}_j$ . Let  $\mathfrak{a}_j := \bigcap_{i=1, i \neq j}^n \mathfrak{q}_i$ . Then  $\mathfrak{a}_j \mathfrak{p}_j^m \subseteq \mathfrak{a}_j \cap \mathfrak{p}_j^m \subseteq \mathfrak{a}_j \cap \mathfrak{q}_j = \bigcap_{i=1}^n \mathfrak{q}_i = \mathfrak{a}$ . Let  $l = \min\{m \geq 1 \mid \mathfrak{a}_j \mathfrak{p}_j^m \subseteq \mathfrak{a}\}$ . Note  $\mathfrak{a}_j \mathfrak{p}_j^0 = \mathfrak{a}_j \not\subseteq \mathfrak{a}$ . Since  $\mathfrak{a}_j \mathfrak{p}_j^{l-1} \not\subseteq \mathfrak{a}$ , there exists  $x \in \mathfrak{a}_j \mathfrak{p}_j^{l-1} \setminus \mathfrak{a} \subseteq \mathfrak{a}_j \setminus \mathfrak{a} = (\bigcap_{i=1, i \neq j}^n \mathfrak{q}_i) \setminus \mathfrak{q}_j$ , i.e.,  $x \in \mathfrak{q}_i$  for  $1 \leq i \leq n$  with  $i \neq j$  and  $x \notin \mathfrak{q}_j$ . So by the proof of Proposition 4.30,  $(\mathfrak{a} : x) \subseteq \text{rad}(\mathfrak{a} : x) = \mathfrak{p}_j$ . On the other hand, since  $x \mathfrak{p}_j \subseteq \mathfrak{a}_j \mathfrak{p}_j^{l-1} \mathfrak{p}_j = \mathfrak{a}_j \mathfrak{p}_j^l \subseteq \mathfrak{a}$ , we have  $\mathfrak{p}_j \subseteq (\mathfrak{a} : x)$ . Hence  $\mathfrak{p}_j = (\mathfrak{a} : x)$ .  $\square$

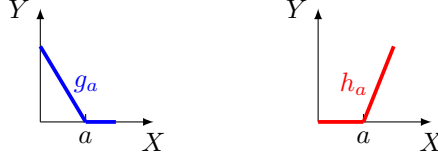
**Example 4.32.** If  $R$  is not noetherian, then  $\mathfrak{a} \subsetneq R$  may not have a primary decomposition. Let  $R = \mathcal{C}([0, 1]) = \{\text{continuous } f : [0, 1] \rightarrow \mathbb{R}\}$  with pointwise operations. Claim.  $0 \leq R$  does not have a primary decomposition.

(a) For  $a \in [0, 1]$ , define  $\Phi_a : R \rightarrow \mathbb{R}$  by  $\Phi_a(f) = f(a)$ . Then  $\Phi_a$  is a well-defined ring epimorphism. So  $\frac{R}{\text{Ker}(\Phi_a)} \cong \mathbb{R}$ . Hence  $\{f \in R \mid f(a) = 0\} = \text{Ker}(\Phi_a) \in \text{m-Spec}(R) \subseteq \text{Spec}(R)$ .

---

$^\dagger \text{Ass}_R(\mathfrak{a}) = \text{Spec}(R) \cap \{\text{rad}(\mathfrak{a} : x) \mid x \notin \mathfrak{a}\}.$

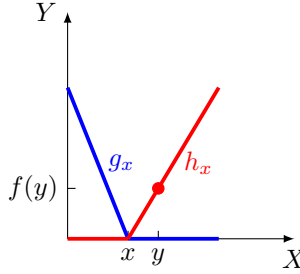
(b) Claim.  $0 \notin \text{Spec}(R)$ . For  $a \in (0, 1)$ , there exist  $g_a, h_a \in R$  such that  $g_a h_a = 0$  but  $g_a, h_a \neq 0$ .



(c) Claim.  $\text{Nil}(R) = 0$ . Let  $f \in \text{Nil}(R)$ . Then  $f^m = 0$  for some  $m \geq 1$ , i.e.,  $(f(a))^m = 0$  for  $a \in [0, 1]$ . Since  $f([0, 1]) \subseteq \mathbb{R}$  and  $\mathbb{R}$  is an integral domain,  $f(a) = 0$  for  $a \in [0, 1]$ , i.e.,  $f = 0$ .

(d) Claim.  $(0 : f) = \text{rad}(0 : f)$  for  $f \in R$ . “ $\subseteq$ ”. Done. “ $\supseteq$ ”. Let  $g \in \text{rad}(0 : f)$ . Then  $g^m \cdot f = 0$  for some  $m \geq 1$ . So  $g^m f^m = 0$ . Hence  $gf \in \text{Nil}(R) = 0$  by (c), i.e.,  $g \in (0 : f)$ .

(e) Claim.  $(0 : f) \notin \text{Spec}(R)$  for  $f \in R$ . Suppose  $(0 : f) \in \text{Spec}(R)$ . Then  $(0 : f) \neq R$ , i.e.,  $f \neq 0$ . So there exists  $y \in [0, 1]$  such that  $f(y) \neq 0$ . Since  $f$  is continuous, there exists  $y \in (0, 1)$  such that  $f(y) \neq 0$ . Let  $0 < x < y$ . Then  $g_x h_x = 0 \in (0 : f) \in \text{Spec}(R)$ .



So  $g_x \in (0 : f)$  or  $h_x \in (0 : f)$ , i.e.,  $g_x f = 0$  or  $h_x f = 0$ . Since  $h_x(y)f(y) > 0$ ,  $h_x f \neq 0$ . So  $g_x f = 0$ . Also, since  $g_x(a) \neq 0$  for  $0 < a < x < y$ , we have  $f(a) = 0$  for  $0 < a < x < y$ . Since  $x \in (0, y)$  is arbitrary,  $f(a) = 0$  for  $0 < a < y$ . Since  $f$  is continuous,  $f(y) = \lim_{a \rightarrow y^-} f(a) = 0$ , a contradiction.

Now suppose  $0 = \bigcap_{i=1}^n \mathfrak{q}_i$  is a primary decomposition. Assume without loss of generality that the decomposition is minimal by Proposition 4.27. By (d), (e) and Proposition 4.30, there exists  $f_1 \in R$  such that  $\text{Spec}(R) \not\ni (0 : f_1) = \text{rad}(0 : f_1) = \text{rad}(\mathfrak{q}_1) \in \text{Spec}(R)$ , a contradiction.

(f) Note  $0 = \{f \in R \mid f(a) = 0, \forall a \in [0, 1]\} = \bigcap_{a \in [0, 1]} \underbrace{\{f \in R \mid f(a) = 0\}}_{\in \text{Spec}(R), \therefore \text{primary}} = \bigcap_{a \in [0, 1]} \text{Ker}(\Phi_a) =$

$\bigcap_{a \in [0, 1] \cap \mathbb{Q}} \text{Ker}(\Phi_a) = \dots$  cannot be pruned to a minimal primary decomposition.

**Proposition 4.33.**

$$\{x \in R \mid (\mathfrak{a} : x) \neq \mathfrak{a}\} = \bigcup_{i=1}^n \mathfrak{p}_i = \bigcup_{\mathfrak{p} \in \text{Ass}_R(\mathfrak{a})} \mathfrak{p}.$$

*Proof.* Claim.  $\{x \in R \mid (\mathfrak{a} : x) \neq \mathfrak{a}\} = \bigcup_{y \notin \mathfrak{a}} \text{rad}(\mathfrak{a} : y)$ . “ $\subseteq$ ”. Then  $x \in R$  such that  $(\mathfrak{a} : x) \neq \mathfrak{a}$ . So  $(\mathfrak{a} : x) \supsetneq \mathfrak{a}$ . Then there exists  $z \in (\mathfrak{a} : x) \setminus \mathfrak{a}$ , i.e.,  $z \notin \mathfrak{a}$  and  $xz \in \mathfrak{a}$ , i.e.,  $z \notin \mathfrak{a}$  and  $x \in (\mathfrak{a} : z) \subseteq \text{rad}(\mathfrak{a} : z) \subseteq \bigcup_{y \notin \mathfrak{a}} \text{rad}(\mathfrak{a} : y)$ . “ $\supseteq$ ”. Let  $x \in \text{rad}(\mathfrak{a} : y)$  for some  $y \notin \mathfrak{a}$ . Then  $x^m y \in \mathfrak{a}$

for some  $m \geq 1$ . Let  $n = \min\{m \geq 1 \mid x^m y \in \mathfrak{a}\}$ . Note  $x^0 y = y \notin \mathfrak{a}$ . Then  $x^n y \in \mathfrak{a}$  but  $x^{n-1} y \notin \mathfrak{a}$ . So  $x^{n-1} y \in (\mathfrak{a} : x)$ . Hence  $(\mathfrak{a} : x) \neq \mathfrak{a}$ .

Claim.  $\bigcup_{y \notin \mathfrak{a}} \text{rad}(\mathfrak{a} : y) = \bigcup_{i=1}^n \mathfrak{p}_i$ . “ $\subseteq$ ”. Let  $y \notin \mathfrak{a} = \bigcap_{i=1}^n \mathfrak{q}_i$ . Then by the proof of Proposition 4.30,  $\text{rad}(\mathfrak{a} : y) = \bigcap_{i=1, y \notin \mathfrak{q}_i}^n \mathfrak{p}_i = \bigcap_{i=1}^n \mathfrak{p}_i \subseteq \bigcup_{i=1}^n \mathfrak{p}_i$ . “ $\supseteq$ ”. By Proposition 4.30, there exists  $y_i \notin \mathfrak{a}$  such that  $\mathfrak{p}_i = \text{rad}(\mathfrak{a} : y_i)$  for  $i = 1, \dots, n$ . So  $\bigcup_{y \notin \mathfrak{a}} \text{rad}(\mathfrak{a} : y) \supseteq \bigcup_{i=1}^n \mathfrak{p}_i$ .  $\square$

**Corollary 4.34.** Set  $\mathfrak{a} = 0$  in Proposition 4.33, we get

$$\text{ZD}(R) = \{x \in R \mid (0 : x) \neq 0\} = \bigcup_{i=1}^n \mathfrak{p}_i = \bigcup_{\mathfrak{p} \in \text{Ass}_R(0)} \mathfrak{p}.$$

**Summary 4.35.** Let  $R$  be noetherian and  $\mathfrak{a} = 0$ . Then  $\text{ZD}(R) = \bigcup_{i=1}^n \mathfrak{p}_i = \bigcup_{\mathfrak{p} \in \text{Ass}_R(0)} \mathfrak{p}$ . (Use with prime avoidance to get useful information about ideals and  $\text{NZD}(R)$ .)

$$\text{Nil}(R) = \text{rad}(0) = \text{rad}\left(\bigcap_{i=1}^n \mathfrak{q}_i\right) = \bigcap_{i=1}^n \mathfrak{p}_i = \bigcap_{\mathfrak{p} \in \text{Min}(0)} \mathfrak{p}.$$

**Example.** Let  $R = \frac{k[X, Y]}{\langle X^2, XY \rangle} = \frac{k[X, Y]}{\langle X \rangle \cap \langle X^2, Y \rangle}$  and  $x = \bar{X}, y = \bar{Y} \in R$ . Then  $\langle 0 \rangle R = \langle x \rangle \cap \langle x^2, y \rangle$  is a minimal primary decomposition. So  $\text{ZD}(R) = \langle x \rangle \cup \langle x, y \rangle = \langle x, y \rangle$ . For  $f \in R$  with constant term 0, we have  $f = xf_1 + yf_2$  for some  $f_1, f_2 \in R$ , then  $xf = x^2 f_1 + xyf_2 = 0$ . So  $f \in \text{ZD}(R)$ .

**Proposition 4.36.** We have

$$\text{Min}(\mathfrak{a}) = \min\{\mathfrak{p}_1, \dots, \mathfrak{p}_n\} = \text{Min}(\text{V}(\mathfrak{a})).$$

In particular,

$$\text{Min}(0) = \text{Min}(\text{V}(0)) = \text{Min}(\text{Spec}(R)) = \text{Min}(R).$$

*Proof.* It follows from the proof of Proposition 4.28.  $\square$

**Lemma 4.37.** Let  $U \subseteq R$  be multiplicatively closed and  $\mathfrak{q} \leq R$  be  $\mathfrak{p}$ -primary. Let  $\psi : R \rightarrow U^{-1}R$  be the natural ring homomorphism.

(a) If  $U \cap \mathfrak{p} \neq \emptyset$ , then  $U^{-1}\mathfrak{q} = U^{-1}R$ .

(b) If  $U \cap \mathfrak{p} = \emptyset$ , then  $U^{-1}\mathfrak{q} \leq U^{-1}R$  is  $U^{-1}\mathfrak{p}$ -primary and  $\psi^{-1}(U^{-1}\mathfrak{q}) = \mathfrak{q}$ .

*Proof.* (a) Let  $u \in U \cap \mathfrak{p}$ . Since  $\mathfrak{p} = \text{rad}(\mathfrak{q})$  and  $U$  is multiplicatively closed, there exists  $n \geq 1$  such that  $u^n \in \mathfrak{q} \cap U$ . So by Proposition 3.13,  $U^{-1}\mathfrak{q} = U^{-1}R$ .

(b) Since  $\mathfrak{q} \subseteq \mathfrak{p}$  and  $U \cap \mathfrak{p} = \emptyset$ ,  $U^{-1}\mathfrak{q} \subseteq U^{-1}\mathfrak{p} \subsetneq U^{-1}R$  by Proposition 3.13. Let  $\frac{x}{u}, \frac{y}{v} \in U^{-1}R$ . If  $\frac{y}{v} \in \text{rad}(U^{-1}\mathfrak{q})$ , then  $U^{-1}\mathfrak{q}$  is primary. Assume  $\frac{y}{v} \notin \text{rad}(U^{-1}\mathfrak{q})$ . Since  $\frac{xy}{uv} \in U^{-1}\mathfrak{q}$ , there exists  $w \in U$  such that  $x(wy) = wxy \in \mathfrak{q}$ . Since  $\frac{y}{v} \notin \text{rad}(U^{-1}\mathfrak{q}) = U^{-1}\text{rad}(\mathfrak{q}) = U^{-1}\mathfrak{p}$  by Proposition 3.12(d),  $wy \notin \mathfrak{p} = \text{rad}(\mathfrak{q})$ . Also, since  $\mathfrak{q}$  is primary,  $x \in \mathfrak{q}$ . So  $\frac{x}{u} \in U^{-1}\mathfrak{q}$ . Hence  $U^{-1}\mathfrak{q}$  is primary.

