Commutative Algebra

September 27, 2023

Contents

Introduction

The study and application of commutative rings with identity.

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

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

$$\text{algebraic properties of } I(G) \rightleftarrows \text{combinatorial properties of } G.$$

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

$$\text{algebraic properties of } J(\Delta) \rightleftarrows \text{combinatorics properties of } \Delta.$$

Let $\mathcal{P}$ be a poset and $\Delta(\mathcal{P}) =$ "order complex of $\mathcal{P}$" $= \{\text{chains in } \mathcal{P}\}$. 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, $f_1, \ldots, f_m \in k[X_1, \ldots, X_d]$,

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

where V is for "variety", and

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

$$\text{algebraic properties of } \mathrm{I}(V) \rightleftarrows \text{geometric properties of } V.$$

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 $V = \mathrm{V}(f_1, \ldots, f_m)$, $W = \mathrm{V}(g_1, \ldots, g_n)$ and $\phi : V \to W$. What does it mean for ϕ 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 $\phi : R \to S$ 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 $\phi : R \to S$ 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 $r_1, \ldots, r_m, s_1, \ldots, s_m \in R$.

(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 $\mathbb{N}_0 = \{0, 1, 2, \cdots\} \subseteq \mathbb{Z}$ 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 $\varepsilon : S \to R$ 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 $r_1, \ldots, r_m \in R$, then

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

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

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

Fact 1.12. For any $r_1, \ldots, r_m \in R$, $\langle r_1, \ldots, r_m \rangle$ is the smallest ideal of R containing $r_1, \ldots, r_m$, i.e., for any $\mathfrak{a} \leq R$, $r_1, \ldots, r_m \in \mathfrak{a}$ if and only if $\langle r_1, \ldots, r_m \rangle \subseteq \mathfrak{a}$. 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 $\pi : R \to R/\mathfrak{a}$ be given by $\pi(r) = \bar{r}$. Then π is a well-defined ring epimorphism.

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

$$\begin{tikzcd}
R \arrow[rrr, "\phi"] \arrow[ddd, "\pi"'] & & & S \\
& r \arrow[r, mapsto] \arrow[d, mapsto] & \phi(r) & \\
& \bar{r} \arrow[ur, mapsto] & & \\
R/\mathfrak{a} \arrow[uuurrr, dashed, "\exists!\ \overline{\phi}"'] & & &
\end{tikzcd}$$

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

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.

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

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

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

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

We claim that $\frac{R/\mathfrak{a}}{J/\mathfrak{a}} \cong \frac{R}{J}$.

$$\begin{tikzcd}
R \arrow[r, "p"] \arrow[ddd, "\pi"'] & R/\mathfrak{a} \arrow[rr, "\tau"] & & \frac{R/\mathfrak{a}}{J/\mathfrak{a}} \\
& r \arrow[r, mapsto] \arrow[d, mapsto] & \bar{r} \arrow[r, mapsto] & \bar{\bar{r}} \\
& \bar{r} \arrow[urr, mapsto] & & \\
R/J \arrow[uuurrr, dashed, "\exists!\ \overline{\phi}"'] & & &
\end{tikzcd}$$

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

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

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

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

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

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

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

$$\begin{tikzcd}
R \arrow[r, "\phi"] \arrow[ddd, "p"'] & S \arrow[rr, "\pi"] & & S/\mathfrak{q} \\
& r \arrow[r, mapsto] \arrow[d, mapsto] & \phi(r) \arrow[r, mapsto] & \overline{\phi(r)} \\
& \bar{r} \arrow[urr, mapsto] & & \\
\frac{R}{\phi^{-1}(\mathfrak{q})} \arrow[uuurrr, dashed, "\exists!\ \overline{\pi\circ\phi}"'] & & &
\end{tikzcd}$$

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

Example. Let $\phi : \mathbb{Z} \to \mathbb{Q}$ be an inclusion map. Note that $\mathfrak{q} := (0)\mathbb{Q} \leq \mathbb{Q}$ is maximal, but $\phi^{-1}(\mathfrak{q}) = \phi^{-1}(0) = \operatorname{Ker}(\phi) = 0\mathbb{Z}$, which is not maximal in $\mathbb{Z}$. Hence the map ϕ^* 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 $\mathfrak{a} \lneq R$, there exists a maximal ideal $\mathfrak{m} \supseteq \mathfrak{a}$. In particular, $\mathrm{V}(\mathfrak{a}) = \{\mathfrak{p} \in \operatorname{Spec}(R) \mid \mathfrak{p} \supseteq \mathfrak{a}\} \neq \emptyset$.

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 $\mathfrak{a} \lneq R$. Then $0 \neq R/\mathfrak{a}$ is a commutative ring with identity. Hence $R/\mathfrak{a}$ 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 that $0 \neq \mathbb{Z}/\langle p^n \rangle$ has a maximal ideal $\mathfrak{m} = \langle p \rangle / \langle p^n \rangle$, where $\langle p \rangle$ is a maxiaml ideal of R 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. Hence $\langle p \rangle = \mathfrak{m}_1$. 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 $\operatorname{Spec}(\mathbb{Z}/\langle p^n \rangle) = \{\langle p \rangle / \langle p^n \rangle\}$.

(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, $\operatorname{Spec}(R) = \{\langle X \rangle / \langle X^n \rangle\}$.

(d) Let k be a field and $R = k[X_1, \dots, X_d]/\langle X_1^{a_1}, \cdots, X_d^{a_d} \rangle$, 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, $\operatorname{Spec}(R) = \{\langle X_1, \dots, X_d \rangle / \langle X_1^{a_1}, \cdots, X_d^{a_d} \rangle\}$.

Fact 1.20. If $(R, \mathfrak{m})$ is local and $\mathfrak{a} \lneq R$, 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) $R \smallsetminus R^\times \lneq R$.

(iii) There exists $\mathfrak{a} \lneq R$ such that $R \smallsetminus \mathfrak{a} \subseteq R^\times$.

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

Proof. (i)$\Longrightarrow$(ii) Assume $(R, \mathfrak{m})$ is local.

We claim that $\mathfrak{m} = R \smallsetminus R^\times$. It suffices to show $R \smallsetminus \mathfrak{m} = R^\times$. $\supseteq$ Let $u \in R^\times$. Then $\langle u \rangle = R$ and so $u \notin \mathfrak{m} \lneq R$, i.e., $u \in R \smallsetminus \mathfrak{m}$. Hence $R^\times \subseteq R \smallsetminus \mathfrak{m}$. $\subseteq$ Let $x \in R \smallsetminus R^\times$. Then $\langle x \rangle \lneq R$. Since $\mathfrak{m}$ is the unique maximal ideal in R, $\langle x \rangle \subseteq \mathfrak{m}$, i.e., $x \in \mathfrak{m}$. Thus, $R \smallsetminus R^\times \subseteq \mathfrak{m}$, i.e., $R \smallsetminus \mathfrak{m} \subseteq R^\times$.

(ii)$\Longrightarrow$(iii) Assume $R \smallsetminus R^\times \lneq R$. Set $\mathfrak{a} = R \smallsetminus R^\times$. Then $R \smallsetminus \mathfrak{a} = R^\times$.

(iii)$\Longrightarrow$(i) Let $\mathfrak{a} \lneq R$ such that $R \smallsetminus \mathfrak{a} \subseteq R^\times$.

We claim that $\mathfrak{a} = R \smallsetminus R^\times$. "$\supseteq$". It is straightforward. "$\subseteq$". Let $a \in \mathfrak{a} \lneq R$, then $a \notin R^\times$ since $\mathfrak{a} \lneq R$, so $a \in R \smallsetminus R^\times$ and hence $\mathfrak{a} \subseteq R \smallsetminus R^\times$. Thus, $\mathfrak{a} = R \smallsetminus R^\times$.

Let $\mathfrak{n} \lneq R$ be maximal and $y \in \mathfrak{n}$. Then $y \notin R^\times$. Hence $y \in R \smallsetminus R^\times = \mathfrak{a}$. Thus, $\mathfrak{n} \subseteq \mathfrak{a} \lneq R$. 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 $\mathfrak{m} \lneq R$ be maximal such that $1 + \mathfrak{m} \subseteq R^\times$. Then R is local.

Proof. By the previous proposition, it suffices to show $R \smallsetminus \mathfrak{m} \subseteq R^\times$. Let $x \in R \smallsetminus \mathfrak{m}$. 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, $\langle x, \mathfrak{m} \rangle = R$. Hence $ax + m = 1$ 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

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

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

Proposition 1.26. We have the following.

(a) $\operatorname{Nil}(R) \leq R$.

(b) $\operatorname{Nil}(R/\operatorname{Nil}(R)) = \{0\}$.

(c) $\operatorname{Nil}(R) = R$ if and only if $R = 0$.

(d) $\operatorname{Nil}(R) = \bigcap_{\mathfrak{p}\in\operatorname{Spec}(R)} \mathfrak{p}$.

Proof. (a) Since $0 \in \operatorname{Nil}(R)$, $\operatorname{Nil}(R) \neq \emptyset$. Let $r \in R$ and $a, b \in \operatorname{Nil}(R)$. Then there exists $m, n \geq 1$ such that $a^m = 0 = b^n$. Then $(ra)^m = r^m a^m = 0$ and so $ra \in \operatorname{Nil}(R)$. 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 $i = 0, \ldots, m+n$, either $i \geq m$ or $i < m$, i.e., $i \geq m$ or $m+n-i > n$, we have that $a^i = 0$ when $i \geq m$, and $b^{m+n-i} = 0$ when $m+n-i > n$. Hence $(a+b)^{m+n} = 0$ and thus $a+b \in \operatorname{Nil}(R)$.

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

(c) We have that $\operatorname{Nil}(R) = R$ if and only if $1 \in \operatorname{Nil}(R)$ 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 $x \in \operatorname{Nil}(R)$. Then there exists $n \geq 1$ such that $x^n = 0 \in \mathfrak{p}$ for $\mathfrak{p} \in \operatorname{Spec}(R)$. Hence $x \in \mathfrak{p}$ for $\mathfrak{p} \in \operatorname{Spec}(R)$. Thus, $x \in \bigcap_{\mathfrak{p}\in\operatorname{Spec}(R)} \mathfrak{p}$.

"$\supseteq$". Let $x \in R \smallsetminus \operatorname{Nil}(R)$. Need to show $x \notin \bigcap_{\mathfrak{p}\in\operatorname{Spec}(R)}$. It is equivalent to show there exists $\mathfrak{p} \in \operatorname{Spec}(R)$ such that $x \notin \mathfrak{p}$. Let $\Sigma = \{\mathfrak{a} \leq R \mid x, x^2, x^3 \cdots \notin \mathfrak{a}\}$. Since $x \notin \operatorname{Nil}(R)$, $x^k \neq 0$ for $k \geq 1$. Hence $(0) \in \Sigma$ and then $\Sigma \neq \emptyset$. Let $\mathscr{C} \subseteq \Sigma$ be chain. Then we have that $\mathfrak{q} := \bigcup_{\mathfrak{a}\in\mathscr{C}} \mathfrak{a} \leq R$. Suppose $x^n \in \mathfrak{q}$ for some $n \geq 1$. Then $x^n \in \mathfrak{a}$ for some $\mathfrak{a} \in \mathscr{C} \subseteq \Sigma$, contradicting $\mathfrak{a} \in \Sigma$. Hence $x^n \notin \mathfrak{q}$ for $n \geq 1$ and hence $\mathfrak{q} \in \Sigma$. Hence $\mathfrak{q}$ is an upper bound for $\mathscr{C}$ in Σ. Since the chain $\mathscr{C} \subseteq \Sigma$ is arbitrary, by Zorn's lemma, Σ has a maximal element I. We claim that $I \in \operatorname{Spec}(R)$. Suppose $I = R$. Then $x \in R = I$, contradicting $I \in \Sigma$. Hence $I \lneq R$. Let $r, s \in R \smallsetminus I$. Then $I \subsetneq \langle r, I\rangle \leq R$ and $I \subsetneq \langle s, I\rangle \leq R$. By the maximality of I in Σ, we have that $\langle r, I\rangle, \langle s, I\rangle \notin \Sigma$. Hence 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 $j \in I$. Hence

$$x^{m+n} = x^m x^n = (ar+i)(bs+j) = abrs + (\underbrace{arj + bsi + ij}_{\in I}) \in \langle rs, I\rangle.$$

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

† $\operatorname{Nil}(R) \subseteq \operatorname{ZD}(R)$, but not conversely.

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 $\operatorname{Nil}(R) = \langle X_1, \dots, X_d\rangle/\langle X_1^{a_1}, \dots, X_d^{a_d}\rangle$.

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

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

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 $\langle \bar{r}_1, \cdots, \bar{r}_n\rangle = \langle r_1, \dots, r_n\rangle/\mathfrak{a}$.

The Jacobson Radical

Definition 1.27. The *Jacobson radical* of R is

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

Fact 1.28.

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

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 $x \in \mathfrak{J}(R) \subseteq \mathfrak{m}$, $xy \in \mathfrak{m}$. Hence $1 = (1 - xy) + xy \in \mathfrak{m}$, 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 $x \notin \mathfrak{m}$. Hence $\mathfrak{m} \subsetneq \langle \mathfrak{m}, x\rangle \subseteq R$. 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., $1 - xy = m \in \mathfrak{m}$. Hence $1 - xy \notin R^\times$, 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 Λ 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 $b\in\mathfrak{b}$, $b=0+b\in I$. Hence $\mathfrak{a}\cup\mathfrak{b}\subseteq I$. 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 that $a,b\in\mathfrak{a}\cup\mathfrak{b}\subseteq\mathfrak{a}+\mathfrak{b}\leq R$, so $a+b\in\mathfrak{a}+\mathfrak{b}$.

(d) Let $I\leq R$. Note that $I\supseteq\mathfrak{a}\cup\mathfrak{b}$ 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 $I\supseteq S\cup T$. Hence

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

(e) By (d).

(f) By (c).

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

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

Proposition 1.32. Let $S\subseteq R$.

(a) $\mathrm{V}(S)=\mathrm{V}(\langle S\rangle)$.

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

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

(d) If $\mathfrak{a}\subseteq\mathfrak{b}$, then $\mathrm{V}(\mathfrak{a})\supseteq\mathrm{V}(\mathfrak{b})$[†]. If $S\subseteq T\subseteq R$, then $\mathrm{V}(S)\supseteq\mathrm{V}(T)$.

Proof. (d) Since $S\subseteq T\subseteq R$, we have that $\mathrm{V}(S)\supseteq\mathrm{V}(T)$ by definition.

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

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

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

[†] $\mathrm{V}(\mathfrak{a})\subseteq\mathrm{V}(\mathfrak{b})$ if and only if $\mathrm{rad}(\mathfrak{a})\supseteq\mathrm{rad}(\mathfrak{b})$; $\mathrm{V}(\mathfrak{a})=\mathrm{V}(\mathfrak{b})$ if and only if $\mathrm{rad}(\mathfrak{a})=\mathrm{rad}(\mathfrak{b})$.

Proposition 1.33. We have the following.

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

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

Proof. (a) Since $\mathfrak{a}+\mathfrak{b} = \langle\mathfrak{a}\cup\mathfrak{b}\rangle$, $\mathrm{V}(\mathfrak{a}+\mathfrak{b}) = \mathrm{V}(\langle\mathfrak{a}\cup\mathfrak{b}\rangle) = \mathrm{V}(\mathfrak{a}\cup\mathfrak{b})$.
Let $\mathfrak{p}\in\mathrm{Spec}(R)$. Note that $\mathfrak{p}\supseteq\mathfrak{a}\cup\mathfrak{b}$ if and only if $\mathfrak{p}\supseteq\mathfrak{a}$ and $\mathfrak{p}\supseteq\mathfrak{b}$. Hence $\mathrm{V}(\mathfrak{a}\cup\mathfrak{b}) = \mathrm{V}(\mathfrak{a})\cap\mathrm{V}(\mathfrak{b})$.

(b) $\mathrm{V}(\mathfrak{a})\cap\mathrm{V}(\mathfrak{b}) = \emptyset$ if and only if $\mathrm{V}(\mathfrak{a}+\mathfrak{b}) = \emptyset$ 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 $\mathfrak{a}_1,\ldots,\mathfrak{a}_n$ for all $n\in\mathbb{Z}_{\geq 3}$ and same properties as above hold for finite sums.

Definition 1.34.

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

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) $\mathrm{V}(\sum_{\lambda\in\Lambda}\mathfrak{a}_\lambda) = \mathrm{V}(\bigcup_{\lambda\in\Lambda}\mathfrak{a}_\lambda) = \bigcap_{\lambda\in\Lambda}\mathrm{V}(\mathfrak{a}_\lambda)$.

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

Products of Ideals

Definition 1.37.

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

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) $\mathfrak{a}\mathfrak{b} = \{\sum_i^{\text{finite}} a_ib_i \mid a_i\in\mathfrak{a},\ b_i\in\mathfrak{b}, \forall i\}$.

(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 $\mathfrak{a} = \langle x_1,\ldots,x_m\rangle$ and $\mathfrak{b} = \langle y_1,\ldots,y_n\rangle$, then $\mathfrak{a}\mathfrak{b} = \langle x_iy_j \mid i = 1,\ldots,m, j = 1,\ldots,n\rangle$.

(f) $\mathfrak{ab} \subseteq \mathfrak{a} \cap \mathfrak{b}$.

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 $I \subseteq \mathfrak{ab} \subseteq I$ like Fact 1.31(c).

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

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

Proposition 1.39. We have the following.

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

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

Proof. (a) Let $\mathfrak{p} \in \mathrm{Spec}(R)$. We claim that $\mathfrak{p} \supseteq \mathfrak{ab}$ if and only if $\mathfrak{p} \supseteq \mathfrak{a}$ or $\mathfrak{p} \supseteq \mathfrak{b}$*.

$\Longleftarrow$ Let $\mathfrak{p} \supseteq \mathfrak{a}$ or $\mathfrak{p} \supseteq \mathfrak{b}$. Then $\mathfrak{p} = \mathfrak{p}R \supseteq \mathfrak{a}R \supseteq \mathfrak{ab}$ or $\mathfrak{p} = R\mathfrak{p} \supseteq R\mathfrak{b} \supseteq \mathfrak{ab}$.

$\Longrightarrow$ Let $\mathfrak{p} \supseteq \mathfrak{ab}$. 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 $\mathfrak{p} \in \mathrm{Spec}(R)$, $ab \notin \mathfrak{p}$, contradicting $ab \in \mathfrak{ab} \subseteq \mathfrak{p}$.

Hence $\mathrm{V}(\mathfrak{ab}) = \mathrm{V}(\mathfrak{a}) \cup \mathrm{V}(\mathfrak{b})$.

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

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

Proposition 1.40. We have the following.

(a) $\mathfrak{ab} = \mathfrak{ba}$ and $(\mathfrak{ab})\mathfrak{c} = \mathfrak{a}(\mathfrak{bc})$.

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

(c) $\mathfrak{a} \cap \mathfrak{b} = \mathfrak{ab}$ 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 $\mathfrak{a} \cap \mathfrak{b} \supseteq \mathfrak{ab}$.

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

Method 1. Note that $1 = a + b$ 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 $x \in \mathfrak{a}$. Hence $x = 1 \cdot x = (a + b)x = ax + bx = ax + xb \in \mathfrak{ab}$. Hence $\mathfrak{a} \cap \mathfrak{b} \subseteq \mathfrak{ab}$.

Method 2. Note that

$$\mathfrak{a} \cap \mathfrak{b} = R(\mathfrak{a} \cap \mathfrak{b}) = (\mathfrak{a} + \mathfrak{b})(\mathfrak{a} \cap \mathfrak{b}) = \mathfrak{a}(\underbrace{\mathfrak{a} \cap \mathfrak{b}}_{\subseteq \mathfrak{b}}) + \mathfrak{b}(\underbrace{\mathfrak{a} \cap \mathfrak{b}}_{\subseteq \mathfrak{a}}) \subseteq \mathfrak{ab}$$

by (a) and (b).