Since  $\mathfrak{q} \subseteq \mathfrak{p} = \text{rad}(\mathfrak{q}) \in \text{Spec}(R)$ , by Proposition 3.12(d), we have  $\text{rad}(U^{-1}\mathfrak{q}) \subseteq \text{rad}(U^{-1}\mathfrak{p}) = U^{-1}\text{rad}(\mathfrak{p}) = U^{-1}\mathfrak{p} = U^{-1}\text{rad}(\mathfrak{q}) = \text{rad}(U^{-1}\mathfrak{q})$ . So  $\text{rad}(U^{-1}\mathfrak{q}) = U^{-1}\mathfrak{p}$ .

Claim.  $\psi^{-1}(U^{-1}\mathfrak{q}) = \mathfrak{q}$ . “ $\supseteq$ ”. By Proposition 1.63(a). “ $\subseteq$ ”. Let  $x \in \psi^{-1}(U^{-1}\mathfrak{q})$ . Then  $\frac{x}{1} = \psi(x) \in U^{-1}\mathfrak{q}$ . So there exists  $u \in U$  such that  $xu \in \mathfrak{q}$ . Since  $U \cap \mathfrak{p} = \emptyset$ ,  $u \notin \mathfrak{p} = \text{rad}(\mathfrak{q})$ . Also, since  $\mathfrak{q}$  is primary,  $x \in \mathfrak{q}$ .  $\square$



**Theorem 4.38** (Second uniqueness theorem). (a) Let  $\mathfrak{q} = \mathfrak{q}_i$  be  $\mathfrak{p}$ -primary for some  $i \in \{1, \dots, n\}$  with  $\mathfrak{p} \in \text{Min}(\mathfrak{a})$ . Then  $\mathfrak{q} = \psi^{-1}(\mathfrak{a}_{\mathfrak{p}})^{\dagger}$ , where  $\psi : R \rightarrow R_{\mathfrak{p}}$  and  $U = R \setminus \mathfrak{p}$ , so  $\mathfrak{q}$  is independent of choice of minimal primary decomposition.

(b) If  $\Lambda = \langle \mathfrak{p}_{i_1}, \dots, \mathfrak{p}_{i_m} \rangle$  is an “isolated” subset of  $\text{Ass}_R(\mathfrak{a}) = \{\mathfrak{p}_1, \dots, \mathfrak{p}_n\}$ , then  $\bigcap_{j=1}^m \mathfrak{q}_{i_j} = \Psi^{-1}(U^{-1}\mathfrak{a})$ , where  $\Psi : R \rightarrow U^{-1}R$  and  $U = R \setminus \{\mathfrak{p}_{i_1} \cup \dots \cup \mathfrak{p}_{i_m}\}$ . So  $\bigcap_{j=1}^m \mathfrak{q}_{i_j}$  is independent of choice of minimal primary decomposition.

*Proof.* (b) By Proposition 3.12(b) and Lemma 4.37, we have  $\Psi^{-1}(U^{-1}\mathfrak{a}) = \Psi^{-1}(U^{-1}(\bigcap_{i=1}^n \mathfrak{q}_i)) = \Psi^{-1}(\bigcap_{i=1}^n U^{-1}\mathfrak{q}_i) = \bigcap_{i=1}^n \Psi^{-1}(U^{-1}\mathfrak{q}_i) = \bigcap_{i=1, \mathfrak{p}_i \cap U = \emptyset}^n \mathfrak{q}_i = \bigcap_{j=1}^m \mathfrak{q}_{i_j}$  since  $\Lambda$  is “isolated”.

(a) It follows from (b) since  $\{\mathfrak{p}\}$  is “isolated” for  $\mathfrak{p} \in \text{Min}(\mathfrak{a})$ .  $\square$

**Definition 4.39.**  $\Lambda \subseteq \text{Ass}_R(\mathfrak{a})$  is “isolated” if it is “closed under subsets”, i.e., if  $\mathfrak{p}, \mathfrak{p}' \in \text{Ass}_R(\mathfrak{a})$  such that  $\mathfrak{p}' \subseteq \mathfrak{p}$  and  $\mathfrak{p} \in \Lambda$ , then  $\mathfrak{p}' \in \Lambda$ .

**Discussion 4.40.** Consider the following.

(a) If  $\mathfrak{m} \in \text{m-Spec}(R)$ , then  $\mathfrak{m}^n$  is  $\mathfrak{m}$ -primary for  $n \geq 1$  by Example 4.11(b).

(b) Let  $k$  be a field. If  $\mathfrak{p} = \langle X_{i_1}, \dots, X_{i_m} \rangle \leq k[X_1, \dots, X_d]$ , then  $\mathfrak{p}^n$  is  $\mathfrak{p}$ -primary for  $n \geq 1$ .

*Proof.* (b) Note  $\langle X_{i_1}^{a_1}, \dots, X_{i_m}^{a_m} \rangle$  is  $\mathfrak{p}$ -primary for  $a_1, \dots, a_m \geq 1$  by Example 4.12(c). Let  $\Lambda = \{\underline{a} \in \mathbb{N}^m \mid a_1 + \dots + a_m = m + n - 1\}$ . Set  $\mathfrak{p}_{\underline{a}} = \langle X_{i_1}^{a_1}, \dots, X_{i_m}^{a_m} \rangle$  for  $\underline{a} \in \Lambda$ . Claim.  $\mathfrak{p}^n = \bigcap_{\underline{a} \in \Lambda} \mathfrak{p}_{\underline{a}}$ , then by Proposition 4.22,  $\mathfrak{p}^n$  is  $\mathfrak{p}$ -primary.

“ $\subseteq$ ”. Let  $\Lambda_0 = \{\underline{e} \in \mathbb{Z}_{\geq 0}^m \mid e_1 + \dots + e_m = n\}$ . For  $n \geq 1$ ,  $\mathfrak{p}^n = (\langle X_{i_1} \rangle + \dots + \langle X_{i_m} \rangle)^n = \sum_{\underline{e} \in \Lambda_0} \langle X_{i_1}^{e_1} \dots X_{i_m}^{e_m} \rangle$ . Suppose  $X_{(i)}^{\underline{e}} := X_{i_1}^{e_1} \dots X_{i_m}^{e_m} \in \mathfrak{p}^n \setminus \mathfrak{p}_{\underline{a}}$  for some  $\underline{e} \in \Lambda_0$  and  $\underline{a} \in \Lambda$ . Then  $a_i \geq e_i + 1$  for  $i = 1, \dots, m$ . So  $m + n - 1 = \sum_{i=1}^m a_i \geq m + \sum_{i=1}^m e_i = m + n$ , a contradiction. So  $X_{(i)}^{\underline{e}} \in \mathfrak{p}_{\underline{a}}$  for all  $\underline{e} \in \Lambda_0$  and  $\underline{a} \in \Lambda$ . Hence  $\mathfrak{p}^n \subseteq \bigcap_{\underline{a} \in \Lambda} \mathfrak{p}_{\underline{a}}$ .

“ $\supseteq$ ”. Let  $R' := k[X_{i_1}, \dots, X_{i_m}] \subseteq k[X_1, \dots, X_d]$  and  $\mathfrak{p}' = (X_{i_1}, \dots, X_{i_m})R'$ . Set  $\mathfrak{p}'_{\underline{a}} = \langle X_{i_1}^{a_1}, \dots, X_{i_m}^{a_m} \rangle R'$  for  $\underline{a} \in \Lambda$ . We know  $\mathfrak{p}'^n$  in  $R'$  has an (irredundant) parametric decomposition  $\mathfrak{p}'^n = \bigcap_{f' \in C_{R'}(\mathfrak{p}')} P_{R'}(f') = \bigcap_{\underline{a} \in \Lambda} \mathfrak{p}'_{\underline{a}}$ . Let  $q = \#\Lambda$ . Since  $\bigcap_{\underline{a} \in \Lambda} \mathfrak{p}_{\underline{a}}$  and  $\bigcap_{\underline{a} \in \Lambda} \mathfrak{p}'_{\underline{a}}$  have the same generating set  $\{\text{lcm}(f_1, \dots, f_q) \mid f_j \text{ is a generator of } \mathfrak{p}_{\underline{a}_j} \text{ with } \underline{a}_j \in \Lambda \text{ for } j = 1, \dots, q\}$ , we have the generators of  $\bigcap_{\underline{a} \in \Lambda} \mathfrak{p}_{\underline{a}}$  are in  $\bigcap_{\underline{a} \in \Lambda} \mathfrak{p}'_{\underline{a}} = \mathfrak{p}'^n \subseteq \mathfrak{p}^n$ . Hence  $\mathfrak{p}^n \supseteq \bigcap_{\underline{a} \in \Lambda} \mathfrak{p}_{\underline{a}}$ .  $\square$

**Example 4.41.** In general,  $\mathfrak{p}^n$  is not  $\mathfrak{p}$ -primary for  $\mathfrak{p} \in \text{Spec}(R)$ . For example, let  $R = \frac{k[X, Y, Z]}{\langle XY - Z^2 \rangle}$  and  $x = \bar{x}, y = \bar{Y}, z = \bar{Z} \in R$ , then  $\mathfrak{p} := \langle x, z \rangle \in \text{Spec}(R)$ , but  $\mathfrak{p}^2$  is not  $\mathfrak{p}$ -primary since  $xy = z^2 \in \mathfrak{p}^2$  but  $x \notin \mathfrak{p}^2$  and  $y \notin \mathfrak{p} = \text{rad}(\mathfrak{p}^2)$ .

**Definition 4.42.** Let  $\mathfrak{p} \in \text{Spec}(R)$  and  $\psi : R \rightarrow R_{\mathfrak{p}}$ . Then for  $n \geq 1$ , the  $n^{\text{th}}$  symbolic power of  $\mathfrak{p}$  is

$$\mathfrak{p}^{(n)} = \psi^{-1}((\mathfrak{p}^n)_{\mathfrak{p}}) = \psi^{-1}((\mathfrak{p}_{\mathfrak{p}})^n).$$

**Note 4.43.**  $\mathfrak{p}^n \subseteq \mathfrak{p}^{(n)}$  because by Proposition 1.63(a),  $\mathfrak{p}^n \subseteq \psi^{-1}((\mathfrak{p}^n)_{\mathfrak{p}}) = \mathfrak{p}^{(n)}$ .

**Example 4.44.** We have the following examples.

<sup>†</sup>That is,  $\mathfrak{q}$  is the kernel of the ring homomorphism  $R \rightarrow (R/\mathfrak{a})_{\mathfrak{p}}$ .

(a) Let  $\mathfrak{m} \in \text{m-Spec}(R)$  and  $\psi : R \rightarrow R_{\mathfrak{m}}$ . Since  $\mathfrak{m}^n$  is  $\mathfrak{m}$ -primary by Example 4.11(b) and  $\mathfrak{m} \cap (R \setminus \mathfrak{m}) = \emptyset$ , by Lemma 4.37(b),  $\mathfrak{m}^n = \psi^{-1}((\mathfrak{m}^n)_{\mathfrak{m}}) =: \mathfrak{m}^{(n)}$  for  $n \geq 1$ .

(b) Let  $k$  be a field and  $\mathfrak{p} = \langle X_{i_1}, \dots, X_{i_m} \rangle \leq k[X_1, \dots, X_d]$ . Since  $\mathfrak{p}^n$  is  $\mathfrak{p}$ -primary by Discussion 4.40(b) and  $\mathfrak{p} \cap (R \setminus \mathfrak{p}) = \emptyset$ , by Lemma 4.37(b),  $\mathfrak{p}^n = \psi^{-1}((\mathfrak{p}^n)_{\mathfrak{p}}) =: \mathfrak{p}^{(n)}$  for  $n \geq 1$ .

(c) Let  $R = \frac{k[X,Y,Z]}{\langle XY-Z^2 \rangle}$  and  $x = \overline{X}, y = \overline{Y}, z = \overline{Z} \in R$ . Let  $\mathfrak{p} = \langle x, z \rangle$ . Claim.  $\mathfrak{p}^{(2)} = \langle x \rangle$ . “ $\supseteq$ ”. Since  $y \notin \mathfrak{p}$  and  $xy = z^2 \in \mathfrak{p}^2$ , we have  $x = \frac{x}{1} = \frac{xy}{y} \in (\mathfrak{p}^2)_{\mathfrak{p}}$  in  $R_{\mathfrak{p}}$ . So  $x \in \psi^{-1}(\mathfrak{p}^2)_{\mathfrak{p}} = \mathfrak{p}^{(2)}$ . “ $\subseteq$ ”. Let  $a \in \mathfrak{p}^{(2)}$ . Then  $a = \frac{a}{1} = \psi(a) \in (\mathfrak{p}^2)_{\mathfrak{p}}$ . So there exists  $b \in R \setminus \mathfrak{p}$  such that  $ab \in \mathfrak{p}^2 = \langle x^2, xz, z^2 \rangle = \langle x^2, xz, xy \rangle$ . Also, since  $b \notin \langle x \rangle$ ,  $a \in \langle x \rangle$ . Hence  $\mathfrak{p}^{(2)} \subseteq \langle x \rangle$ . Thus,  $\mathfrak{p}^{(2)} = \langle x \rangle \supsetneq \langle x^2, xz, xy \rangle = \mathfrak{p}^2$ .

Note a basis for  $R$  over  $k$  is  $\{x^a y^b, x^a y^b z \mid a, b \geq 0\}$ .