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

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

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 $i = 1, \ldots, n$, and $p_1, \ldots, p_n \in R$ 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 $\mathfrak{b} = \langle p_1^{f_1} \cdots p_n^{f_n} \rangle$, $\mathfrak{a} \cap \mathfrak{b} = \operatorname{lcm}(p_1^{e_1} \cdots p_n^{e_n}, p_1^{f_1} \cdots p_n^{f_n})R = p_1^{\max\{e_1,f_1\}} \cdots p_n^{\max\{e_n,f_n\}} R$. By Fact 1.38(e), $\mathfrak{a}\mathfrak{b} = p_1^{e_1+f_1} \cdots p_n^{e_n+f_n}$. Hence $\max\{e_i, f_i\} = e_i + f_i$, i.e, $e_i = 0$ or $f_i = 0$ for $i = 1, \ldots, n$. In other words, for $\mathfrak{p} \in \operatorname{Spec}(R)$, either $\mathfrak{a} \nsubseteq \mathfrak{p}$ or $\mathfrak{b} \nsubseteq \mathfrak{p}$[†]. Hence $\mathrm{V}(\mathfrak{a}) \cap \mathrm{V}(\mathfrak{b}) = \emptyset$ for $\mathfrak{p} \in \operatorname{Spec}(R)$. Thus, $\mathfrak{a} + \mathfrak{b} = R$ by Proposition 1.33(b). □

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

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 $\mathfrak{a} + \mathfrak{b} = \langle X, Y \rangle \subsetneq R$. Hence 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 $\mathfrak{a}^2 = \langle X^2, XY, Y^2 \rangle \neq \langle f^2 \mid f \in \mathfrak{a} \rangle \not\ni XY$.

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

(a) $\mathfrak{a}^n = \langle N \rangle$ and for any $\mathfrak{b} \leq R$, we have that $\mathfrak{a}^n \subseteq \mathfrak{b}$ if and only if $N \subseteq \mathfrak{b}$.

(b) $\mathfrak{a}^n$ is the (unique) smallest ideal of R containing N.

(c) $\mathfrak{a}^n = \{\sum_i^{\text{finite}} a_{i1} \cdots a_{in} \mid a_{ij} \in \mathfrak{a}, \forall i, \forall j = 1, \ldots, n\}$.

(d) If $\mathfrak{a} = \langle S \rangle$, then $\mathfrak{a}^n = \langle s_1 \cdots s_n \mid s_i \in S, \forall i = 1, \ldots, n \rangle$.

(e) If $\mathfrak{a} = \langle x_1, \ldots, x_m \rangle$, then $\mathfrak{a}^n = \langle x_{i_1} \cdots x_{i_n} \mid i_j \in \{1, \ldots, m\}, \forall j = 1, \ldots, n \rangle$.

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

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

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

(a) The function $\phi : R \to (R/\mathfrak{a}_1) \times \cdots \times (R/\mathfrak{a}_n)$ given by $\phi(x) = (\bar{x}, \cdots, \bar{x}) = (x + \mathfrak{a}_1, \ldots, x + \mathfrak{a}_n)$ 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., $\{\mathfrak{a}_1, \ldots, \mathfrak{a}_n\}$ 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 $i = 1, \ldots, n$.

(c) ϕ 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) $\operatorname{Ker}(\phi) = \bigcap_{i=1}^n \mathfrak{a}_i$.

(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 $R \cong (R/\mathfrak{a}_1) \times \cdots \times (R/\mathfrak{a}_n)$.

[†]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.

Proof. (b) Let $i \in \{1, \ldots, n\}$. To show $\mathfrak{a}_i + (\bigcap_{j \neq i} \mathfrak{a}_j)R = R$, it suffices to show $\mathrm{V}(\mathfrak{a}_i) \bigcap \left(\bigcup_{j \neq i} \mathrm{V}(\mathfrak{a}_j) \right)$ $= \mathrm{V}(\mathfrak{a}_i) \bigcap \mathrm{V}\left(\bigcap_{j \neq i} \mathfrak{a}_j \right) = \mathrm{V}(\mathfrak{a}_i + \bigcap_{j \neq i} \mathfrak{a}_j) = \emptyset$. Suppose $\mathrm{V}(\mathfrak{a}_i) \bigcap \left(\bigcup_{j \neq i} \mathrm{V}(\mathfrak{a}_j) \right) \neq \emptyset$. Then there exists $\mathfrak{p} \in \mathrm{V}(\mathfrak{a}_i) \cap \mathrm{V}(\mathfrak{a}_j) = \mathrm{V}(\mathfrak{a}_i + \mathfrak{a}_j) = \mathrm{V}(R) = \emptyset$ 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 $\mathfrak{a}_n + \mathfrak{a}_1 \cdots \mathfrak{a}_{n-1} = \mathfrak{a}_n + \bigcap_{j=1}^{n-1} \mathfrak{a}_j = R$. Hence by Proposition 1.40(c), we have that

$$\bigcap_{i=1}^{n} \mathfrak{a}_i = \left(\bigcap_{i=1}^{n-1} \mathfrak{a}_i \right) \bigcap \mathfrak{a}_n = (\mathfrak{a}_1 \cdots \mathfrak{a}_{n-1}) \cap \mathfrak{a}_n = (\mathfrak{a}_1 \cdots \mathfrak{a}_{n-1})\mathfrak{a}_n = \mathfrak{a}_1 \cdots \mathfrak{a}_n.$$

(c) $\Longrightarrow$ Assume ϕ is surjective. In particular, there exists $x \in R$ such that $(\bar{1}, \bar{0}, \ldots, \bar{0}) = \phi(x) = (\bar{x}, \bar{x}, \cdots, \bar{x})$. Hence $x + \mathfrak{a}_1 = 1 + \mathfrak{a}_1$ and $x + \mathfrak{a}_i = 0 + \mathfrak{a}_i$ for $i = 2, \ldots, n$. Hence $1 - x \in \mathfrak{a}_1$ and $x \in \mathfrak{a}_i$ for $i = 2, \ldots, n$. Also, since $\underbrace{(x)}_{\in \mathfrak{a}_i} + \underbrace{(1 - x)}_{\in \mathfrak{a}_1} = 1$, we have that $\mathfrak{a}_i + \mathfrak{a}_1 = R$ for $i = 2, \ldots, n$.

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

$\Longleftarrow$ Assume $\mathfrak{a}_i + \mathfrak{a}_j = R$ for $1 \leq i, j \leq n$ with $i \neq j$. By (b), $\mathfrak{a}_1 + (\bigcap_{j=2}^n \mathfrak{a}_j)R = R$. Hence $a_1 + y = 1$ 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 $j = 2, \ldots, n$. Then

$$\phi(y) = (\bar{y}, \bar{y}, \cdots, \bar{y}) = (y + \mathfrak{a}_1, y + \mathfrak{a}_2, \cdots, y + \mathfrak{a}_n) = (1 + \mathfrak{a}_1, 0 + \mathfrak{a}_2, \ldots, 0 + \mathfrak{a}_n) = (\bar{1}, \bar{0}, \cdots, \bar{0}).$$

Similarly, for $j = 1, \ldots, n$, there exists y_j such that $\phi(y_j) = (\bar{0}, \cdots, \bar{0}, \underset{\uparrow j\text{th}}{\bar{1}}, \bar{0}, \cdots, \bar{0})$. Then for any $(\bar{r}_1, \ldots, \bar{r}_n) \in \frac{R}{\mathfrak{a}_1} \times \cdots \times \frac{R}{\mathfrak{a}_n}$,

$$(\bar{r}_1, \ldots, \bar{r}_n) = \sum_{j=1}^{n} r_j (\bar{0}, \cdots, \bar{0}, \underset{\uparrow j\text{th}}{\bar{1}}, \bar{0}, \cdots, \bar{0}) = \sum_{j=1}^{n} r_j \phi(y_j) = \phi\left(\sum_{j=1}^{n} r_j y_j \right).$$

Hence ϕ is surjective. □

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

(a) If $\mathfrak{p} = \mathfrak{a}_1 \cdots \mathfrak{a}_n$, then $\mathfrak{p} = \mathfrak{a}_i$ for some $i \in \{1, \ldots, n\}$.

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

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

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

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

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

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 $\mathfrak{a}_1 \cap \mathfrak{a}_2 = \langle XY \rangle \neq \langle X \rangle = \mathfrak{p} = \langle X \rangle \neq \langle XY \rangle = \mathfrak{a}_1\mathfrak{a}_2$.

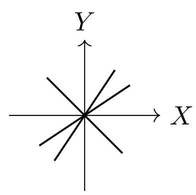
Prime Avoidence

Lemma 1.48. Let k be an infinite field, $0 \neq V$ a vector space over k, and $V_1, \ldots, V_n \lneq V$. 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 $\bigcup_{i\neq j} V_j \subsetneq V$ for $j = 1, \ldots, n$. Then there exists $0 \neq v_j \in V \setminus \{\bigcup_{i\neq j} V_j\}$ for $j = 1, \ldots, n$. By way of contradiction, suppose $\bigcup_{i=1}^{n} V_i = V$. Then $v_j \in \{\bigcup_{i=1}^{n} V_i\} \setminus \{\bigcup_{i\neq j} V_j\} \subseteq V_j$ for $j = 1, \ldots, n$. Let $1 \leq i, j \leq n$ with $i \neq j$. Since $v_j \neq 0$, we have that $v_i + \lambda v_j \neq v_i + \mu v_j$ 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 that $v_j \in V_l$. Since $v_j \notin V_k$ for any $k \neq j$ and $v_j \in V_j$, we have that $l = j$. 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 that $v_i \in V_l$ and then similarly, we have that $l = i$. 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, $V = k^2 = \bigcup_{v\in k^2} \{v\} = \bigcup_{0\neq v \in k^2} \operatorname{span}\{v\}$ but $0 \neq \operatorname{span}(v) \lneq k^2 = V$ for $0 \neq v \in k^2$.