**Proposition 4.45.** If  $\mathfrak{p} \in \text{Spec}(R)$ , then  $\mathfrak{p}^{(n)}$  is the “ $\mathfrak{p}$ -primary component” of  $\mathfrak{p}^n$ , i.e., if  $\mathfrak{p}^n$  has a minimal primary decomposition  $\mathfrak{p}^n = \bigcap_{i=1}^m \mathfrak{q}_i$  such that  $\mathfrak{p}_i = \text{rad}(\mathfrak{q}_i)$  for  $i = 1, \dots, m$ , then  $\mathfrak{p}_j = \mathfrak{p}$  and  $\mathfrak{q}_j = \mathfrak{p}^{(n)}$  for some  $j \in \{1, \dots, m\}$ .

*Proof.* Since  $\text{rad}(\mathfrak{p}^n) = \mathfrak{p}$ ,  $\text{Min}(\mathfrak{p}^n) = \{\mathfrak{p}\}$ . So  $\mathfrak{p} = \text{rad}(\mathfrak{q}_j) = \mathfrak{p}_j$  for some  $j \in \{1, \dots, m\}$ . Then by the second uniqueness theorem,  $\mathfrak{q}_j = \psi^{-1}((\mathfrak{p}_j^n)_{\mathfrak{p}_j}) = \psi^{-1}((\mathfrak{p}^n)_{\mathfrak{p}}) = \mathfrak{p}^{(n)}$ .  $\square$

**Example 4.46.** Let  $R = \frac{k[X,Y,Z]}{\langle XY-Z^2 \rangle}$  and  $x = \overline{X}, y = \overline{Y}, z = \overline{Z} \in R$ . Let  $\mathfrak{p} = \langle x, z \rangle \in \text{Spec}(R)$ . Then by Example 4.44(c),  $\mathfrak{p}^{(2)} = \langle x \rangle$ . Note  $\mathfrak{p}^2 = \langle x \rangle \cap \langle x^2, z, y \rangle$  with  $\text{rad}(\langle x \rangle) = \langle x, z \rangle = \mathfrak{p}$  since  $z^2 = xy$ , and with  $\text{rad}(\langle x^2, z, y \rangle) = \langle x, y, z \rangle \in \text{m-Spec}(R)$  since  $R/\langle x, y, z \rangle \cong \frac{k[X,Y,X]}{\langle XY-Z^2, X, Y, Z \rangle} = \frac{k[X,Y,Z]}{\langle X, Y, Z \rangle} \cong k$ .

**Definition 4.47** (Calculus content). Let  $R = \mathbb{C}[X_1, \dots, X_d]$  and  $\mathfrak{p} \in \text{Spec}(R)$  (Zariski).

$$\mathfrak{p}^{(2)} = \left\{ f \in \mathfrak{p} \mid \frac{\partial f}{\partial x_i} \in \mathfrak{p}, \forall i = 1, \dots, d \right\},$$

$$\mathfrak{p}^{(n)} = \left\{ f \in \mathfrak{p} \mid \frac{\partial^i f}{\partial \underline{x}} \in \mathfrak{p}, \text{ all partials of order } i = 1, \dots, n-1 \right\}, \forall n \geq 3.$$



## Chapter 5

# Modules and Integral Dependence

### Modules

Let  $R$  be a commutative ring with identity.

**Definition 5.1.** An  $R$ -module is an additive abelian group  $M$  equipped with a scalar multiplication  $R \times M \rightarrow M$  denoted  $(r, m) \mapsto rm$  that is unital, associative and distributive.

- $1m = m$  for all  $m \in M$ .
- $r(sm) = (rs)m$  for all  $r, s \in R$  and  $m \in M$ .
- $(r + s)m = rm + sm$  for all  $r, s \in R$  and  $m \in M$ .
- $r(m + n) = rm + rn$  for all  $r \in R$  and  $m, n \in M$ .

(Closure)  $rm \in M$  for all  $r \in R$  and  $m \in M$ .

**Example 5.2.** (a) For  $n = 1, 2, 3, \dots$ , let  $R^n = \left\{ \begin{bmatrix} r_1 \\ \vdots \\ r_n \end{bmatrix} \mid r_1, \dots, r_n \in R \right\}$  with  $s \begin{bmatrix} r_1 \\ \vdots \\ r_n \end{bmatrix} = \begin{bmatrix} sr_1 \\ \vdots \\ sr_n \end{bmatrix}$  for  $s \in R$ , then  $R^n$  is an  $R$ -module. e.g.,  $R$  is an  $R$ -module.

(b) A  $\mathbb{Z}$ -module is an additive abelian group.

(c) Let  $\varphi : R \rightarrow S$  be a ring homomorphism. Then  $S$  is an  $R$ -module with  $r \cdot s = \varphi(r)s$  for  $r \in R$  and  $s \in S$ .

Let  $M$  be an  $R$ -module.

**Definition 5.3.** A *submodule* of  $M$  is a subset  $N \subseteq M$  such that  $N$  is an  $R$ -module using the operations from  $M$ .

**Example 5.4.** (a) If  $I \leq R$ , then  $I$  is a submodule of  $R$ .

(b) A submodule of an  $\mathbb{Z}$ -module is a subgroup.

(c) Submodule test.  $0 \neq N \subseteq M$  is a submodule of  $M$  if and only if  $n + n' \in N$  for all  $n, n' \in N$  and  $rn \in N$  for all  $r \in R$  and  $n \in N$  if and only if  $n + rn' \in N$  for all  $r \in R$  and  $n, n' \in N$ .

(d) If  $M_\lambda \subseteq M$  is a submodule for  $\lambda \in \Lambda$ , then  $\bigcap_{\lambda \in \Lambda} M_\lambda \subseteq M$  and  $\sum_{\lambda \in \Lambda} M_\lambda \subseteq M$  are submodules.

**Definition 5.5.** Let  $Y \subseteq M$ . Define

$$\langle Y \rangle = R\langle Y \rangle = R(Y) = \bigcap_{Y \subseteq N \subseteq M} N,$$

intersection of all submodules  $N \subseteq M$  such that  $Y \subseteq N$ . This is the (unique) smallest submodule of  $M$  containing  $Y$ . e.g., for a submodule  $N \subseteq M$ ,  $\langle Y \rangle \subseteq N$  if and only if  $Y \subseteq N$ .

$\langle Y \rangle$  is the *submodule* of  $M$  generated by  $Y$ .

$M$  is *finitely generated* if there exist  $y_1, \dots, y_n \in M$  such that  $M = \langle y_1, \dots, y_n \rangle$ .

**Fact 5.6.** (a) Let  $Y \subseteq M$ . Then

$$\langle Y \rangle = \left\{ \sum_{y \in Y}^{\text{finite}} r_y y \mid r_y \in R, \forall y \right\} = \sum_{y \in Y} \langle y \rangle.$$

(b) If  $y_1, \dots, y_n \in M$ , then

$$\langle y_1, \dots, y_n \rangle = \left\{ \sum_{i=1}^n r_i y_i \mid r_1, \dots, r_n \in R \right\}.$$

**Example 5.7.** Submodules of a finitely generated  $R$ -module may not be finitely generated. Note  $R := k[X_1, X_2, \dots] = \langle 1 \rangle$  is a finitely generated  $R$ -module, but  $\mathfrak{m} = \langle X_1, X_2, \dots \rangle \subseteq R$  is not finitely generated.

## Integral Dependence

Let  $R$  be a nonzero commutative ring with identity. Let  $R \subseteq S$  be a subring.

**Definition 5.8.** An element  $s \in S$  is *integral* over  $R$  if there exists a monic  $f \in R[X]$  such that  $f(s) = 0$ , i.e., there exists  $n \geq 1$  and  $r_0, \dots, r_{n-1} \in R$  such that  $s^n + r_{n-1}s^{n-1} + \dots + r_0 = 0$ .

$S$  is *integral*  $R$  if every  $s \in S$  is integral over  $R$ , (or  $R \subseteq S$  is an *integral extension*).

**Example 5.9.** (a) Let  $k \subseteq K$  be a field extension. Then  $K$  is integral over  $k$  if and only if  $k \subseteq K$  is an algebraic extension.

(b) Every  $r \in R$  is integral over  $R$  since  $r$  satisfies  $X - r \in R[X]$ .

(c)  $\mathbb{Z} \subseteq \mathbb{Z}[i]$  is an integral extension since  $a + bi \in \mathbb{Z}[i]$  satisfies  $X^2 - 2aX + (a^2 + b^2) \in \mathbb{Z}[X]$ .

(d)  $\mathbb{Z} \subseteq \mathbb{Q}$ . The only  $\frac{r}{s} \in \mathbb{Q}$  that are integral over  $\mathbb{Z}$  are the elements of  $\mathbb{Z}$ .

*Proof.* (c) Let  $\frac{r}{s} \in \mathbb{Q}$  be integral over  $\mathbb{Z}$ , where  $s \neq 0$  and  $(r, s) = 1$ . Then  $(\frac{r}{s})^n + c_{n-1}(\frac{r}{s})^{n-1} + \dots + c_1(\frac{r}{s}) + c_0 = 0$  for some  $n \geq 1$  and  $c_0, \dots, c_{n-1} \in \mathbb{Z}$ . So  $\frac{r^n + c_{n-1}r^{n-1}s + \dots + c_1rs^{n-1} + c_0s^n}{s^n} = 0$ , i.e.,  $r^n = -(c_{n-1}r^{n-1}s + \dots + c_1rs^{n-1} + c_0s^n) = -s(c_{n-1}r^{n-1} + \dots + c_1rs^{n-2} + c_0s^{n-1})$ . Hence  $s \mid r^n$ . Since  $(r, s) = 1$ ,  $(r^n, s) = 1$ . So  $s = \pm 1$ . Thus,  $\frac{r}{s} = \pm r \in \mathbb{Z}$ .  $\square$

**Definition 5.10.** An *intermediate subring* is a subring  $T \subseteq S$  such that  $R \subseteq T$ . (Notice if  $R \subseteq T \subseteq S$  is an intermediate subring, then  $R \subseteq T$  is a subring.)

Let  $y_1, \dots, y_n \in S$ . Define the *subring* of  $S$  generated over  $R$  by  $y_1, \dots, y_n$  by

$$R[y_1, \dots, y_n] = \bigcap_{\substack{R \subseteq T \subseteq S, \\ y_1, \dots, y_n \in T}} T,$$

where the intersection is taken over all intermediate subrings  $R \subseteq T \subseteq S$  such that  $y_1, \dots, y_n \in T$ .

**Fact 5.11.** Let  $y_1, \dots, y_n \in S$ .

- (a)  $R[y_1, \dots, y_n] = \{f(y_1, \dots, y_n) \in S \mid f \in R[Y_1, \dots, Y_n]\}$ .
- (b)  $\psi : R[Y_1, \dots, Y_n] \rightarrow S$  given by  $\psi(f) = f(y_1, \dots, y_n)$  is a well-defined ring homomorphism with  $\text{Im}(\psi) = R[y_1, \dots, y_n]$  and  $\overline{Y_1}, \dots, \overline{Y_n} \in R[Y_1, \dots, Y_n]/\text{Ker}(\psi) \cong R[y_1, \dots, y_n]$ . So if  $y_1, \dots, y_n$  have no polynomial relations, then  $\text{Ker}(\psi) = 0$  and hence  $R[Y_1, \dots, Y_n] \cong R[y_1, \dots, y_n]$ .
- (c) Let  $T \subseteq S$  be a subring. Then  $R[y_1, \dots, y_n] \subseteq T$  if and only if  $R \subseteq T$  and  $y_1, \dots, y_n \in T$ .

**Example 5.12.**  $\mathbb{Z} \subseteq \mathbb{Z}[i] \subseteq \mathbb{C}$  is an intermediate subring, where  $\mathbb{Z}[i] \cong \mathbb{Z}[X]/\langle X^2 + 1 \rangle$ .

**Proposition 5.13.** Let  $s \in S$ . Then the following are equivalent.

- (i)  $s$  is integral over  $R$ .
- (ii)  $R[s]$  is a finitely generated  $R$ -module.
- (iii) There exists an intermediate subring  $R \subseteq T \subseteq S$  such that  $s \in T$  and  $T$  is a finitely generated  $R$ -module.

*Proof.* “(i) $\Rightarrow$ (ii)”. Assume  $s$  is integral over  $R$ . Then  $s^n + r_{n-1}s^{n-1} + \dots + r_0 = 0$  for some  $n \geq 1$  and  $r_0, \dots, r_{n-1} \in R$ . Claim.  $R[s] = R\langle 1, s, \dots, s^{n-1} \rangle$ . “ $\supseteq$ ”. It is straightforward. “ $\subseteq$ ”. It suffices to show  $s^m \in R\langle 1, s, \dots, s^{n-1} \rangle$  for  $m = n, n+1, \dots$ . Use induction on  $m$ . Base case:  $s^n = -\sum_{i=0}^{n-1} r_i s^i \in R\langle 1, s, \dots, s^{n-1} \rangle$ . Inductive step: assume  $m \geq n+1$  and  $s^k \in R\langle 1, s, \dots, s^{n-1} \rangle$  for  $0 \leq k \leq m-1$ . Then  $s^m = s^n s^{m-n} = -\sum_{i=0}^{n-1} r_i s^{i+m-n} \in R\langle s^{m-n}, \dots, s^{m-1} \rangle \subseteq R\langle 1, s, \dots, s^{n-1} \rangle$  by inductive hypothesis.

“(ii) $\Rightarrow$ (iii)”. Use  $T = R[s]$ .