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

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

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

(b) $\mathfrak{b}_3, \ldots, \mathfrak{b}_n \in \operatorname{Spec}(R)$.

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

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

(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 $a_1 \notin \mathfrak{b}_1$, $a_1 \in \mathfrak{b}_2$. Hence $a_2 = (a_1 + a_2) - a_1 \in \mathfrak{b}_2$, a contradiction.

Induction step $n \geq 3$. Let $\mathfrak{a} \not\subseteq \mathfrak{b}_i$ for $i = 1, \ldots, n$. Assume $\mathfrak{a} \not\subseteq \bigcup_{i\neq j} \mathfrak{b}_i$ for $j = 1, \ldots, n$. Then there exists $a_j \in \mathfrak{a} \setminus \{\bigcup_{i\neq j} \mathfrak{b}_i\}$ for $j = 1, \ldots, n$. 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 $j = 1, \ldots, n$. Note that $a_1 \cdots a_{n-1} + a_n \in \mathfrak{a} \subseteq \bigcup_{i=1}^{n} \mathfrak{b}_i$. Hence there exists $l \in \{1, \ldots, n\}$ 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 that $\mathfrak{b}_n \in \operatorname{Spec}(R)$ 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 that $a_n \in \mathfrak{b}_l$, a contradiction. $\square$

Theorem 1.51 (Prime avoidence)**.** *Let* $\mathfrak{p}_1, \dots, \mathfrak{p}_n \in \operatorname{Spec}(R)$*. 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 (Avoidence 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 $f_1 + \cdots + f_m \in \mathfrak{a} \subseteq \bigcup_{i=1}^n \mathfrak{b}_i$. Hence $f_1 + \cdots + f_m \in \mathfrak{b}_i$ 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, $\mathfrak{a} = \langle f_1, \dots, f_m \rangle \subseteq \mathfrak{b}_i$. □

Colon Ideals

Definition 1.52. Let $S \subseteq R$.

(a) Define the *colon ideal* by

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

(b) Define the *annihilator* of S by

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

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

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

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

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

(b)

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

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

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

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

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

(f) $\mathfrak{b} \subseteq \mathfrak{a}$ 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 that $br \in \mathfrak{a}$. 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. Hence $rs = r(\sum_i^{\text{finite}} a_i s_i) = \sum_i^{\text{finite}} a_i(rs_i) \in R$. 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 that $r \in ((\mathfrak{a} : \mathfrak{b}) : \mathfrak{c})$ 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). □

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)

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

Radicals of Ideals

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

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

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

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

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

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

(a) $\operatorname{rad}(\mathfrak{a}) = \pi^{-1}(\operatorname{Nil}(R/\mathfrak{a})) \leq R$.

(b) If $\mathfrak{a} \subseteq \mathfrak{b}$, then $\mathrm{rad}(\mathfrak{a}) \subseteq \mathrm{rad}(\mathfrak{b})$.

(c) $\mathfrak{a} \subseteq \mathrm{rad}(\mathfrak{a}) = \mathrm{rad}(\mathrm{rad}(\mathfrak{a}))$.

(d) $\mathrm{rad}(\mathfrak{a}\mathfrak{b}) = \mathrm{rad}(\mathfrak{a} \cap \mathfrak{b}) = \mathrm{rad}(\mathfrak{a}) \cap \mathrm{rad}(\mathfrak{b})$.

(e) $\mathrm{rad}(\mathfrak{a}) = R$ if and only if $\mathfrak{a} = R$.

(f) $\mathrm{rad}(\mathfrak{a} + \mathfrak{b}) = \mathrm{rad}(\mathrm{rad}(\mathfrak{a}) + \mathrm{rad}(\mathfrak{b}))$.

(g) $\mathrm{rad}(\mathfrak{a}) = \bigcap_{\mathfrak{p} \in \mathrm{V}(\mathfrak{a})} \mathfrak{p}$.

(h) $\mathrm{rad}(\bigcap_{i=1}^n \mathfrak{p}_i^{e_i}) = \bigcap_{i=1}^n \mathfrak{p}_i$, where $\mathfrak{p}_i \in \mathrm{Spec}(R)$ and $e_i \geq 1$ for $i = 1, \dots, n$.

(i) $\mathfrak{a} + \mathfrak{b} = R$ if and only if $\mathrm{rad}(\mathfrak{a}) + \mathrm{rad}(\mathfrak{b}) = R$.

Proof. (a) Let $r \in R$. Then $r \in \pi^{-1}(\mathrm{Nil}(R/\mathfrak{a}))$ if and only if $\pi(r) \in \mathrm{Nil}(R/\mathfrak{a})$ 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 $r \in \mathrm{rad}(\mathfrak{a})$.

(b) It is straightforward.

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

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

(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 $\mathrm{rad}(\mathfrak{a}) = R$.

(f) Since $\mathfrak{a} + \mathfrak{b} \subseteq \mathrm{rad}(\mathfrak{a}) + \mathrm{rad}(\mathfrak{b})$, we have that $\mathrm{rad}(\mathfrak{a} + \mathfrak{b}) \subseteq \mathrm{rad}(\mathrm{rad}(\mathfrak{a}) + \mathrm{rad}(\mathfrak{b}))$.
Let $x \in \mathrm{rad}(\mathrm{rad}(\mathfrak{a}) + \mathrm{rad}(\mathfrak{b}))$. Then there exists $n \geq 1$ such that $x^n \in \mathrm{rad}(\mathfrak{a}) + \mathrm{rad}(\mathfrak{b})$. Hence there exist $a \in \mathrm{rad}(\mathfrak{a})$ and $b \in \mathrm{rad}(\mathfrak{b})$ such that $x^n = a + b$. Then there exist $j, k \geq 1$ such that $a^j \in \mathfrak{a}$ and $b^k \in \mathfrak{b}$. Hence

$$x^{n(j+k)} = (x^n)^{j+k} = (a+b)^{j+k} = \sum_{l=0}^{j+k} \binom{l}{j+k} a^l b^{j+k-l}.$$

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 that $a^l \in \mathfrak{a}$ when $l \geq j$, and $b^{j+k-l} \in \mathfrak{b}$ when $j+k-l > n$. Hence $x^{n(j+k)} = 0$. Thus, $x \in \mathrm{rad}(\mathfrak{a} + \mathfrak{b})$.

(g) By Fact 1.15, $\mathrm{Spec}(R/\mathfrak{a}) = \{\mathfrak{p}/\mathfrak{a} \mid \mathfrak{p} \in \mathrm{V}(\mathfrak{a})\}$. Hence $\mathrm{Nil}(R/\mathfrak{a}) = \bigcap_{\mathfrak{p} \in \mathrm{Spec}(R/\mathfrak{a})} \mathfrak{p} = \bigcap_{\mathfrak{p} \in \mathrm{V}(\mathfrak{a})} \mathfrak{p}/\mathfrak{a}$. Then by (a),

$$\mathrm{rad}(\mathfrak{a}) = \pi^{-1}(\mathrm{Nil}(R/\mathfrak{a})) = \pi^{-1}\left(\bigcap_{\mathfrak{p} \in \mathrm{V}(\mathfrak{a})} \mathfrak{p}/\mathfrak{a}\right) = \bigcap_{\mathfrak{p} \in \mathrm{V}(\mathfrak{a})} \pi^{-1}(\mathfrak{p}/\mathfrak{a}) = \bigcap_{\mathfrak{p} \in \mathrm{V}(\mathfrak{a})} \mathfrak{p}.$$

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

$$\operatorname{rad}\left(\bigcap_{i=1}^{n} \mathfrak{p}_i^{e_i}\right) = \bigcap_{i=1}^{n} \operatorname{rad}(\mathfrak{p}_i^{e_i}) = \bigcap_{i=1}^{n} \operatorname{rad}(\mathfrak{p}_i) = \bigcap_{i=1}^{n} \mathfrak{p}_i.$$

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

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

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

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

$$\operatorname{rad}(\mathfrak{a}_i) = \operatorname{rad}(\langle X_1^i, \dots, X_i^i\rangle) = \operatorname{rad}(\langle X_1, \dots, X_i\rangle) = \langle X_1, \dots, X_i\rangle.$$

Hence

$$\bigcap_{i=1}^{\infty} \operatorname{rad}(\mathfrak{a}_i) = \bigcap_{i=1}^{\infty} \langle X_1, \dots, X_i\rangle = \langle X_1\rangle \supsetneq 0 = \operatorname{rad}(0) = \operatorname{rad}\left(\bigcap_{i=1}^{\infty} \mathfrak{a}_i\right).$$

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

$$\operatorname{rad}(\mathfrak{a}) + \operatorname{rad}(\mathfrak{b}) = \mathfrak{a} + \mathfrak{b} = \langle X + Y^2, X\rangle = \langle X, Y^2\rangle \subsetneq \langle X, Y\rangle = \operatorname{rad}(\langle X, Y^2\rangle) = \operatorname{rad}(\mathfrak{a} + \mathfrak{b}).$$

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 that $\mathfrak{a} = \mathfrak{b}_1 \cup \mathfrak{b}_2 \cup \mathfrak{b}_3$.

(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 $R \cong \mathbb{F}_2 \oplus \mathbb{F}_2 x \oplus \mathbb{F}_2 y$ and $\mathfrak{a} := \langle x, y\rangle \cong \mathbb{F}_2 x \oplus \mathbb{F}_2 y$ 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 $\mathfrak{a} = \mathfrak{b}_1 \cup \mathfrak{b}_2 \cup \mathfrak{b}_2$.

Extensions and Contractions

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

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

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

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

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

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 $\epsilon : R \to Q(R)$ given by $\varepsilon(r) = r/1$. Note that $0Q(R) = 0$ and $\mathfrak{a}Q(R) = Q(R)$ for $0 \ne \mathfrak{a} \le R$.

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

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

(d) Let $\varepsilon : k[X] \xrightarrow{\subseteq} k[X,Y]$. Since $\langle X,Y\rangle k[X,Y] \le k[X,Y]$, we have that $\varepsilon^{-1}(\langle X,Y\rangle k[X,Y]) = \langle X,Y\rangle k[X,Y] \bigcap k[X] = \langle X\rangle k[X]$.

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 $\mathfrak{a}_1 S \subseteq \mathfrak{a}_2 S$. 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., $\mathfrak{a}^e = \mathfrak{a}^{ece}$ and $\mathfrak{b}^c = \mathfrak{b}^{cec}$.[†]

(c) $(\mathfrak{a}_1 + \mathfrak{a}_2)S = \mathfrak{a}_1 S + \mathfrak{a}_2 S$ 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 $f^{-1}(\mathfrak{b}_1) = 0 = f^{-1}(\mathfrak{b}_2)$. Hence

$$f^{-1}(\mathfrak{b}_1 + \mathfrak{b}_2) = f^{-1}(S) = R \supsetneq 0 = f^{-1}(\mathfrak{b}_1) + f^{-1}(\mathfrak{b}_2).$$

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

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

$$(\mathfrak{a}_1 \cap \mathfrak{a}_2)S = \langle \overline{X^2 + XY^2}\rangle S = 0 \subsetneq \langle \overline{X}\rangle S = \mathfrak{a}_1 S \cap \mathfrak{a}_2 S.$$

[†] We have a bijection $\{\mathfrak{a} \le R \mid \mathfrak{a}^{ec} = \mathfrak{a}\} \rightleftarrows \{\mathfrak{b} \le S \mid \mathfrak{b}^{ce} = \mathfrak{b}\}$ given by $\mathfrak{a} \mapsto \mathfrak{a}^e$ and $\mathfrak{b}^c \mapsfrom \mathfrak{b}$.

(e) $(\mathfrak{a}_1\mathfrak{a}_2)S = (\mathfrak{a}_1 S)(\mathfrak{a}_2 S)$ 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 $f : R = k[X] \to S$, where

$$S = k[X]/(X(X-1)) = k[X]/(X^2 - X) \cong k[X]/\langle X\rangle \times k[X]/\langle X-1\rangle \cong k \times k$$

by Chinese Remainder Theorem. Note that in $k \times k$, $(1,0) = (1,0)^2$. Let $\mathfrak{b}_1 = \langle \overline{X}\rangle S = \mathfrak{b}_2$. Then $\mathfrak{b}_1\mathfrak{b}_2 = \langle \overline{X}^2\rangle S = \langle \overline{X}\rangle S = \mathfrak{b}_1$. Hence

$$f^{-1}(\mathfrak{b}_1\mathfrak{b}_2) = f^{-1}(\mathfrak{b}_1) = f^{-1}(\langle \overline{X}\rangle S) = \langle X\rangle R \supsetneq \langle X^2\rangle R = f^{-1}(\mathfrak{b}_1)f^{-1}(\mathfrak{b}_2).$$

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

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

$$(\mathfrak{a}_1 S : \mathfrak{a}_2 S) = (0 : 0) = S \supsetneq 0 = \langle X\rangle S = (\langle X^2\rangle : \langle X\rangle)S = (\mathfrak{a}_1 : \mathfrak{a}_2)S.$$

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

$$f^{-1}(\mathfrak{b}_1 : \mathfrak{b}_2) = f^{-1}(\langle X\rangle) = 0 \subsetneq R = (0:0) = (f^{-1}(\mathfrak{b}_1) : f^{-1}(\mathfrak{b}_2)).$$

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

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

$$\operatorname{rad}(\mathfrak{a})S = \operatorname{rad}(0R)S = 0S = 0 \subsetneq \langle \overline{X}\rangle S = \operatorname{rad}(0S) = \operatorname{rad}(\mathfrak{a}S).$$

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

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

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

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), $\mathfrak{b} \supseteq f^{-1}(\mathfrak{b})S$, hence $f^{-1}(\mathfrak{b}) \supseteq f^{-1}(f^{-1}(\mathfrak{b})S)$. $\subseteq$ Let $x \in f^{-1}(\mathfrak{b})$. Then $f(x) = f(x) \cdot 1 \in \langle f(f^{-1}\mathfrak{b})\rangle S = f^{-1}(\mathfrak{b})S$. Hence $x \in f^{-1}(f^{-1}(\mathfrak{b})S)$.

(c) $\supseteq$ Since $\mathfrak{a}_1 + \mathfrak{a}_2 \supseteq \mathfrak{a}_1, \mathfrak{a}_2$, we have that $(\mathfrak{a}_1 + \mathfrak{a}_2)S \supseteq \mathfrak{a}_1 S, \mathfrak{a}_2 S$. Hence $(\mathfrak{a}_1 + \mathfrak{a}_2)S \supseteq \mathfrak{a}_1 S + \mathfrak{a}_2 S$. $\subseteq$ A set of generators of $(\mathfrak{a}_1 + \mathfrak{a}_2)S$ over S is

$$\{f(a_1 + a_2) = f(a_1) + f(a_2) \mid a_1 \in \mathfrak{a}_1, a_2 \in \mathfrak{a}_2\} \subseteq \mathfrak{a}_1 S + \mathfrak{a}_2 S.$$

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

Note that $x \in f^{-1}(\mathfrak{b}_1 \cap \mathfrak{b}_2)$ 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

$$\left\{ f\left(\sum_i^{\text{finite}} \alpha_i\beta_i\right) = \sum_i^{\text{finite}} f(\alpha_i)f(\beta_i) \;\middle|\; \alpha_i \in \mathfrak{a}_1,\ \beta_i \in \mathfrak{a}_2, \forall i \right\} \subseteq (\mathfrak{a}_1 S)(\mathfrak{a}_2 S).$$

$\supseteq$ Note that

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

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 $i = 1, \ldots, n$. Then $f(a_{1i}) \in \mathfrak{b}_1$ and $f(a_{2i}) \in \mathfrak{b}_2$ for $i = 1, \ldots, n$. Since f is a ring homomorphism, $f(\sum_{i=1}^n a_{1i}a_{2i}) = \sum_{i=1}^n f(a_{1i})f(a_{2i}) \in \mathfrak{b}_1\mathfrak{b}_2$. Hence $\sum_{i=1}^n a_{1i}a_{2i} \in f^{-1}(\mathfrak{b}_1\mathfrak{b}_2)$.

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

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

Note that

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

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

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

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

Note that $x \in f^{-1}(\operatorname{rad}(\mathfrak{b}))$ if and only if $f(x) \in \operatorname{rad}(\mathfrak{b})$ 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 $x \in \operatorname{rad}(f^{-1}(\mathfrak{b}))$. ☐

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

Proof. For any $y \in \operatorname{Nil}(R)$, there is a $n \geq 1$ such that $y^n = 0$, so

$$(1 - y + y^2 - \cdots + (-1)^{n-1}y^{n-1})(1 + y) = 1 - y^n = 1,$$

hence $1 + y \in R^\times$.

Let $u \in R^\times$ and $x \in \operatorname{Nil}(R)$. Then $u^{-1}x \in \operatorname{Nil}(R)$. Hence $1 + u^{-1}x \in R^\times$. Thus, $u + x = u(1 + (u^{-1}x)) \in R^\times$. ☐

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

(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

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

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

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

(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 $\epsilon^* : \mathrm{Spec}(A[\![X]\!]) \to \mathrm{Spec}(A)$ 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,

$$\begin{aligned} \text{m-Spec}(A) &\overset{\epsilon^*}{\underset{\Lambda}{\rightleftarrows}} \text{m-Spec}(A[\![X]\!]) \\ \mathfrak{n} &\longmapsto \langle \mathfrak{n}, X \rangle A[\![X]\!] \\ \mathfrak{m} \cap A &\longleftarrow\!\shortmid \mathfrak{m} \end{aligned}$$

Proof. (a) $\Longrightarrow$ 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

$$1_A = f \cdot f^{-1} = \left(\sum_{i=0}^\infty a_i X^i \right) \left(\sum_{j=0}^\infty b_j X^j \right) = a_0 b_0 + (a_0 b_1 + a_1 b_0) X + \cdots .$$

Hence $a_0 b_0 = 1_A$ and hence $a_0 \in A^\times$.

$\Longleftarrow$ We try to find $g = \sum_{j=0}^\infty b_i X^i \in A[\![X]\!]$ such that $fg = 1$, i.e., $1 = \sum_{i=0}^\infty (\sum_{j=0}^i a_j b_{i-j}) X^i$. Then $a_0 b_0 = 1$, $a_0 b_1 + a_1 b_0 = 0$, $a_0 b_2 + a_1 b_1 + a_2 b_0 = 0$, $\cdots$. 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 that $a_0 \in A^\times$ 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

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

(c) Let $\tau : A \twoheadrightarrow A/\mathfrak{a}$ be the natural projection. Then by (b), $\tau[\![X]\!] : A[\![X]\!] \to \frac{A}{\mathfrak{a}}[\![X]\!]$ is a well-defined ring homomorphism with $A[\![X]\!] \geq \text{Ker}(\tau[\![X]\!]) = \text{Ker}(\tau)[\![X]\!] = \mathfrak{a}[\![X]\!]$. Since τ 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 that $\langle \mathfrak{a} \rangle A[\![X]\!] \subseteq \text{Ker}(\tau[\![X]\!]) = \mathfrak{a}[\![X]\!]$.