“(iii) $\Rightarrow$ (i)” (determinant trick). Assume  $s \in T = R\langle y_1, \dots, y_n \rangle$  for some  $y_1, \dots, y_n \in S$ . Then for  $j = 1, \dots, n$ ,  $sy_j \in T$  and so there exist  $a_{1j}, \dots, a_{nj} \in R$  such that  $\sum_{i=1}^n \delta_{ij} sy_i = sy_j = \sum_{i=1}^n a_{ij} y_i$ , i.e.,  $\sum_{i=1}^n (\delta_{ij} s - a_{ij}) y_i = 0$ . Let  $B = (\delta_{ij} s - a_{ij}) \in T^{n \times n}$ . Then  $B\vec{y} = \vec{0}$ . Let  $(\delta_{ij}) \in T^{n \times n}$  be the identity matrix. Then  $(\det(B)(\delta_{ij}))\vec{y} = \text{adj}(B)B\vec{y} = \vec{0}$ ,<sup>†</sup> i.e.,  $\det(B)y_j = 0$  for  $j = 1, \dots, n$ . Since  $1 \in T = R\langle y_1, \dots, y_n \rangle$ , there exist  $c_1, \dots, c_n \in R$  such that  $1 = \sum_{j=1}^n c_j y_j$ . So  $\det(\delta_{ij} s - a_{ij}) = \det(B) \cdot 1 = \det(B) \sum_{j=1}^n c_j y_j = \sum_{j=1}^n c_j \det(B) y_j = 0$ , i.e.,

$$0 = \det(\delta_{ij} s - a_{ij}) = \begin{vmatrix} s - a_{11} & -a_{12} & \cdots & -a_{1n} \\ -a_{21} & s - a_{22} & \cdots & -a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ -a_{n1} & -a_{n2} & \cdots & s - a_{nn} \end{vmatrix} = s^n + c_{n-1}s^{n-1} + \cdots + c_1s + c_0,$$

where  $c_0, \dots, c_{n-1} \in R$  since they are built from  $a_{ij}$ 's  $\in R$ . □

<sup>†</sup>  $A \text{adj}(A) = \text{adj}(A)A = \det(A)(\delta_{ij})$  for  $A \in \text{Mat}_n(R)$ . When  $A$  is invertible,  $\text{adj}(A)$  is unique.

**Theorem 5.14.** *If  $s_1, \dots, s_n \in S$  are integral over  $R$ , then  $R[s_1, \dots, s_n]$  is a finitely generated  $R$ -module.*

*Proof.* Assume  $B = A\langle b_1, \dots, b_m \rangle$  and  $C = B\langle c_1, \dots, c_n \rangle$  with  $A \subseteq B \subseteq C$  an intermediate subring. Claim.  $C = A\langle b_i c_j \mid i = 1, \dots, m, j = 1, \dots, n \rangle$ . “ $\supseteq$ ”. It is straightforward. “ $\subseteq$ ”. Let  $c \in C$ . Then  $c = \sum_{j=1}^n \beta_j c_j$  for some  $\beta_1, \dots, \beta_n \in B$ . Note for  $j = 1, \dots, n$ ,  $\beta_j = \sum_{i=1}^m \alpha_{ij} b_i$  for some  $\alpha_{1j}, \dots, \alpha_{mj} \in A$ . So  $c = \sum_{j=1}^n (\sum_{i=1}^m \alpha_{ij} b_i) c_j = \sum_{i=1}^m \sum_{j=1}^n \alpha_{ij} b_i c_j$ .

Since  $s_1$  is integral over  $R$ , by Proposition 5.13,  $R[s_1]$  is a finitely generated  $R$ -module. Since  $s_2$  is integral over  $R$ , clearly  $s_2$  is integral over  $R[s_1]$  and then  $R[s_1, s_2] = R[s_1][s_2]$  is a finitely generated  $R[s_1]$ -module. So  $R[s_1, s_2]$  is a finitely generated  $R$ -module by our result. Continuing in this fashion, we have  $R[s_1, \dots, s_n]$  is a finitely generated  $R$ -module.  $\square$

**Theorem 5.15.** *Let  $\bar{R} := \{s \in S \mid s \text{ is integral over } R\}$ . Then  $R \subseteq \bar{R} \subseteq S$  is an intermediate subring. So for  $s, s' \in S$  integral over  $R$ , the elements  $s \pm s'$  and  $ss'$  are integral over  $R$ .*

*Proof.*  $R \subseteq \bar{R}$  is straightforward. Since  $s, s'$  are integral over  $R$ ,  $T := R[s, s']$  is a finitely generated  $R$ -module by Theorem 5.14. So  $s \pm s', ss'$  are integral over  $R$  by Proposition 5.13(iii). Hence  $s \pm s', ss' \in \bar{R}$ . Since  $R \subseteq S$  is a subring,  $1_S = 1_R \in \bar{R}$ . So by subring test,  $\bar{R} \subseteq S$  is a subring.  $\square$

**Note.** Let  $s, s' \in R$  be integral over  $R$ . Assume  $s, s'$  satisfies a monic  $f, g \in R[X]$  of degree  $m, n$ , respectively. Since  $s'$  also satisfies the monic  $g \in R[s][X]$  of degree  $n$ , by the proof “(i) $\Rightarrow$ (ii)” of Proposition 5.13, we have

$$\begin{aligned} R[s, s'] &= R[s][s'] = R[s]\langle 1, s', \dots, s'^{n-1} \rangle = R\langle 1, s, \dots, s^{m-1} \rangle \langle 1, s', \dots, s'^{n-1} \rangle \\ &= R\langle 1, s', \dots, s'^{n-1}, s, ss', \dots, ss'^{n-1}, \dots, s^{m-1}, s^{m-1}s', s^{m-1}s'^{n-1} \rangle, \end{aligned}$$

which has  $mn$  generators. Hence by the proof “(iii) $\Rightarrow$ (i)” of Proposition 5.13, we have all elements in  $R[s, s']$ , e.g.,  $s \pm s, ss'$  satisfy a monic polynomial of degree  $mn$  in  $R[X]$ .

**Definition 5.16.**  $\bar{R} = \{s \in S \mid s \text{ is integral over } R\}$  is the *integral closure* of  $R$  in  $S$ .

If  $\bar{R} = S$ , then  $S$  is *integral* over  $R$ . If  $\bar{R} = R$ , then  $R$  is *integrally closed* in  $S$ .

**Example 5.17.** (a)  $\mathbb{Z}[i]$  is integral over  $\mathbb{Z}$  with  $\bar{\mathbb{Z}} = \mathbb{Z}[i]$ .

(b)  $\mathbb{Z}$  is integrally closed in  $\mathbb{Q}$  with  $\bar{\mathbb{Z}} = \mathbb{Z}$ .

(c)  $\bar{\mathbb{Z}} = \mathbb{Z}[i]$  in  $\mathbb{Q}(i)$ .

**Definition 5.18.** Let  $\varphi : R \rightarrow S$  be a ring homomorphism. Then  $\varphi$  is *integral* if  $\text{Im}(\varphi) \subseteq S$  is an integral extension.

**Theorem 5.19.** *The following are equivalent.*

- (i)  $S$  is a finitely generated  $R$ -module.
- (ii)  $S = R[s_1, \dots, s_n]$  for some  $s_1, \dots, s_n$  and is integral over  $R$ .
- (iii)  $S = R[s_1, \dots, s_n]$  for some  $s_1, \dots, s_n$  integral over  $R$ .

*Proof.* “(i) $\Rightarrow$ (ii)”. Assume  $S = R\langle s_1, \dots, s_n \rangle$ . Then  $S = R\langle s_1, \dots, s_n \rangle \subseteq R[s_1, \dots, s_n] \subseteq S$ . So  $S = R[s_1, \dots, s_n]$ . Note there exists an intermediate subring  $R \subseteq R[s_1, \dots, s_n] := T \subseteq S$  such that  $T$  is a finitely generated  $R$ -module. Then  $s_1, \dots, s_n \in S$  are integral over  $R$  by Proposition 5.13. Since  $\bar{R} \subseteq S$  is a subring by Theorem 5.15,  $S = R[s_1, \dots, s_n] \subseteq \bar{R} \subseteq S$  by Fact 5.11(c). So  $\bar{R} = S$ .

“(ii) $\Rightarrow$ (iii)”. Done.

“(iii) $\Rightarrow$ (i)”. By Theorem 5.14.  $\square$

**Corollary 5.20.** If  $R \subseteq S$  and  $S \subseteq T$  are integral extensions, then  $R \subseteq T$  is an integral extension.

*Proof.* Let  $t \in T$ . Then  $t$  is integral over  $S$ . So  $t^n + s_{n-1}t^{n-1} + \dots + s_0 = 0$  for some  $n \geq 1$  and  $s_0, \dots, s_{n-1} \in S$ . So  $t$  is integral over  $R[s_0, \dots, s_{n-1}]$ . Hence  $R[s_0, \dots, s_{n-1}, t] = R[s_0, \dots, s_{n-1}][t]$  is a finitely generated  $R[s_0, \dots, s_{n-1}]$ -module by Proposition 5.13. Since  $S$  is integral over  $R$  and  $s_0, \dots, s_{n-1} \in S$ ,  $s_0, \dots, s_{n-1}$  are integral over  $R$ . So  $R[s_0, \dots, s_{n-1}]$  is a finitely generated  $R$ -module by Theorem 5.14. Thus,  $R[s_0, \dots, s_{n-1}, t]$  is a finitely generated  $R$ -module by the claim in the proof of Theorem 5.14. Therefore,  $t$  is integral over  $R$  by Proposition 5.13(iii).  $\square$

**Corollary 5.21.** If  $\bar{R}$  is an integral closure of  $R$  in  $S$ , then  $\bar{R}$  is integrally closed in  $S$ , i.e.,  $\overline{\bar{R}} = \bar{R}$ .

*Proof.* Let  $s \in \overline{\bar{R}}$ . Then  $s \in S$  be integral over  $\bar{R}$ . So  $R \subseteq \bar{R} \subseteq \bar{R}[s]$  are integral extensions by Theorem 5.15. Hence  $R \subseteq \bar{R}[s]$  is an integral extension by Corollary 5.20. So  $s$  is integral over  $\bar{R}$ , i.e.,  $s \in \bar{R}$ .  $\square$

**Proposition 5.22.** Let  $R \subseteq S$  be an integral extension.

- (a) If  $\mathfrak{b} \leq S$  and  $\mathfrak{a} = R \cap \mathfrak{b}$ , then  $R/\mathfrak{a} \rightarrow S/\mathfrak{b}$  given by  $r + \mathfrak{a} \mapsto r + \mathfrak{b}$  is 1-1 and integral.
- (b) If  $U \subseteq R$  is multiplicatively closed, then  $U^{-1}R \subseteq U^{-1}S$  given by  $\frac{r}{u} \mapsto \frac{r}{u}$  is an integral extension.

*Proof.* (a) Consider

$$\begin{array}{ccc} R & \xrightarrow[\rho]{\subseteq} & S \\ \downarrow \tau & \searrow \rho & \downarrow \pi \\ R/\mathfrak{a} & \xrightarrow[\exists \bar{\rho}]{\subseteq} & S/\mathfrak{b} \\ \bar{r} & \xrightarrow{\quad} & \bar{r} \end{array}$$

Since  $\text{Ker}(\rho) = \text{Ker}(\pi) \cap R = \mathfrak{b} \cap R = \mathfrak{a}$ , by the first isomorphism,  $R/\mathfrak{a} \cong \text{Im}(\bar{\rho}) \subseteq S/\mathfrak{b}$ .

Let  $\bar{s} \in S/\mathfrak{b}$ . Then  $s$  is integral over  $R$  since  $S$  is integral over  $R$ . So  $s$  satisfies  $X^n + \sum_{i=0}^{n-1} a_i X^i$  for some  $a_0, \dots, a_{n-1} \in R$ . Hence  $\bar{s}$  satisfies  $X^n + \sum_{i=0}^{n-1} \bar{a}_i X^i$  for some  $\bar{a}_0, \dots, \bar{a}_{n-1} \in R/\mathfrak{a} \cong \text{Im}(\bar{\rho})$ .

(b) Let  $\frac{s}{u} \in U^{-1}S$  with  $s \in S$  and  $u \in U$ . Then  $s$  is integral over  $R$ . So  $s^n + a_{n-1}s^{n-1} + \dots + a_0 = 0$  for some  $a_0, \dots, a_{n-1} \in R$ . Hence

$$0 = \frac{s^n + a_{n-1}s^{n-1} + \dots + a_1 s + a_0}{u^n} = \left(\frac{s}{u}\right)^n + \left(\frac{a_{n-1}}{u}\right)\left(\frac{s}{u}\right)^{n-1} + \dots + \left(\frac{a_1}{u^{n-1}}\right)\left(\frac{s}{u}\right) + \left(\frac{a_0}{u^n}\right)$$

for some  $\frac{a_0}{u^n}, \frac{a_1}{u^{n-1}}, \dots, \frac{a_{n-1}}{u} \in U^{-1}R$ .  $\square$



**Discussion 5.23.** Let  $\mathfrak{p} \in \text{Spec}(R)$ . When does there exist  $\mathfrak{q} \in \text{Spec}(S)$  such that  $\mathfrak{p} = \mathfrak{q} \cap R$ ? i.e., when is the induced map  $\text{Spec}(S) \rightarrow \text{Spec}(R)$  surjective?

By Cohen-Seidenberg, it is a surjection when  $S$  is integral over  $R$ .

Let  $R \subseteq S$  be an integral extension.

**Proposition 5.24.** Let  $S$  be an integral domain. Then  $R$  is a field if and only if  $S$  is a field.

*Proof.* “ $\Rightarrow$ ”. Assume  $R$  is a field. Let  $0 \neq s \in S$ . Then  $s$  is integral over  $R$  since  $S$  is integral over  $R$ . So there exists  $n := \min\{\deg(f) \mid s \text{ satisfies a monic } f \in R[X]\}$ . Then  $s^n + a_{n-1}s^{n-1} + \cdots + a_0 = 0$  for some  $a_0, \dots, a_{n-1} \in R$ . Suppose  $a_0 = 0$ . Then  $s(s^{n-1} + \cdots + a_1) = 0$ . Since  $s \neq 0$  and  $S$  is an integral domain,  $s^{n-1} + \cdots + a_1 = 0$ , contradicting the minimality of  $n$ . So  $a_0 \neq 0$ . Since  $R$  is a field,  $a_0 \in R^\times \subseteq S^\times$ . Hence  $s(s^{n-1} + \cdots + a_1) = -a_0 \in S^\times$ . Thus,  $s \in S^\times$ .