In addition, assume $\mathfrak{a} = (\alpha_1, \ldots, \alpha_n)A$ for some $\alpha_1, \ldots, \alpha_n \in \mathfrak{a}$. Let $f \in \mathfrak{a}[\![X]\!]$. Then $a_i \in \mathfrak{a} = (\alpha_1, \ldots, \alpha_n)A$ for $i \geq 0$. Hence for $i \geq 0$, we have that $a_i = \sum_{j=1}^n b_{ij} \alpha_j$ for some $b_{i1}, \ldots, b_{in} \in A$. 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 that

$$\begin{tikzcd} A[\![X]\!] \arrow[rrr, "\pi"] \arrow[ddd, "\tau[\![X]\!]"'] & & & A \arrow[ddd, "\tau"] \\ & \sum_{i=0}^{\infty} b_i X^i \arrow[r, mapsto] \arrow[d, mapsto] & b_0 \arrow[d, mapsto] & \\ & \sum_{i=0}^{\infty} \bar{b}_i X^i \arrow[r, mapsto] & \bar{b}_0 & \\ \frac{A}{\mathfrak{a}}[\![X]\!] \arrow[rrr, "\pi'"'] & & & \frac{A}{\mathfrak{a}} \end{tikzcd}$$

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

Note that

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

In general,

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

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 $\sum_{i=0}^{\infty} b_i X^i = b_0 + X \sum_{i=0}^{\infty} b_{i+1} X^i$ $\in \mathfrak{a} + XA[\![X]\!] \subseteq \langle X, \mathfrak{a} \rangle A[\![X]\!]$. Hence $I \subseteq \langle X, \mathfrak{a} \rangle A[\![X]\!]$.

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

Thus, by (c),

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

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

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

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

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

(f) $\Longrightarrow$ Assume $f \in \mathrm{Jac}(A[\![X]\!])$. Then by Proposition 1.29, $1 - fg \in A[\![X]\!]^\times$ for $g \in A[\![X]\!]$. Hence $(1 - a_0 a) + a_1 a x + a_2 a x^2 + \cdots = 1 - fa \in A[\![X]\!]^\times$ for $a \in A$. Then by (a), $1 - a_0 a \in A^\times$ for $a \in A$. Hence $a_0 \in \mathrm{Jac}(A)$ by Proposition 1.29.

$\Longleftarrow$ If $a_0 \in \mathrm{Jac}(A)$, 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 $f \in \mathrm{Jac}(A[\![X]\!])$. 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 that

$$1 - fg = 1 - \left(\sum_{i=0}^{\infty} a_i X^i\right)\left(\sum_{i=0}^{\infty} b_i X^i\right) = \underbrace{(1 - a_0 b_0)}_{\in A^\times} + \cdots .$$

Thus,

$$\mathrm{Jac}(A[\![X]\!]) = \left\{\sum_{i=0}^{\infty} a_i X^i \mid a_0 \in \mathrm{Jac}(A)\right\} = \langle \mathrm{Jac}(A), X\rangle A[\![X]\!]$$

by (d).

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

$\Longleftarrow$ Let A be an integral domain and $f, g \neq 0$ in $A[\![X]\!]$. Then $\mathrm{ord}(f), \mathrm{ord}(g) \neq \infty$. Hence $\mathrm{ord}(fg) = \mathrm{ord}(f)\,\mathrm{ord}(g) \neq \infty$. Hence $fg \neq 0$.

$\Longrightarrow$ 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), $X \notin A[\![X]\!]^\times$. Hence $A[\![X]\!]$ is not a field.

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

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

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

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

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

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

Since $\frac{A}{\mathfrak{a}}[\![X]\!]$ 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 $X \in \mathrm{Jac}(A[\![X]\!])$ by (f), and $\mathfrak{m} \in \text{m-Spec}(A[\![X]\!])$, we have that $X \in \mathfrak{m}$.

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

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

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

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

(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 that $\langle \mathfrak{m} \cap A, X\rangle = \mathfrak{m}$.

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

Note that $\Lambda(\text{m-Spec}(A)) \subseteq \text{m-Spec}(A[\![X]\!])$ 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 that

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

by (3).

Note that

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

by the proof of (c) for any $\mathfrak{n} \leq \text{m-Spec}(A)$.

Therefore, we have a 1-1 correspondence between m-Spec$(A[\![X]\!])$ and 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 $A = k[Y_1, Y_2, Y_3, \cdots]$ and $\mathfrak{a} = \langle Y_1, Y_2, Y_3, \cdots\rangle A$. Let $f = \sum_{i=1}^{\infty} Y_i X^i \in \mathfrak{a}[\![X]\!]$. We claim that $f \notin \langle \mathfrak{a}\rangle A[\![X]\!] = \langle Y_1, Y_2, \cdots\rangle A[\![X]\!]$. Suppose that $f \in \langle Y_1, Y_2, \cdots\rangle A[\![X]\!]$. Then there exists $m \geq 1$ and $\sum_{j=0}^{\infty} b_{ij} X^j = g_i \in A[\![X]\!]$ for $i = 1, \ldots, m$ such that

$$\sum_{j=1}^{\infty} Y_j X^j = f = \sum_{i=1}^{m} g_i Y_i = \sum_{i=1}^{m} \sum_{j=0}^{\infty} b_{ij} X^j Y_i = \sum_{j=0}^{\infty} \sum_{i=1}^{m} b_{ij} Y_i X^j.$$

Hence for $j \geq 1$, we have that $Y_j = \sum_{i=1}^{m} b_{ij} Y_i \in \langle Y_1, \ldots, Y_m\rangle A$. Then $Y_{m+1} \in \langle Y_1, \ldots, Y_m\rangle A$, a contradiction.

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

We claim that $f \notin \text{Nil}(A[\![X]\!])$. Note that

$$f^2 = \left(\sum_{i=1}^{\infty} \overline{Y}_i X^i\right)^2 = \underbrace{\overline{Y}_1^2 X^2}_{=0} + \underbrace{(2\overline{Y}_1 \overline{Y}_2) X^3}_{\neq 0} + \cdots,$$

and

$$f^3 = \left(\sum_{i=1}^{\infty} \overline{Y}_i X^i \right)^3 = \underbrace{\overline{Y}_1^3 X^3}_{=0} + \underbrace{(2\overline{Y}_1 \overline{Y}_3 + \overline{Y_2^2}) X^4}_{\neq 0} + \cdots ,$$

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 $d \geq 2$,

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

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

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

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 ϵ is

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

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 (possible 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_λ is open for $\lambda \in \Lambda$, then $\bigcup_{\lambda \in \Lambda} U_\lambda$ is open, and if U_i open for $i = 1, \ldots, d$, 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 $\mathscr{T}$ of subsets of X ($\mathscr{T} \subseteq \mathcal{P}(X)$) such that

(a) $\emptyset, X \in \mathscr{T}$,

(b) for any $\{U_\lambda\}_{\lambda \in \Lambda} \subseteq \mathscr{T}$, $\bigcup_{\lambda \in \Lambda} U_\lambda \in \mathscr{T}$ and

(c) for $n \geq 1$ and $U_1, \ldots, U_n \in \mathscr{T}$, $\bigcap_{i=1}^n U_\lambda \in \mathscr{T}$.

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

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

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 $\operatorname{Spec}(R) = X$ has open sets

$$\{\operatorname{Spec}(R) \smallsetminus \mathrm{V}(S) \mid S \subseteq R\} = \{\mathfrak{p} \in \operatorname{Spec}(R) \mid \mathfrak{p} \not\supseteq S \subseteq R\}.$$

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

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

Notation. Denote the Zariski open sets

$$\mathscr{Z} = \{\mathrm{Spec}(R) \setminus \mathrm{V}(S) \mid S \subseteq R\} = \{\mathrm{Spec}(R) \setminus \mathrm{V}(\mathfrak{a}) \mid \mathfrak{a} \leq R\}.$$

Example 2.7. Compute $\mathscr{Z}$ of $\mathrm{Spec}(\mathbb{Z}) = X$. Since $\mathbb{Z}$ is a P.I.D., $\mathscr{Z} = \{\mathrm{Spec}(\mathbb{Z}) \setminus \mathrm{V}(m) \mid m \geq 0\}$. Since $\mathrm{V}(0) = \mathrm{Spec}(\mathbb{Z})$, $X_0 = \mathrm{Spec}(\mathbb{Z}) \setminus \mathrm{V}(0) = \emptyset$, and since $\mathrm{V}(1) = \emptyset$, $X_1 = \mathrm{Spec}(\mathbb{Z}) \setminus \mathrm{V}(1) = \mathrm{Spec}(\mathbb{Z})$. For $m \geq 2$, write $m = p_1^{e_1} \cdots p_n^{e_n}$ with $p_1, \ldots, p_n$ distinct primes and $e_1, \ldots, e_n \geq 1$, then $\mathrm{V}(m) = \{\langle p_1 \rangle, \cdots, \langle p_n \rangle\}$ and so $X_m = \mathrm{Spec}(\mathbb{Z}) \setminus \mathrm{V}(m) = X \setminus \{\langle p_1 \rangle, \ldots, \langle p_n \rangle\}$. Note that $\mathscr{Z} = \bigcup_{m=0}^{\infty} X_m$. 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 $X = \mathrm{Spec}(R)$. Then $X_0 = X \setminus \mathrm{V}(0) = \emptyset$ and $X_1 = X \setminus \mathrm{V}(1) = X$.

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

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 $i = 1, \ldots, n$ if and only if $f_i \notin \mathfrak{p}$ for $i = 1, \ldots, n$ if and only if 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 $X = \mathrm{Spec}(R)$, the closed sets are $\{\mathrm{V}(S) \mid S \subseteq R\} = \{\mathrm{V}(\mathfrak{a}) \mid \mathfrak{a} \leq R\}$.

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

(a) $X, \emptyset \in \mathscr{V}$,

(b) closed under arbitrary intersections, i.e., for any $\{V_\lambda\}_{\lambda \in \Lambda} \subseteq \mathscr{V}$, then $\bigcap_{\lambda \in \Lambda} V_\lambda \in \mathscr{V}$,

(c) closed under fintie unions, i.e., for $n \geq 1$ and $V_1, \ldots, V_n \in \mathscr{V}$, $\bigcup_{i=1}^{n} V_i \in \mathscr{V}$.

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* $\mathrm{Spec}(R) = X$ *is a topology.*

Proof. Note that $\mathscr{Z} = \{\mathrm{Spec}(R) \setminus \mathrm{V}(\mathfrak{a}) \mid \mathfrak{a} \leq R\}$. Let $\mathscr{V} = \{X \setminus Z \mid Z \in \mathscr{Z}\} = \{\mathrm{V}(\mathfrak{a}) \mid \mathfrak{a} \leq R\}$.

(a) $X = \mathrm{V}(0) \in \mathscr{V}$ and $\emptyset = \mathrm{V}(1) \in \mathscr{V}$,

(b) For $\mathfrak{a}_\lambda \leq \mathfrak{a}$ for any $\lambda \in \Lambda$, $\bigcap_{\lambda \in \Lambda} \mathrm{V}(\mathfrak{a}_\lambda) = \mathrm{V}(\sum_{\lambda \in \Lambda} \mathfrak{a}_\lambda) \in \mathscr{V}$ by Fact 1.36.

(c) For $n \geq 1$ and $\mathfrak{a}_1, \ldots, \mathfrak{a}_n \leq R$, $\bigcup_{i=1}^{n} \mathrm{V}(\mathfrak{a}_i) = \mathrm{V}(\bigcap_{i=1}^{n} \mathfrak{a}_i) \in \mathscr{V}$ by Proposition 1.39(a). $\square$

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

Definition 2.14. A *basis* for the topology $\mathscr{T}$ on a topological space X is a subset $\mathcal{B} \subseteq \mathscr{T}$ 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 $X = \operatorname{Spec}(R)$, $\mathcal{B} = \{X_f \mid f \in R\}$ is a basis for the Zariski topology.*

Proof. It suffices to show $X \smallsetminus \mathrm{V}(S) = \bigcup_{s \in S} X_s$ for $S \subseteq R$. Note that $\mathfrak{p} \in X \smallsetminus \mathrm{V}(S)$ 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 $U \subseteq X = \operatorname{Spec}(R)$, there exist $s_1, \ldots, s_n \in R$ such that $U = X_{s_1} \cup \cdots \cup X_{s_n}$, i.e., open sets are the finite union of the basis open sets.

Proof. Write $U = X \smallsetminus \mathrm{V}(\mathfrak{a})$ for some $\mathfrak{a} \leq R$. Since R is noetherian, $\mathfrak{a} = \langle s_1, \ldots, s_n \rangle$ for some $n \geq 1$ and $s_1, \ldots, s_n \in \mathfrak{a}$. Then

$$U = X \smallsetminus \mathrm{V}(\langle s_1, \ldots, s_n \rangle) = X \smallsetminus \mathrm{V}(s_1, \ldots, s_n) = \bigcup_{i=1}^{n} X_{s_i}$$

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 $\{U_\lambda\}_{\lambda \in \Lambda} \subseteq \mathscr{T}$, if $X = \bigcup_{\lambda \in \Lambda} U_\lambda$, then there exist $n \geq 1$ and $\lambda_1, \ldots, \lambda_n \in \Lambda$ such that $X = \bigcup_{i=1}^{n} U_{\lambda_i}$.

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

Proof. Since each open set U_λ can be written as a union of X_f's with $f \in R$, without loss of generality, assmue $X = \bigcup_{\lambda \in \Lambda} X_{f_\lambda} = X \smallsetminus \mathrm{V}(\bigcup_{\lambda \in \Lambda} f_\lambda)$ by the proof of Theorem 2.16. Then $\emptyset = \mathrm{V}(\bigcup_{\lambda \in \Lambda} f_\lambda) = \mathrm{V}(\langle \bigcup_{\lambda \in \Lambda} f_\lambda \rangle)$. Hence by Proposition 1.32(b), $\langle \bigcup_{\lambda \in \Lambda} f_\lambda \rangle = R \ni 1$. Then $1 = g_{\lambda_1} f_{\lambda_1} + \cdots + g_{\lambda_n} f_{\lambda_n}$ for some $n \geq 1$, $\lambda_1, \ldots, \lambda_n \in \Lambda$ and $g_{\lambda_1}, \ldots, g_{\lambda_n} \in R$. Hence $\langle f_{\lambda_1}, \ldots, f_{\lambda_n} \rangle = R$. Then

$$\mathrm{V}(f_{\lambda_1}, \ldots, f_{\lambda_n}) = \mathrm{V}(\langle f_{\lambda_1}, \ldots, f_{\lambda_n} \rangle) = \mathrm{V}(R) = \emptyset.$$

Thus, $X = X \smallsetminus \emptyset = X \smallsetminus \mathrm{V}(f_{\lambda_1}, \ldots, f_{\lambda_n}) = X_{f_{\lambda_1}} \cup \cdots \cup X_{f_{\lambda_n}}$. $\square$

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

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

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

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

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

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

We have that

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

Hilbert's Nullstellensatz: If $k = \overline{k}$, then $\mathrm{Z}(\mathfrak{b}) \neq \emptyset$ for $\mathfrak{b} \lneq k[\underline{X}]$.
Grothendieck: there exists more geometric data in $\mathrm{Spec}(k[\underline{X}])$.
Let $V := \mathrm{Z}(T) = \mathrm{Z}(\mathfrak{b})$, where $\mathfrak{b} = \langle T \rangle \leq k[\underline{X}]$. Then

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

Hilbert's Nullstellensatz: If $k = \overline{k}$, then $\mathrm{I}(\mathrm{Z}(\mathfrak{b})) = \mathfrak{b}$.
Coordinate ring of V: $\Gamma(V) = k[\underline{X}]/\,\mathrm{I}(V)$.
We have that

$$\begin{aligned} \overline{\varphi} : V &\longhookrightarrow \text{m-Spec}(k[V]) \subseteq \mathrm{Spec}(k[V]) \\ \underline{a} &\longmapsto \frac{(X_1 - a_1, \ldots, X_d - a_d)}{\mathrm{I}(V)} = (x_1 - a_1, \ldots, x_d - a_d). \end{aligned}$$

Hilbert's Nullstellensatz: If $k = \overline{k}$, then similarly, $\overline{\varphi}$ is onto.
Grothenick: there exists more geometric data in $\mathrm{Spec}(k[V])$.

Set up: $R \ni f$,

$$X = \mathrm{Spec}(R) \supseteq X_f = X \smallsetminus \mathrm{V}(f) = \{\mathfrak{p} \in \mathrm{Spec}(R) \mid f \notin \mathfrak{p}\}.$$

Recall. Let $S = \{1, f, f^2, \cdots\}$. We have that

$$R_f = S^{-1}R = \left\{ \frac{r}{f^n} \mid r \in R, n \geq 0 \right\} = R[1/f].$$

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

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

(b) Restrict codomain, the induced map $\varphi^*_f : \mathrm{Spec}(R_f) \to X_f$ is 1-1 and onto.

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

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

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

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

Since $f^n \notin \mathfrak{p}$ for $n \geq 0$, $\frac{1}{1} \notin \mathfrak{p}_f$. Hence $\mathfrak{p}_f \lneq R_f$. 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 $\mathfrak{p} \in \mathrm{Spec}(R)$, $x \in \mathfrak{p}$ or $y \in \mathfrak{p}$. Hence $\frac{x}{f^n} \in \mathfrak{p}_f$ or $\frac{y}{f^m} \in \mathfrak{p}_f$. Hence $\mathfrak{p}_f \in \mathrm{Spec}(R_f)$.

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

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

$\square$

Subspaces

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

Proof. $Y = X \cap Y \in \mathscr{T}_Y$ since $X \in \mathscr{T}$. $\emptyset = \emptyset \cap Y \in \mathscr{T}_Y$ since $\emptyset \in \mathscr{T}$. Let $\{U_\lambda \cap Y \mid U_\lambda \in \mathscr{T}\}_{\lambda\in\Lambda} \subseteq \mathscr{T}_Y$. Since $\mathscr{T}$ is a topology on X, $\bigcup_{\lambda\in\Lambda} U_\lambda \subseteq \mathscr{T}$. Hence $\bigcup_{\lambda\in\Lambda}(U_\lambda \cap Y) = (\bigcup_{\lambda\in\Lambda} U_\lambda) \cap Y \in \mathscr{T}_Y$. Let $U_1 \cap Y, \ldots, U_n \cap Y \in \mathscr{T}_Y$. Similarly, we have that $\bigcap_{i=1}^n (U_\lambda \cap Y) \in \mathscr{T}_Y$. $\square$

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

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

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

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

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

(a) closed sets: $\mathrm{V}(\mathfrak{a}) \cap X_f = \{\mathfrak{p} \in \operatorname{Spec}(R) \mid \mathfrak{a} \subseteq \mathfrak{p} \not\ni f\}$, where $\mathfrak{a} \leq R$;

(b) open sets: $(X \smallsetminus \mathrm{V}(\mathfrak{a})) \cap X_f = \{\mathfrak{p} \in \operatorname{Spec}(R) \mid \mathfrak{a} \not\subseteq \mathfrak{p} \not\ni f\}$, 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 $\mathrm{V}(\mathfrak{a}) \subseteq X = \operatorname{Spec}(R)$ has

(a) closed sets: $\mathrm{V}(\mathfrak{b}) \cap \mathrm{V}(\mathfrak{a}) = \{\mathfrak{p} \in \operatorname{Spec}(R) \mid \mathfrak{b} + \mathfrak{a} \subseteq \mathfrak{p}\}$, where $\mathfrak{b} \leq R$;

(b) open sets: $(X \smallsetminus \mathrm{V}(\mathfrak{b})) \cap \mathrm{V}(\mathfrak{a}) = \{\mathfrak{p} \in \operatorname{Spec}(R) \mid \mathfrak{b} \not\subseteq \mathfrak{p} \supseteq \mathfrak{a}\}$, where $\mathfrak{b} \leq R$;

(c) basic open sets: $X_g \cap \mathrm{V}(\mathfrak{a})$, where $g \in R$.

Proposition 2.24. Let $\mathfrak{a} \leq R$, $\varphi : R \to R_f$ and $\varphi_f^* : \operatorname{Spec}(R_f) =: Z \to X_f$ as in Proposition 2.20.

(a) $(\varphi_f^*)^{-1}(\mathrm{V}(\mathfrak{a}) \cap X_f) = \mathrm{V}(\mathfrak{a}_f)$.

(b) $(\varphi_f^*)^{-1}((X \smallsetminus \mathrm{V}(\mathfrak{a})) \cap X_f) = \operatorname{Spec}(R_f) \smallsetminus \mathrm{V}(\mathfrak{a}_f)$.