“ $\Leftarrow$ ”. Assume  $S$  is a field. Let  $0 \neq r \in R \subseteq S$ . Then  $r^{-1} \in S$ . Note  $r^{-1}$  is integral over  $R$  since  $S$  is integral over  $R$ . Then  $r^{n-1}[(r^{-1})^n + a_{n-1}(r^{-1})^{n-1} + \cdots + a_1(r^{-1}) + a_0] = 0$  for some  $a_0, a_1, \dots, a_{n-1} \in R$ . So  $r^{-1} + \underbrace{a_{n-1} + \cdots + a_1 r^{n-2} + a_0 r^{n-1}}_{\in R} = 0$ . Hence  $r^{-1} \in R$ .  $\square$

**Example.** Conclusion of Proposition 5.24 fails if  $S$  is not an integral domain. Let  $k$  be a field. Restrict the domain of the projection  $\varphi : k[X] \rightarrow k[X]/(X^2)$ , we have an induced ring homomorphism  $\varphi|_k : k \rightarrow k[X]/(X^2)$ . Since  $\varphi|_k(1) = \bar{1} \neq 0$  in  $k[X]/(X^2)$ ,  $\varphi|_k \neq 0$ . Also, since  $k$  is a field,  $\varphi|_k$  is 1-1. So we regard  $R := k$  as a subring of  $S := k[X]/(X^2)$ . Let  $x = \bar{X} \in S$ . Then  $x$  is integral over  $k$  since  $x^2 = 0$ . So  $S = k[x]$  is integral over  $k$ . However,  $R$  is a field but  $S$  is not a field.

Let  $\epsilon \neq 0$  and  $\epsilon^2 = 0$  in a ring extension  $T \supseteq k$ , then  $\varphi : k[X] \rightarrow k[\epsilon]$  given by  $f \mapsto f(\epsilon)$  is a ring epimorphism with  $\text{Ker}(\varphi) = (X^2)$ , so  $k[X]/(X^2) \cong k[\epsilon] = k\epsilon + k$ .

**Corollary 5.25.** Let  $\mathfrak{q} \in \text{Spec}(S)$  and  $\mathfrak{p} = \mathfrak{q} \cap R$ . Then  $\mathfrak{p} \in \text{m-Spec}(R)$  if and only if  $\mathfrak{q} \in \text{m-Spec}(S)$ .

*Proof.* Since  $S$  is integral over  $R$ ,  $R/\mathfrak{p} \subseteq S/\mathfrak{q}$  is an integral extension by Proposition 5.22(a). Since  $S/\mathfrak{q}$  is an integral domain, by Proposition 5.24,  $R/\mathfrak{p}$  is a field if and only if  $S/\mathfrak{q}$  is a field.  $\square$

**Theorem 5.26.**  $\text{Spec}(S) \rightarrow \text{Spec}(R)$  given by  $\mathfrak{q} \mapsto \mathfrak{q} \cap R$  is a surjection, i.e., for  $\mathfrak{p} \in \text{Spec}(R)$ , there exists  $\mathfrak{q} \in \text{Spec}(S)$  such that  $\mathfrak{p} = \mathfrak{q} \cap R$ .

*Proof.* Let  $U = R \setminus \mathfrak{p}$ . Consider

$$\begin{array}{ccccc} & & \mathfrak{p} & & \\ & & \uparrow & & \\ & & R & \xrightarrow{\subseteq} & S \\ & & \downarrow \psi & & \downarrow \rho \\ & & U^{-1}R & \xrightarrow{\subseteq} & U^{-1}S \\ \mathfrak{p}_{\mathfrak{p}} = R_{\mathfrak{p}} \cap Q & \longleftarrow & & & \longrightarrow Q \end{array}$$

Since  $R \subseteq S$  is an integral extension,  $U^{-1}R \subseteq U^{-1}S$  is an integral extension by Proposition 5.22(b). Since  $0 \neq R \subseteq S$ ,  $0 \neq R_{\mathfrak{p}} = U^{-1}R \subseteq U^{-1}S$ . So there exists  $Q \in \text{m-Spec}(U^{-1}S)$ . By Corollary 5.25,  $Q \cap R_{\mathfrak{p}} \in \text{m-Spec}(R_{\mathfrak{p}}) = \{\mathfrak{p}_{\mathfrak{p}}\}$  by Corollary 3.14. So  $Q \cap R_{\mathfrak{p}} = \mathfrak{p}_{\mathfrak{p}}$ . Consider  $\psi : R \rightarrow U^{-1}R$ . Since  $U \cap \mathfrak{p} = \emptyset$ , by Proposition 3.13, we have  $\mathfrak{p} \cdot U^{-1}(U^{-1}R) = \mathfrak{p} \cdot U^{-1}R \neq U^{-1}R = U^{-1}(\mathfrak{p} \cdot U^{-1}R)$ . So by Theorem 3.24,  $\mathfrak{p} = \psi^{-1}(\mathfrak{p} \cdot U^{-1}R) = \psi^{-1}(\mathfrak{p}_{\mathfrak{p}}) = \psi^{-1}(Q \cap R_{\mathfrak{p}}) = \rho^{-1}(Q) \cap R$ . Let  $\mathfrak{q} := \rho^{-1}(Q)$ . Since  $Q \in \text{Spec}(U^{-1}S)$ ,  $\mathfrak{q} \in \text{Spec}(S)$  by Fact 1.16.  $\square$

**Proposition 5.27.** Let  $\mathfrak{q}, \mathfrak{q}' \in \text{Spec}(S)$  such that  $\mathfrak{q} \cap R = \mathfrak{q}' \cap R$ . Then  $\mathfrak{q} \subseteq \mathfrak{q}'$  if and only if  $\mathfrak{q} = \mathfrak{q}'$ .

*Proof.* Let  $\mathfrak{p} = \mathfrak{q} \cap R = \mathfrak{q}' \cap R \in \text{Spec}(R)$  by Fact 1.16. Let  $U = R \setminus \mathfrak{p}$ . By prime correspondence for localization,  $\text{Spec}(U^{-1}S) \leftrightarrow \{\gamma \in \text{Spec}(S) \mid \gamma \cap (R \setminus \mathfrak{p}) = \emptyset\} = \{\gamma \in \text{Spec}(S) \mid \gamma \cap R \subseteq \mathfrak{p}\}$  given by  $U^{-1}\gamma \leftrightarrow \gamma$ . So  $U^{-1}\mathfrak{q}, U^{-1}\mathfrak{q}' \in \text{Spec}(U^{-1}S)$ . Hence  $U^{-1}\mathfrak{q} \cap R_{\mathfrak{p}}, U^{-1}\mathfrak{q}' \cap R_{\mathfrak{p}} \in \text{Spec}(R_{\mathfrak{p}})$ .

$$\begin{array}{ccc}
 \mathfrak{p} & \xleftarrow{\quad} & \mathfrak{q}, \mathfrak{q}' \\
 \downarrow & \begin{array}{c} R \xrightarrow{\subseteq} S \\ \downarrow \psi \quad \downarrow \rho \\ U^{-1}R \xrightarrow{\subseteq} U^{-1}S \end{array} & \downarrow \\
 \mathfrak{p}_{\mathfrak{p}} & & U^{-1}\mathfrak{q}, U^{-1}\mathfrak{q}'
 \end{array}$$

Since  $U^{-1}\mathfrak{q}, U^{-1}\mathfrak{q}' \supseteq U^{-1}\mathfrak{p} = \mathfrak{p}_{\mathfrak{p}}$  and  $R_{\mathfrak{p}} \supseteq \mathfrak{p}_{\mathfrak{p}}, R_{\mathfrak{p}} \supsetneq U^{-1}\mathfrak{q} \cap R_{\mathfrak{p}}, U^{-1}\mathfrak{q}' \cap R_{\mathfrak{p}} \supseteq \mathfrak{p}_{\mathfrak{p}} \in \text{m-Spec}(R_{\mathfrak{p}})$ . So  $U^{-1}\mathfrak{q} \cap R_{\mathfrak{p}} = \mathfrak{p}_{\mathfrak{p}} = U^{-1}\mathfrak{q}' \cap R_{\mathfrak{p}}$ .<sup>†</sup> Since  $R \subseteq S$  is an integral extension,  $U^{-1}R \subseteq U^{-1}S$  is an integral extension by Proposition 5.22(b). So by Corollary 5.25,  $U^{-1}\mathfrak{q}, U^{-1}\mathfrak{q}' \in \text{m-Spec}(U^{-1}S)$ . Also, since  $U^{-1}\mathfrak{q} \subseteq U^{-1}\mathfrak{q}', U^{-1}\mathfrak{q} = U^{-1}\mathfrak{q}'$ . Thus,  $\mathfrak{q} = \mathfrak{q}'$  by the prime correspondence for localization.  $\square$

**Theorem 5.28** (Going up theorem). Let  $\mathfrak{p}_1 \subseteq \cdots \subseteq \mathfrak{p}_n$  be a chain in  $\text{Spec}(R)$  and  $\mathfrak{q}_1 \subseteq \cdots \subseteq \mathfrak{q}_m$  ( $m < n$ ) be a chain in  $\text{Spec}(S)$  such that  $\mathfrak{p}_i = \mathfrak{q}_i \cap R$  for  $i = 1, \dots, m$ . Then there exists a chain  $\mathfrak{q}_m \subseteq \cdots \subseteq \mathfrak{q}_n$  in  $\text{Spec}(S)$  such that  $\mathfrak{q}_i \cap R = \mathfrak{p}_i$  for  $i = 1, \dots, n$ .

*Proof.* By induction on  $n - m$ . It suffices to consider the case  $n = 2$  and  $m = 1$ . Need to find  $\mathfrak{q}_2 \in V(\mathfrak{q}_1) \subseteq \text{Spec}(S)$  such that  $\mathfrak{q}_2 \cap R = \mathfrak{p}_2$ . Consider

$$\begin{array}{ccc}
 \mathfrak{p}_2 & \xleftarrow{\quad} & \mathfrak{q}_2 \\
 \uparrow & \begin{array}{c} R \xrightarrow{\subseteq} S \\ \downarrow \pi \quad \downarrow \tau \\ R/\mathfrak{p}_1 \xrightarrow{\subseteq} S/\mathfrak{q}_1 \end{array} & \uparrow \\
 \mathfrak{p}_2/\mathfrak{p}_1 & \xleftarrow{\quad} & \mathfrak{q}_2/\mathfrak{q}_1
 \end{array}$$

Since  $R \subseteq S$  is an integral extension and  $\mathfrak{p}_1 = \mathfrak{q}_1 \cap R$ , by Proposition 5.22(a),  $R/\mathfrak{p}_1 \subseteq S/\mathfrak{q}_1$  is an integral extension. Also, since  $\mathfrak{p}_2/\mathfrak{p}_1 \in \text{Spec}(R/\mathfrak{p}_1)$  by prime correspondence for quotients, there exists  $\mathfrak{q}_2/\mathfrak{q}_1 \in \text{Spec}(S/\mathfrak{q}_1)$  such that  $(\mathfrak{q}_2/\mathfrak{q}_1) \cap (R/\mathfrak{p}_1) = \mathfrak{p}_2/\mathfrak{p}_1$  by Theorem 5.26.

Note  $x + \mathfrak{p}_1 \in (R \cap \mathfrak{q}_2)/\mathfrak{p}_1$  if and only if  $x \in R$  and  $x \in \mathfrak{q}_2$  if and only if  $x + \mathfrak{q}_1 = x + \mathfrak{p}_1 \in (\mathfrak{q}_2/\mathfrak{q}_1) \cap (R/\mathfrak{p}_1) = \mathfrak{p}_2/\mathfrak{p}_1$  since we can regard  $R/\mathfrak{p}_1 \subseteq S/\mathfrak{q}_1$  by Proposition 5.22(a). So  $(\mathfrak{q}_2 \cap R)/\mathfrak{p}_1 = \mathfrak{p}_2/\mathfrak{p}_1$ . Thus,  $\mathfrak{q}_2 \cap R = \mathfrak{p}_2$  by prime correspondence for quotients.  $\square$

**Example 5.29.** Integral assumption is crucial.

(a)  $\mathbb{Z} \subseteq \mathbb{Q}$ . Let  $0 \subseteq 2\mathbb{Z}$  be a chain in  $\text{Spec}(\mathbb{Z})$ , Note 0 is a (unique) chain in  $\text{Spec}(\mathbb{Q}) = \{0\}$ .

(b)  $\mathbb{Z} \subseteq \mathbb{Z}[X]$ . Let  $0 \subseteq 2\mathbb{Z}$  be a chain in  $\text{Spec}(\mathbb{Z})$  and  $\langle 2X - 1 \rangle$  be a chain in  $\text{Spec}(\mathbb{Z}[X])$  since  $\frac{\mathbb{Z}[X]}{(2X-1)} \cong \mathbb{Z}_2^{\dagger} = \mathbb{Z}[\frac{1}{2}] \subseteq \mathbb{Q}$  given by  $\bar{X} \mapsto \frac{1}{2}$  and  $\mathbb{Z}[\frac{1}{2}]$  is an integral domain. Note  $\mathbb{Z} \cap \langle 2X - 1 \rangle = 0$ .

<sup>†</sup>  $U^{-1}\mathfrak{q} \cap R_{\mathfrak{p}} = U^{-1}\mathfrak{q} \cap U^{-1}R = U^{-1}(\mathfrak{q} \cap R) = U^{-1}\mathfrak{p} = \mathfrak{p}_{\mathfrak{p}} = U^{-1}\mathfrak{p} = U^{-1}(\mathfrak{q}' \cap R) = U^{-1}\mathfrak{q}' \cap U^{-1}R = U^{-1}\mathfrak{q}' \cap R_{\mathfrak{p}}$ .

<sup>‡</sup>  $\mathbb{Z}_2$  is the localization of  $\mathbb{Z}$  away from 2 while  $\mathbb{Z}_{(2)}$  is the localization of  $\mathbb{Z}$  at 2.

Suppose there exists  $Q \in \text{Spec}(\mathbb{Z}[X])$  such that  $\langle 2X - 1 \rangle \subseteq Q$  and  $\mathbb{Z} \cap Q = 2\mathbb{Z}$ . Then  $2, 2x - 1 \in Q$ . So  $1 \in Q$ , i.e.,  $Q = \mathbb{Z}[X]$ , a contradiction.

This example also shows the need for integral assumption in Proposition 5.27 because

- (1)  $0, \langle 2X - 1 \rangle \in \text{Spec}(\mathbb{Z}[X])$  and  $\mathbb{Z} \cap 0 = 0 = \mathbb{Z} \cap \langle 2X - 1 \rangle$ , but  $0 \subsetneq \langle 2X - 1 \rangle$ ;
- (2)  $\langle 2 \rangle, \langle 2, X \rangle \in \text{Spec}(\mathbb{Z}[X])$  and  $\mathbb{Z} \cap \langle 2 \rangle = 2\mathbb{Z} = \mathbb{Z} \cap \langle 2, X \rangle$ , but  $\langle 2 \rangle \subsetneq \langle 2, X \rangle$ .

**Proposition 5.30.** Let  $U \subseteq R$  be multiplicatively closed. Let  $\bar{R}$  be the integral closure of  $R$  in  $S$  and  $\overline{U^{-1}R}$  be the integral closure of  $U^{-1}R$  in  $U^{-1}S$ . Then  $\overline{U^{-1}R} = U^{-1}\bar{R}$ .

*Proof.* “ $\supseteq$ ”. Since  $R \subseteq \bar{R} \subseteq S$  with  $R \subseteq \bar{R}$  integral, we have  $U^{-1}R \subseteq U^{-1}\bar{R} \subseteq U^{-1}S$  with  $U^{-1}R \subseteq U^{-1}\bar{R}$  integral by Proposition 5.22(b). So  $U^{-1}\bar{R} \subseteq \overline{U^{-1}R}$ .

“ $\subseteq$ ”. Let  $\frac{s}{u} \in \overline{U^{-1}R} \subseteq U^{-1}S$ . Then  $0 = (\frac{s}{u})^n + (\frac{a_{n-1}}{v_{n-1}})(\frac{s}{u})^{n-1} + \cdots + (\frac{a_1}{v_1})(\frac{s}{u}) + (\frac{a_0}{v_0})$  in  $U^{-1}S$  for some  $a_0, \dots, a_{n-1} \in R$  and  $v_0, \dots, v_{n-1} \in U$ . Let  $v := v_0 \cdots v_{n-1} \in U$  and multiply the equation by  $(uv)^n$ ,  $0 = (vs)^n + \underbrace{(u \frac{v}{v_{n-1}} a_{n-1})(vs)^{n-1}}_{b_{n-1} \in R} + \cdots + \underbrace{(u^{n-1} \frac{v^{n-1}}{v_1} a_1)(vs)}_{b_1 \in R} + \underbrace{(u^n \frac{v^n}{v_0} a_0)}_{b_0 \in R}$  in  $U^{-1}R$ . So there exists  $w \in U \subseteq R$  such that  $0 = w^n \cdot 0 = (wvs)^n + \underbrace{(wb_{n-1})(wvs)^{n-1}}_{\in R} + \cdots + \underbrace{(w^{n-1}b_1)(wvs)}_{\in R} + \underbrace{(w^n b_0)}_{\in R}$ .

Hence  $wvs \in \bar{R}$ . Thus,  $\frac{s}{u} = \frac{wvs}{wvu} \in U^{-1}\bar{R}$ .  $\square$

**Definition 5.31.** If  $R$  is an integral domain, then  $R$  is *integrally closed* if it is integrally closed in the field of fraction  $Q(R)$ .

**Example 5.32.** (a)  $\mathbb{Z}$  is integrally closed.

(b) Any UFD is integrally closed.

(c) Let  $R := k[X^2, XY, Y^2] \subseteq k[X, Y]$ . Then  $R$  is not a UFD since  $X^2Y^2 = (XY)(XY)$  with  $X^2, Y^2, XY$  irreducible in  $R$ .

Note  $Q(R) = k(X, Y) = Q(k[X, Y])$ . Since  $X, Y$  satisfies  $Z^2 - X^2, Z^2 - Y^2 \in R[Z]$ , respectively, we have  $X, Y$  are integral over  $R$ . Also, since  $k$  is integral over  $R$ ,  $R \subseteq k[X, Y]$  is integral. Since  $k[X, Y]$  is a UFD,  $k[X, Y]$  is integrally closed by (b). Hence  $R$  is integrally closed by Corollary 5.20.

Claim.  $R \cong \frac{k[U, V, W]}{\langle V^2 - UW \rangle}$ . Let  $\varphi : k[U, V, W] \rightarrow k[X, Y]$  be a ring homomorphism given by  $U \mapsto X^2$ ,  $V \mapsto XY$  and  $W \mapsto Y^2$ . Then  $\text{Im}(\varphi) = k[X^2, XY, Y^2]$  and  $\langle V^2 - UW \rangle \subseteq \text{Ker}(\varphi)$ . Let  $f \in \text{Ker}(\varphi)$ . Then by long division,  $f = (V^2 - UW)q + r$  for some  $q, r \in k[U, W][V]$  and  $\deg(r) < 2$  in  $k[U, W][V]$ . Since  $\varphi(f) = 0$  and  $\varphi$  is a ring homomorphism,  $((XY)^2 - X^2Y^2)\varphi(q) + \varphi(r) = 0$ , i.e.,  $\varphi(r) = 0$ . Note  $r = aV + b$  for some  $a, b \in k[U, W]$ . So  $a(X^2, Y^2)XY + b(X^2, Y^2) = 0$ . Hence  $a = 0 = b$ , i.e.,  $r = 0$ . So  $f \in \langle V^2 - UW \rangle$ .

**Example.** If  $S$  is noetherian, then  $R$  is not necessarily noetherian. Let  $\bar{\mathbb{Q}}$  be the algebraic closure of  $\mathbb{Q}$  in  $\mathbb{C}$  and  $R := \mathbb{Q} + X\bar{\mathbb{Q}}[X] \subseteq \bar{\mathbb{Q}}[X] =: S$ . Note  $R \subseteq S$  is an integral extension since  $\bar{\mathbb{Q}}$  is algebraic over  $\mathbb{Q} \subseteq R$  and  $X \in R$ , but  $R$  is not noetherian since  $[\bar{\mathbb{Q}} : \mathbb{Q}] = \infty$ .

**Lemma 5.33.** If  $R$  is an integral domain, then  $R = \bigcap_{\mathfrak{m} \in \text{m-Spec}(R)} R_{\mathfrak{m}} \subseteq Q(R)$ .

*Proof.* “ $\subseteq$ ”. Since  $R$  is an integral domain, we have  $R \setminus \mathfrak{m} \subseteq \text{NZD}(R)$ . So  $R \subseteq R_{\mathfrak{m}} \subseteq Q(R)$  for  $\mathfrak{m} \in \text{m-Spec}(R)$ . Hence  $R \subseteq \bigcap_{\mathfrak{m} \in \text{m-Spec}(R)} R_{\mathfrak{m}} \subseteq Q(R)$ .

“ $\supseteq$ ”. Let  $x \in \bigcap_{\mathfrak{m} \in \text{m-Spec}(R)} R_{\mathfrak{m}}$ . Let  $I = \{r \in R \mid rx \in R\} =: (R :_R x) \leq R$ . By Proposition 3.12(f),  $I_{\mathfrak{m}} = (R :_R x)_{\mathfrak{m}} = (R_{\mathfrak{m}} :_{R_{\mathfrak{m}}} x) = R_{\mathfrak{m}}$  for  $\mathfrak{m} \in \text{m-Spec}(R)$ . So  $I \cap (R \setminus \mathfrak{m}) \neq \emptyset$ , i.e.,  $I \not\subseteq \mathfrak{m}$  for  $\mathfrak{m} \in \text{m-Spec}(R)$ . Hence  $I = R$ , i.e.,  $1 \in I = (R :_R x)$ . Thus,  $x = 1 \cdot x \in R$ .  $\square$

**Proposition 5.34** (being integrally closed is a “local condition”). Let  $R$  be an integral domain. Then the following are equivalent.

- (i)  $R$  is integrally closed.
- (ii)  $U^{-1}R$  is integrally closed for multiplicatively closed  $U \subseteq R$  with  $0 \notin U$ .
- (iii)  $R_{\mathfrak{p}}$  is integrally closed for  $\mathfrak{p} \in \text{Spec}(R)$ .
- (iv)  $R_{\mathfrak{m}}$  is integrally closed for  $\mathfrak{m} \in \text{m-Spec}(R)$ .

*Proof.* “(i) $\Rightarrow$ (ii)”. Assume  $R$  is integrally closed. Let  $U \subseteq R$  be multiplicatively closed with  $0 \notin U$ . Since  $R$  is an integral domain and  $0 \notin U$ ,  $U \subseteq \text{NZD}(R)$ . So  $R \subseteq U^{-1}R \subseteq Q(R) =: S$  are subrings. By Proposition 5.30,  $U^{-1}\bar{R} = U^{-1}\bar{R} = U^{-1}R$  since  $R$  is integral closed in  $Q(R)$ . So  $U^{-1}R$  is integrally closed in  $U^{-1}S = Q(R)$ . Also, since  $Q(U^{-1}R) = Q(R)^{\dagger}$ ,  $U^{-1}R$  is integrally closed.

“(ii) $\Rightarrow$ (iii)” and “(iii) $\Rightarrow$ (iv)”. Done.

“(iv) $\Rightarrow$ (i)”. Assume  $R_{\mathfrak{m}}$  is integrally closed for  $\mathfrak{m} \in \text{m-Spec}(R)$ . Since  $R$  is an integral domain and  $R \subseteq R_{\mathfrak{m}} \subseteq Q(R)$ ,  $Q(R_{\mathfrak{m}}) = Q(R)$  for  $\mathfrak{m} \in \text{m-Spec}(R)$ . Let  $x \in \bar{R}$ , where  $\bar{R}$  is the integral closure of  $R$  in  $Q(R)$ . Then  $x \in Q(R) = Q(R_{\mathfrak{m}})$  and  $x$  is integral over  $R \subseteq R_{\mathfrak{m}}$  for  $\mathfrak{m} \in \text{m-Spec}(R)$ . So  $x \in \bar{R}_{\mathfrak{m}} = R_{\mathfrak{m}}$  for  $\mathfrak{m} \in \text{m-Spec}(R)$ . Thus, by Lemma 5.33,  $x \in \bigcap_{\mathfrak{m} \in \text{m-Spec}(R)} R_{\mathfrak{m}} = R$ .  $\square$

Let  $R \subseteq S$  be a subring.

**Definition 5.35.** Let  $\mathfrak{a} \leq R$ .  $s \in S$  is *integral over*  $\mathfrak{a}$  if  $s$  satisfies  $f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0$  for some  $n \geq 1$  and  $a_0, \dots, a_{n-1} \in \mathfrak{a}$ .

The *integral closure* of  $\mathfrak{a}$  in  $S$  is

$$\bar{\mathfrak{a}} = \{s \in S \mid s \text{ is integral over } \mathfrak{a}\}.$$

**Warning 5.36.** There exists another notion of integral closure of an ideal.

**Lemma 5.37.** Let  $\bar{R}$  be the integral closure of  $R$  in  $S$  and  $\mathfrak{a} \leq R$ . Then  $\bar{\mathfrak{a}} = \text{rad}(\mathfrak{a}\bar{R}) \leq \bar{R}$ . So  $\bar{\mathfrak{a}}$  is closed under sums and products.

*Proof.* “ $\subseteq$ ”. Let  $s \in \bar{\mathfrak{a}}$ . Then  $s^n + a_{n-1}s^{n-1} + \cdots + a_0 = 0$  for some  $n \geq 1$  and  $a_0, \dots, a_{n-1} \in \mathfrak{a}$ . So  $s^n = -(a_{n-1}s^{n-1} + \cdots + a_0) \in \mathfrak{a}\bar{\mathfrak{a}} \subseteq \mathfrak{a}\bar{R}$ . Hence  $s \in \text{rad}(\mathfrak{a}\bar{R})$ .

“ $\supseteq$ ”. Let  $t \in \text{rad}(\mathfrak{a}\bar{R})$ . Then  $t^n \in \mathfrak{a}\bar{R}$  for some  $n \geq 1$ . So  $t^n = \sum_{i=1}^m \alpha_i s_i$  for some  $m \geq 1$ ,  $\alpha_1, \dots, \alpha_m \in \mathfrak{a}$  and  $s_1, \dots, s_m \in \bar{R}$ . Let  $T := R[s_1, \dots, s_m] \subseteq \bar{R} \subseteq S$ . Then  $t^n \in \mathfrak{a}T$ . So  $t^n T \subseteq \mathfrak{a}T$ . Since  $s_1, \dots, s_m$  is integral over  $R$ ,  $T$  is a finitely generated  $R$ -module by Theorem 5.19. By determinant trick as in the proof of Proposition 5.13, we have  $t^n$  is integral over  $\mathfrak{a}$ . So  $(t^n)^l + b_{l-1}(t^n)^{l-1} + \cdots + b_0 = 0$  for some  $l \geq 1$  and  $b_0, \dots, b_{l-1} \in \mathfrak{a}$ . Hence  $t$  is integral over  $\mathfrak{a}$ .  $\square$

---

<sup>†</sup>Fact: If  $R$  is an integral domain and  $R \subseteq S \subseteq Q(S)$ , then  $Q(S) = Q(R)$ .

**Proposition 5.38.** Let  $R$  be integrally closed and  $\bar{\mathfrak{a}}$  be the integral closure of  $\mathfrak{a} \leq R$  in  $S$ . Let  $s \in \bar{\mathfrak{a}}$  and  $g(X) = X^m + c_{m-1}X^{m-1} + \cdots + c_0 \in Q(R)[X]$  be the minimal polynomial of  $s$  over  $Q(R)$ . Then  $c_0, \dots, c_{m-1} \in \text{rad}(\mathfrak{a})$ .

*Proof.* Let  $s_1 := s, s_2, \dots, s_m$  be the roots of  $g(X)$  in some algebraic closure of  $Q(R)$ . Since  $s$  is integral over  $\mathfrak{a}$ ,  $s$  satisfies a monic  $f \in \mathfrak{a}[X] \subseteq Q(R)[X] = Q(R)[X]$ . Also, since  $g$  is the minimal polynomial of  $s$  over  $Q(R)$ , there exists  $h \in Q(R)[X]$  such that  $f = hg$ . Since  $f(s_i) = h(s_i)g(s_i) = 0$ ,  $s_i \in \bar{\mathfrak{a}}$  for  $i = 1, \dots, m$ . Since  $g(X) = (X - s_1) \cdots (X - s_m)$  and  $\bar{\mathfrak{a}} \leq \bar{R}$  by Lemma 5.37,  $c_0, \dots, c_{m-1} \in \bar{\mathfrak{a}} = \text{rad}(\mathfrak{a}\bar{R}) = \text{rad}(\mathfrak{a}R) = \text{rad}(\mathfrak{a})$ .  $\square$

**Theorem 5.39** (Going down theorem). *Let  $R$  be integrally closed and  $S$  be an integral domain. Let  $\mathfrak{p}_1 \supseteq \cdots \supseteq \mathfrak{p}_n$  be a chain in  $\text{Spec}(R)$  and  $\mathfrak{q}_1 \supseteq \cdots \supseteq \mathfrak{q}_m$  ( $m < n$ ) be a chain in  $\text{Spec}(S)$  such that  $\mathfrak{q}_i \cap R = \mathfrak{p}_i$  for  $i = 1, \dots, m$ . Then there exists a chain  $\mathfrak{q}_m \supseteq \cdots \supseteq \mathfrak{q}_n$  in  $\text{Spec}(S)$  such that  $\mathfrak{q}_i \cap R = \mathfrak{p}_i$  for  $i = 1, \dots, n$ .*

*Proof.* As in the going up theorem, assume without loss of generality that  $m = 1$  and  $n = 2$ . Let  $\mathfrak{p} \supseteq \mathfrak{p}'$  be a chain in  $\text{Spec}(R)$  and  $\mathfrak{q} \in \text{Spec}(S)$  such that  $\mathfrak{q} \cap R = \mathfrak{p}$ . Since  $S$  is an integral domain,  $S \setminus \mathfrak{q} \subseteq \text{NZD}(S)$ . So  $S_{\mathfrak{q}} \supseteq S \supseteq R$ . Claim.  $(\mathfrak{p}'S_{\mathfrak{q}}) \cap R = \mathfrak{p}'$ , then (if and only if) there exists  $Q' \in \text{Spec}(S_{\mathfrak{q}})$  such that  $Q' \cap R = \mathfrak{p}'$  by Theorem 3.24, so (if and only if) there exists  $\mathfrak{q} \supseteq \mathfrak{q}' \in \text{Spec}(S)$  such that  $\mathfrak{q}' \cap R = \mathfrak{p}'^{\dagger}$  by prime correspondence for localization.

“ $\supseteq$ ”. By 1.63(a).

“ $\subseteq$ ”. Let  $0 \neq x \in (\mathfrak{p}'S_{\mathfrak{q}}) \cap R$ . Then  $x \in \mathfrak{p}'S_{\mathfrak{q}} = \mathfrak{p}'(S \setminus \mathfrak{q})^{-1}S = (S \setminus \mathfrak{q})^{-1}(\mathfrak{p}'S)$ . So  $x = \frac{s}{v}$  for some  $s \in \mathfrak{p}'S$  and  $v \in S \setminus \mathfrak{q}$ . Since  $R \subseteq S$  is integral,  $\bar{R} = S$ , where  $\bar{R}$  is the integral closure of  $R$  in  $S$ . So  $s \in \mathfrak{p}'S \subseteq \text{rad}(\mathfrak{p}'S) = \text{rad}(\mathfrak{p}'\bar{R}) = \mathfrak{p}'$  by Lemma 5.37. Hence  $s \in S$  is integral over  $\mathfrak{p}'$ . Let  $g(X) = X^r + u_{r-1}X^{r-1} + \cdots + u_0 \in Q(R)[X]$  be the minimal polynomial of  $s$  over  $Q(R)$ . Then by Proposition 5.38,  $u_0, \dots, u_{r-1} \in \text{rad}(\mathfrak{p}') = \mathfrak{p}'$ . Since  $0 \neq x = \frac{s}{v}$  and  $R$  is an integral domain,  $v = sx^{-1}$  in  $Q(R)$ . Note  $v$  satisfies  $X^r + \underbrace{(u_{r-1}x^{-1})}_{t_{r-1}}X^{r-1} + \underbrace{(u_{r-2}x^{-2})}_{t_{r-2}}X^{r-2} + \cdots + \underbrace{(u_0x^{-r})}_{t_0} \in Q(R)[X]$ ,

which is a minimal polynomial for  $v$  over  $Q(R)$  since if  $v$  satisfies a smaller degree polynomial over  $Q(R)$ , then so does  $S$ . Also, since  $v \in S$  is integral over  $R$ , by Proposition 5.38, we have  $t_0, \dots, t_{r-1} \in \text{rad}(\langle 1 \rangle R) = R$ . Suppose  $x \notin \mathfrak{p}'$ . Since  $u_i = t_i x^{r-i} \in \mathfrak{p}' \in \text{Spec}(R)$ ,  $t_i \in \mathfrak{p}'$  for  $i = 0, \dots, r-1$ . So  $v^r = -(t_{r-1}v^{r-1} + t_{r-2}v^{r-2} + \cdots + t_0) \in \mathfrak{p}'S \subseteq \mathfrak{p}S = (\mathfrak{q} \cap R)S \subseteq \mathfrak{q}S = \mathfrak{q} \in \text{Spec}(S)$ . Hence  $v \in \mathfrak{q}$ , a contradiction. Thus,  $x \in \mathfrak{p}'$ .  $\square$

**Theorem 5.40** (Noether normalization). *Let  $k$  be a field and  $k \subseteq R := k[x_1, \dots, x_n]$  be a subring.*

(a) *There exist an intermediate subring  $k \subseteq S \subseteq R$  and  $y_1, \dots, y_d \in R$  such that  $S = k[y_1, \dots, y_d] \cong k[Y_1, \dots, Y_d]$ , a polynomial ring, with  $d \leq n$  and  $R$  integral over  $S$ . So  $R = S[x_1, \dots, x_n]$  is a finitely generated  $S$ -module. Moreover,  $y_i$  is a polynomial in  $x_j$ 's with coefficients in  $k$  for  $i = 1, \dots, d$ .*

(b) *If  $|k| = \infty$ , then we can take some  $d$  and  $y_i = \sum_{j=1}^n a_{ij}x_j$  for some  $a_{i1}, \dots, a_{in} \in k$  for  $i = 1, \dots, d$ .*

(In fact,  $d$  is uniquely determined and is the Krull dimension of  $R$ .)

<sup>†</sup>For “ $\Rightarrow$ ”, take  $\mathfrak{q}' = Q' \cap S$ , then  $\mathfrak{q}' \cap R = (Q' \cap S) \cap R = Q' \cap R = \mathfrak{p}'$ . For “ $\Leftarrow$ ”, take  $Q' = \mathfrak{q}'S_{\mathfrak{q}}$ , then  $Q' \cap R = (\mathfrak{q}'S_{\mathfrak{q}} \cap S) \cap R = \mathfrak{q}' \cap R = \mathfrak{p}'$  by prime correspondence for localization.

*Proof. Definition.* Let  $z_1, \dots, z_m \in R$  and  $k[Z_1, \dots, Z_m]$  be a polynomial ring. Consider the ring homomorphism  $k[Z_1, \dots, Z_m] \xrightarrow{n} k[z_1, \dots, z_m]$  given by  $F \mapsto F(z_1, \dots, z_m)$ .  $z_1, \dots, z_m$  is algebraically independent over  $k$  if  $n$  is 1-1, i.e.,  $n$  is an isomorphism. (No polynomial relations between the  $z_i$ 's.)

Structure of proof: induct on  $n$ . Base case  $n = 0$ :  $R = k$  ( $S = k$ ). Base case  $n = 1$ :  $R = k[x] \xleftarrow{n} k[X]$ . If  $n$  is 1-1, then  $S = R$ . If  $n$  is not 1-1, then  $x$  satisfies some monic  $F \in k[X]$ , so  $x$  is integral over  $k$ , hence  $S = k \subseteq R = k[x]$  with  $d = 0$  and  $S \subseteq R$  an integral extension.

Inductive step: Assume  $n > 1$  and the result is true for rings of form  $k[z_1, \dots, z_{n-1}]$ . If  $x_1, \dots, x_n$  are algebraically independent over  $k$ , then use  $S = R = k[x_1, \dots, x_n] \xleftarrow{n} k[X_1, \dots, X_n]$ . Assume now  $x_1, \dots, x_n$  are not algebraically independent over  $k$ . Re-order  $x_1, \dots, x_n$  such that  $x_1, \dots, x_r$  ( $r < n$ ) are algebraically independent and  $x_1, \dots, x_r, x_s$  are algebraically dependent for  $s = r + 1, \dots, n$ . Then by inductive hypothesis and Corollary 5.20, it suffices to show  $R$  is integral over  $k[w_1, \dots, w_{n-1}]$  for some  $w_1, \dots, w_{n-1} \in R$ . Consider  $k[X_1, \dots, X_n] \xrightarrow{n} k[x_1, \dots, x_n]$ . Then there exists  $0 \neq F \in k[X_1, \dots, X_n]$  such that  $n(F) = 0$ . Let  $e = \deg(F)$  and write  $F = F_0 + F_1 + \dots + F_e$ , where  $F_i$  is homogeneous of degree  $i$  for  $i = 0, \dots, e$ .

(b) Assume  $|k| = \infty$ . Since  $F_e \neq 0$ ,  $F_e(\lambda_1, \dots, \lambda_{n-1}, 1) \neq 0$  for some  $\lambda_1, \dots, \lambda_{n-1} \in k$ . Look at  $k[w_1, \dots, w_{n-1}, x_n] \in R$ . For  $\underline{b} = (b_1, \dots, b_n) \in \mathbb{Z}_{\geq 0}^n$ ,  $(w_1 + \lambda_1 x_n)^{b_1} \dots (w_{n-1} + \lambda_{n-1} x_n)^{b_{n-1}} \cdot x_n^{b_n} = \lambda_1^{b_1} \dots \lambda_{n-1}^{b_{n-1}} x_n^{|\underline{b}|} + \text{lower degree terms in } x_n$ , where  $|\underline{b}| = b_1 + \dots + b_n$ . Note for  $i = 0, \dots, e$ ,

$$\begin{aligned} F_i(w_1 + \lambda_1 x_n, \dots, w_{n-1} + \lambda_{n-1} x_n, x_n) &= \sum_{|\underline{b}|=i} a_{\underline{b}} (\lambda_1^{b_1} \dots \lambda_{n-1}^{b_{n-1}}) x_n^i + \text{lower degree terms in } x_n \\ &= F_i(\lambda_1, \dots, \lambda_{n-1}, 1) x_n^i + \text{lower degree terms in } x_n. \end{aligned}$$

Let

$$\begin{aligned} G(w_1, \dots, w_{n-1}, x_n) &= F(w_1 + \lambda_1 x_n, \dots, w_{n-1} + \lambda_{n-1} x_n, x_n) \\ &= F_e(\lambda_1, \dots, \lambda_{n-1}, 1) x_n^e + \text{lower degree terms in } x_n. \end{aligned}$$

Let  $w_i := x_i - \lambda_i x_n$  for  $i = 1, \dots, n-1$ . Then  $G(w_1, \dots, w_{n-1}, x_n) = F(x_1 - \lambda_1 x_n + \lambda_1 x_n, \dots, x_{n-1} - \lambda_{n-1} x_n + \lambda_{n-1} x_n, x_n) = F(x_1, \dots, x_{n-1}, x_n) = n(F) = 0$ . Since  $F_e(\lambda_1, \dots, \lambda_{n-1}, 1) \neq 0$ ,  $x_n$  satisfies a monic  $\frac{G(w_1, \dots, w_{n-1}, X_n)}{F_e(\lambda_1, \dots, \lambda_{n-1}, 1)} \in k[w_1, \dots, w_{n-1}][X_n]$ . So  $x_n$  is integral over  $k[w_1, \dots, w_{n-1}]$ . Hence

$$R = k[x_1, \dots, x_{n-1}, x_n] = k[x_1 - \lambda_1 x_n, \dots, x_{n-1} - \lambda_{n-1} x_n, x_n] = k[w_1, \dots, w_{n-1}][x_n]$$

is integral over  $k[w_1, \dots, w_{n-1}]$  by Theorem 5.19.

(a) Look at  $k[w_1, \dots, w_{n-1}, x_n] \in R$ . Let  $e_n = 1$ . For  $\underline{b} = (b_1, \dots, b_n) \in \mathbb{Z}_{\geq 0}^n$  and  $e_1, \dots, e_{n-1} \gg 1$ ,

$$(w_1 + x_n^{e_1})^{b_1} \dots (w_{n-1} + x_n^{e_{n-1}})^{b_{n-1}} \cdot x_n^{b_n} = x_n^{\sum_{i=1}^n e_i b_i} + \text{lower degree terms in } x_n.$$

Write  $F = \sum_{j=1}^m a_j \underline{x}^{\underline{b}_j}$  for some  $m \geq 1$  and distinct  $\underline{x}^{\underline{b}_j} := x_1^{b_{j1}} \dots x_n^{b_{jn}}$  and  $a_j \neq 0$  for  $j = 1, \dots, m$ . Let  $A_i = \max\{b_{1i}, \dots, b_{mi}\} - \min\{b_{1i}, \dots, b_{mi}\}$  for  $i = 1, \dots, n$ . Choose  $e_{i-1} > A_i e_i + \dots + A_n e_n$  for  $i = 2, \dots, n$ . Re-order  $a_1 \underline{x}^{\underline{b}_1}, \dots, a_m \underline{x}^{\underline{b}_m}$  such that  $\underline{b}_1 \succ \dots \succ \underline{b}_m$  is in reverse lexicographical order. Then  $\sum_{i=1}^n e_i b_{1i} > \sum_{i=1}^n e_i b_{2i} > \dots > \sum_{i=1}^n e_i b_{mi}$ . Let

$$\begin{aligned} G(w_1, \dots, w_{n-1}, x_n) &= F(w_1 + x_n^{e_1}, \dots, w_{n-1} + x_n^{e_{n-1}}, x_n) \\ &= a_1 x_n^{\sum_{i=1}^n e_i b_{1i}} + \text{lower degree terms in } x_n. \end{aligned}$$

Let  $w_i := x_i - x_n^{e_i}$  for  $i = 1, \dots, n-1$ . Then  $G(w_1, \dots, w_{n-1}, x_n) = F(x_1, \dots, x_{n-1}, x_n) = n(F) = 0$ . Since  $a_1 \neq 0$ ,  $x_n$  satisfies a monic  $\frac{G(w_1, \dots, w_{n-1}, X_n)}{a_1} \in k[w_1, \dots, w_{n-1}][X_n]$ . So  $x_n$  is integral over  $k[w_1, \dots, w_{n-1}]$ . Hence

$$R = k[x_1, \dots, x_{n-1}, x_n] = k[x_1 - x_n^{e_1}, \dots, x_{n-1} - x_n^{e_{n-1}}, x_n] = k[w_1, \dots, w_{n-1}][x_n]$$

is integral over  $k[w_1, \dots, w_{n-1}]$  by Theorem 5.19.  $\square$

**Theorem 5.41** (Hilbert Nullstellensatz, version 1). *Let  $k \subseteq K := k[x_1, \dots, x_n]$  be a subfield.*

(a)  *$K$  is algebraic over  $k$  and  $[K : k] < \infty$ .*

(b) *If  $k$  is algebraically closed, then  $K = k$ .*

*Proof.* (a) Let  $k \subseteq S \subseteq K$  be a Noether normalization of  $k \subseteq K$ . Then there exists  $y_1, \dots, y_d \in K$  such that  $S = k[y_1, \dots, y_d] = k[Y_1, \dots, Y_d] \subseteq K$  and  $K$  is integral over  $k[Y_1, \dots, Y_d]$ . Since  $K$  is a field, by Proposition 5.24,  $k[Y_1, \dots, Y_d]$  is a field. So  $d = 0$ . Then  $S = k$ . So  $K = k[x_1, \dots, x_n]$  is integral over  $k$ . Hence  $K$  is a finite-dimensional  $k$ -vector space by Theorem 5.19.

(b) Since  $k$  is algebraically closed, there is no proper algebraic extensions. So  $K = k$ .  $\square$

**Theorem 5.42** (Hilbert Nullstellensatz, version 2). *Let  $k$  be an algebraically closed field,  $R = k[X_1, \dots, X_n]$  and  $\mathfrak{m} \in \mathfrak{m}\text{-Spec}(R)$ . Then there exists  $\underline{a} \in k^n$  such that  $\mathfrak{m} = \langle X_1 - a_1, \dots, X_n - a_n \rangle$ .*

*Proof.* Set  $K = R/\mathfrak{m} = k[x_1, \dots, x_n] \hookleftarrow k$ , where  $x_i = \overline{X_i} \in R/\mathfrak{m}$  for  $i = 1, \dots, n$ . Since  $k$  is algebraically closed and  $k \hookrightarrow K$  is a subfield, by Hilbert Nullstellensatz, version 1(b),  $k \hookrightarrow k[x_1, \dots, x_n] = R/\mathfrak{m}$  is onto. Since  $x_i \in R/\mathfrak{m}$ , there exists  $a_i \in k$  such that  $a_i \mapsto x_i$  for  $i = 1, \dots, n$ . So  $x_i - a_i = 0$  in  $R/\mathfrak{m}$ , i.e.,  $X_i - a_i \in \mathfrak{m}$  for  $i = 1, \dots, n$ . Then  $\mathfrak{m} \supseteq \langle X_1 - a_1, \dots, X_n - a_n \rangle$ . Since  $\mathfrak{m}, \langle X_1 - a_1, \dots, X_n - a_n \rangle \in \mathfrak{m}\text{-Spec}(R)$ ,  $\mathfrak{m} = \langle X_1 - a_1, \dots, X_n - a_n \rangle$ .  $\square$

**Theorem 5.43** (Hilbert Nullstellensatz, version 3). *Let  $k$  be an algebraically closed field,  $\mathfrak{a} \leq R = k[X_1, \dots, X_n]$ . Then  $Z(\mathfrak{a}) := \{\underline{a} \in k^n \mid F(\underline{a}) = 0, \forall F \in \mathfrak{a}\} \neq \emptyset$ .*

*Proof.* Since  $\mathfrak{a} \neq R$ , by Hilbert Nullstellensatz, version 2,  $\mathfrak{a} \subseteq \mathfrak{m} := \langle X_1 - a_1, \dots, X_n - a_n \rangle$  for some  $\underline{a} \in k^n$ . Let  $F \in \mathfrak{a} \subseteq \mathfrak{m}$ . Then  $F = \sum_{i=1}^n g_i(X_i - a_i)$  for some  $g_1, \dots, g_n \in R$ . So  $F(\underline{a}) = \sum_{i=1}^n g_i(\underline{a})(a_i - a_i) = 0$ . Thus,  $\underline{a} \in Z(\mathfrak{a})$ .  $\square$

**Theorem 5.44** (Hilbert Nullstellensatz, version 4). *Let  $k$  be an algebraically closed field,  $\mathfrak{a} \leq R = k[X_1, \dots, X_n]$  and  $Z = Z(\mathfrak{a})$ . Let  $I = I(Z) = \{F \in R \mid F(\underline{a}) = 0, \forall \underline{a} \in Z\} \leq R$ . Then  $I = \text{rad}(\mathfrak{a})$ .*

*Proof.* “ $\supseteq$ ”. Since  $I = I(Z) = I(Z(\mathfrak{a})) = \{F \in R \mid F(\underline{a}) = 0, \forall \underline{a} \in Z(\mathfrak{a})\} \supseteq \mathfrak{a}$ ,  $\text{rad}(\mathfrak{a}) \subseteq \text{rad}(I) = I$ .  
“ $\subseteq$ ”. Let  $F \in R \setminus \text{rad}(\mathfrak{a})$ . Then  $F \notin \text{rad}(\mathfrak{a}) = \bigcap_{\mathfrak{p} \in V(\mathfrak{a})} \mathfrak{p}$  by Fact 1.58. So there exists  $\mathfrak{p} \in V(\mathfrak{a})$  such that  $F \notin \mathfrak{p}$ . Set  $\overline{R} = R/\mathfrak{p} = k[x_1, \dots, x_n]$ , an integral domain, where  $x_i = \overline{X_i} \in R/\mathfrak{p}$  for  $i = 1, \dots, n$ . Since  $F \notin \mathfrak{p}$ ,  $f := \overline{F} \neq 0$  in  $\overline{R}$ . Then  $0 \neq \overline{R} \subseteq \overline{R}_f = \overline{R}[1/f] = k[x_1, \dots, x_n, 1/f]$ . So there exists  $\mathfrak{m} \in \mathfrak{m}\text{-Spec}(\overline{R}_f)$ . Consider  $k \hookrightarrow \overline{R}_f/\mathfrak{m} = k[\overline{x}_1, \dots, \overline{x}_n, \overline{1/f}]$ , where  $\overline{1/f} \neq 0$  in  $\overline{R}_f/\mathfrak{m}$  since  $1/f \in \overline{R}_f^\times$ . Since  $k$  is algebraically closed and  $k \hookrightarrow \overline{R}_f/\mathfrak{m}$  is a subfield, by Hilbert Nullstellensatz, version 1(b),  $k \hookrightarrow \overline{R}_f/\mathfrak{m}$  is onto. Since  $\overline{x}_i \in \overline{R}_f/\mathfrak{m}$ , there exists  $a_i \in k$  such that  $a_i \mapsto \overline{x}_i$  for  $i = 1, \dots, n$ . Since  $\mathfrak{a} \subseteq \mathfrak{p}$ ,  $\mathfrak{a} \cdot \overline{R} = 0$ . So  $\mathfrak{a} \cdot \overline{R}_f/\mathfrak{m} = 0$ . Then  $G(\underline{a}) = \overline{g}(\overline{x}_1, \dots, \overline{x}_n) = \overline{g} = 0$  in  $\overline{R}_f/\mathfrak{m}$  for all  $G \in \mathfrak{a}$ . Hence  $\underline{a} \in Z(\mathfrak{a}) = Z$ . Also, since  $F(\underline{a}) = \overline{f}(\overline{x}_1, \dots, \overline{x}_n) = \overline{f} \neq 0$  in  $\overline{R}_f/\mathfrak{m}$ , we have  $F \notin I(Z) = I$ .  $\square$

# Chapter 6

## Appendix

Let  $R$  be a commutative ring with identity and  $k$  be a field.

### Hilbert–Samuel Multiplicity

**Question 6.1.** What is the Hilbert-Samuel multiplicity?

**Example 6.2.** Let  $R = k[X, Y, Z]$  and  $\mathfrak{m} = (X, Y, Z)$ . Then  $l(R/\mathfrak{m}) = 1$  and  $l(R/\mathfrak{m}^2) = l(\frac{k[X, Y, Z]}{X^2, XY, XZ, Y^2, YZ, Z^2}) = 4$  with  $R/\mathfrak{m}^2 \cong k \oplus kX \oplus kY \oplus kZ$  as  $k$ -vector space.

**Theorem 6.3.** Let  $R = k[X_1, \dots, X_d]$  and  $\mathfrak{m} = (X_1, \dots, X_d)$ . Then  $l(R/\mathfrak{m}^t) = \#$  monomials of degree  $< t = \binom{d+(t-1)}{t-1} = \binom{d+(t-1)}{d}$  for  $t \geq 1$ .

**Definition 6.4.** Let  $(R, \mathfrak{m})$  be a local ring and  $I$  be an  $\mathfrak{m}$ -primary ideal. Define the *Hilbert-Samuel multiplicity* of  $I$  on  $R$  to be  $a$ , where  $\frac{a}{(\dim R)!}$  is the leading coefficient of the Hilbert-Samuel polynomial.

**Definition 6.5.**

$$e(I, R) = (\dim R)! \lim_{t \rightarrow \infty} \frac{l(R/I^t)}{t^{\dim R}}.$$

**Example 6.6.** Let  $R = k[X, Y]$ ,  $I = (X^2, XY, Y^2)$  and  $\mathfrak{m} = (X, Y)$ . Then by Theorem 6.3,  $l(R/I^t) = l(R/\mathfrak{m}^{2t}) = \binom{2t+1}{2t-1} = t(2t+1)$  for  $t \geq 1$ . Note  $e(I, R) = 2! \lim_{t \rightarrow \infty} \frac{t(2t+1)}{t^2} = 4$ .

**Fact 6.7.** Let  $R = k[X_1, \dots, X_d]$  and  $\mathfrak{m} = (X_1, \dots, X_d)$ . Then  $e(\mathfrak{m}, R) = 1$ .

*Proof.*  $e(\mathfrak{m}, R) = (d!) \lim_{t \rightarrow \infty} \frac{\binom{d+(t-1)}{t-1}}{t^d} = d! \lim_{t \rightarrow \infty} \frac{t \cdots (t+d-1)}{t^d} = 1.$  □

**Fact 6.8.** The Hilbert-Samuel multiplicity only sees the top dimension part of  $R$ . Let  $R = \frac{\mathbb{R}[X, Y, Z]}{(X, Y) \cap (Z)} = \frac{\mathbb{R}[X, Y, Z]}{(XZ, YZ)}$ . Let  $z = \bar{Z} \in R$ , then  $R/(z) \cong \mathbb{R}[X, Y]$ , so  $e(\mathfrak{m}, R/(z)) = 1$ , where  $\mathfrak{m} = (X, Y)$ .

**Definition 6.9.** Let  $I \leq R$ . Define  $\bar{I}$  be the *integral closure* of  $I$  by

$$\bar{I} = \{r \in R \mid r^n + a_1 r^{n-1} + \cdots + a_n = 0 \text{ for some } n \geq 1 \text{ and } a_i \in I^i, \forall i = 1, \dots, n\}.$$



**Example 6.10.** Let  $R = k[X, Y]$ . Then  $XY$  is integral over  $(X^2, Y^2)$  since  $(XY)^2 + 0 + (-X^2Y^2) = 0$ .

**Fact 6.11.** If  $\bar{I} = \bar{J}$ , then  $e(I, R) = e(J, R)$ .

**Fact 6.12.** If  $I = (f_1, \dots, f_d) \leq R$ ,  $\text{rad}(I) \in \text{m-Spec}(R)$  and  $\dim R = d$ , then  $e(\langle f_1^{t_1}, \dots, f_d^{t_d} \rangle, R) = t_1 \cdots t_d \cdot e(\langle f_1, \dots, f_d \rangle, R)$ .

**Example 6.13.** Let  $R = k[X, Y]$ ,  $I = (X^2, XY, Y^2)$  and  $\mathfrak{m} = (X, Y)$ . Then  $\text{rad}(I) = (X, Y) = \mathfrak{m}$ . Since the integral closure  $\bar{I} = \overline{(X^2, XY, Y^2)} = \overline{(X^2, Y^2)}$  by Example 6.10, then by Fact 6.11,  $e(I, R) = e(\langle X^2, Y^2 \rangle, R) = 2 \cdot 2 \cdot e(\mathfrak{m}, R) = 4$  by Fact 6.12.