(c) $(\varphi_f^*)^{-1}(X_g \cap X_f) = Z_{g|1}$ for $g \in R$.

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

[†]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 φ_f^* is 1-1, $\varphi^{-1}(\mathfrak{p})R_f = \mathfrak{q}R_f = \mathfrak{q}_f = \mathfrak{p}$.

Method 2: We claim that $\varphi^{-1}(I)R_f = I$ 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 $n \geq 0$. Hence $\varphi(r) = \frac{r}{1} = \frac{f^n}{1} \cdot \frac{r}{f^n} \in I$. Then $r \in \varphi^{-1}(I)$. Hence $i = \frac{r}{f^n} = \varphi(r) \cdot \frac{1}{f^n} \in \varphi^{-1}(I)R_f$.

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

(c) Method 1. By (a), we have that

$$\begin{aligned}(\varphi_f^*)^{-1}(X_g \cap X_f) &= (\varphi_f^*)^{-1}((X \smallsetminus \mathrm{V}(g)) \cap X_f) = \operatorname{Spec}(R_f) \smallsetminus \mathrm{V}((g)_f) \\ &= \{\mathfrak{p}_f \mid \mathfrak{p} \in \operatorname{Spec}(R), \mathfrak{p}_f \not\supseteq (g)_f\} = \{\mathfrak{p}_f \mid g \notin \mathfrak{p} \in \operatorname{Spec}(R)\} \\ &= \{\mathfrak{p}_f \mid \mathfrak{p} \in X_g\}.\end{aligned}$$

Method 2. Let $\mathfrak{p} \in \operatorname{Spec}(R_f)$. 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 $\mathfrak{p} \in \{\mathfrak{q}_f \mid \mathfrak{q} \in X_g\}$. □

Continuous Functions and Homeomorphisms

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

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

Remark. Let $Y \subseteq X$. The subspace topology $\mathscr{T}_Y$ is the smallest topology on Y such that $Y \overset{\subseteq}{\hookrightarrow} X$ is continuous.

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

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

Proof. Let $\mathfrak{a} \leq R$ and $\mathfrak{p} \in \operatorname{Spec}(S)$. Then $\mathfrak{p} \in (\varphi^*)^{-1}(\mathrm{V}(\mathfrak{a}))$ if and only if $\varphi^*(\mathfrak{p}) \in \mathrm{V}(\mathfrak{a})$ 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 $\mathfrak{p} \in \mathrm{V}(\mathfrak{a}S)$. □

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

Proof. By Proposition 2.24, we have that φ_f^* is continuous or by Theorem 2.27 and Lemma 2.30.

By Proposition 2.20, φ_f^* is 1-1.

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

Example. Let k be a field and $R = k[\![X]\!]$. We claim that $\operatorname{Spec}(R) = \{0, \langle X\rangle\}$. 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 that $\sum_{i=0}^{\infty} a_{m+i}X^i \in R^\times$. Hence 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 $0 \neq \mathfrak{p} \in \operatorname{Spec}(R)$.

Define $\varphi : R \to S = k \times Q(R)$ 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 that φ is a ring homomorphism and $\operatorname{Spec}(S) = \{k \times 0, 0 \times Q(R)\}$. Hence the continuous function $\varphi^* : \operatorname{Spec}(S) \to \operatorname{Spec}(R)$ sending $k \times 0$ to 0 and $0 \times Q(R)$ to $\langle X\rangle$ is 1-1 and onto.

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

Corollary 2.29. X_f is quasi-compact.

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

Example. $U\subseteq \operatorname{Spec}(R)=X$ may not be quasi-compact. Let $R=k[X_1,X_2,X_3,\cdots]$. Let

$$U=X\smallsetminus \mathrm{V}(X_1,X_2,X_3,\cdots)=X\smallsetminus\bigcap_{i=1}^{\infty}\mathrm{V}(X_i)=\bigcup_{i=1}^{\infty}(X\smallsetminus\mathrm{V}(X_i))$$

by Fact 1.36(a). Let $n\geq 1$. We claim that $\mathrm{V}(X_1,X_2,X_3,\cdots)\neq\mathrm{V}(X_1,X_2,\ldots,X_n)$. "$\subseteq$". It is straightforward. "$\not\supseteq$". Let $\mathfrak{p}=\langle X_1,\ldots,X_n\rangle\in\mathrm{V}(X_1,\ldots,X_n)$. Then $\mathfrak{p}\notin\mathrm{V}(X_1,X_2,\cdots)$ since $\langle X_1,X_2,\cdots\rangle\ni X_{n+1}\notin\mathfrak{p}$. Hence

$$U=X\smallsetminus\mathrm{V}(X_1,X_2,X_3,\cdots)\neq X\smallsetminus\mathrm{V}(X_1,\ldots,X_n)=X\smallsetminus\bigcap_{i=1}^{n}\mathrm{V}(X_i)=\bigcup_{i=1}^{n}(X\smallsetminus\mathrm{V}(X_i))$$

for $n\geq 1$.

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

Proof. Let $U=\bigcup_{\lambda\in\Lambda}U_\lambda$ be an open cover with U_λ open in X for $\lambda\in\Lambda$. Use the fact that X_f's form a basis to assume without losss of generality $U_\lambda=X_{f_\lambda}$ for some $f_\lambda\in R$ for $\lambda\in\Lambda$. Then

$$U=\bigcup_{\lambda\in\Lambda}X_{f_\lambda}=\bigcup_{\lambda\in\Lambda}(X\smallsetminus\mathrm{V}(f_\lambda))=X\smallsetminus\mathrm{V}(\langle f_\lambda\mid\lambda\in\Lambda\rangle).$$

Since R is noetherian, there exist $f_{\lambda_1},\ldots,f_{\lambda_n}\in R$ such that $\langle f_\lambda\mid\lambda\in\Lambda\rangle=\langle f_{\lambda_1},\ldots,f_{\lambda_n}\rangle$. Hence $U=X\smallsetminus\mathrm{V}(\langle f_{\lambda_1},\ldots,f_{\lambda_n}\rangle)=\bigcup_{i=1}^{n}X_{f_{\lambda_i}}$. □

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

Proof. Let $U\subseteq Z$ be open. Since Z has the subspace topology, $U=Z\cap\widetilde{U}$ for some $\widetilde{U}\subseteq Y$ open. Since $f(X)\subseteq Z$,

$$f_Z^{-1}(U)=f^{-1}(Z\cap\widetilde{U})=f^{-1}(Z)\cap f^{-1}(U)=f^{-1}(\widetilde{U})$$

is open in X since f is continuous. □

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

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

(b) Give the codomain subspace topology and restrict the codomain, then $\pi^*_{\mathfrak{b}}:\operatorname{Spec}(R/\mathfrak{b})\to\mathrm{V}(\mathfrak{b})$ is continuous, 1-1 and onto, and $(\pi^*_{\mathfrak{b}})^{-1}$ is continuous. "homeomorphism".

Proof. By prime correspondence,

$$\begin{aligned} \operatorname{Spec}(R/\mathfrak{b}) &\rightleftharpoons \mathrm{V}(\mathfrak{b}) \\ \mathfrak{p}/\mathfrak{b} &\longleftarrow \mathfrak{p} \supseteq \mathfrak{b} \\ \mathfrak{p} &\longmapsto \pi^{-1}(\mathfrak{p}) = \pi^*(\mathfrak{p}). \end{aligned}$$

Hence $\pi^*(\operatorname{Spec}(R/\mathfrak{b})) = \mathrm{V}(\mathfrak{b})$, 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,

$$((\pi^*_{\mathfrak{b}})^{-1})^{-1}(\mathrm{V}(\mathfrak{a}/\mathfrak{b})) = \pi^*_{\mathfrak{b}}(\mathrm{V}(\mathfrak{a}/\mathfrak{b})) = \mathrm{V}(\mathfrak{a}) \cap \mathrm{V}(\mathfrak{b}) = \mathrm{V}(\mathfrak{a}).$$

Hence $(\pi^*_{\mathfrak{b}})^{-1}$ is continuous. □

Corollary 2.32. $\mathrm{V}(\mathfrak{b})$ 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 $X = \operatorname{Spec}(R)$ is irreducible.

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

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 $\mathfrak{q} \in \operatorname{Spec}(R)$, then $\mathrm{V}(\mathfrak{q}) \subseteq \operatorname{Spec}(R)$ with subspace topology is irreducible.

Proof. Let $\mathfrak{q} \in \operatorname{Spec}(R)$. Then $R/\mathfrak{q}$ is an integral domain. Hence $\operatorname{Spec}(R/\mathfrak{q})$ is irreducible by Example 2.34. Since $\mathrm{V}(\mathfrak{q})$ is homeomorphic to $\operatorname{Spec}(R/\mathfrak{q})$ by Theorem 2.31, we have that $\emptyset \neq \mathrm{V}(\mathfrak{q})$ is irreducible. □

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

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

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

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

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

Lemma 2.38. The followings are equivalent.

(i) X is irreducible.

(ii) For $V_1, V_2 \subsetneq X$ closed, $V_1 \cup U_2 \subsetneq X$.

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

"Non-empty open sets are dense".

Proof. (i)$\Longleftrightarrow$(ii) By Definition 2.33.

(ii)$\Longrightarrow$(iii) Assume (b). Let $\emptyset \neq U \subseteq X$ be open. Suppose $V_1 := \overline{U} \neq X$. Let $V_2 := X \setminus U$. Then $V_1, V_2 \subseteq X$ are closed. Hence

$$X = U \cup (X \setminus U) \subseteq \overline{U} \cup (X \setminus U) = V_1 \cup V_2 \subsetneq X$$

by assumption, a contradiction.

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

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. $X = \operatorname{Spec}(R)$ is irreducible if and only if $\operatorname{Nil}(R) \in \operatorname{Spec}(R)$.

Proof. $\Longleftarrow$ Assume $\operatorname{Nil}(R) \in \operatorname{Spec}(R)$. By Proposition 1.32(c), $\operatorname{V}(\operatorname{Nil}(R)) = \operatorname{Spec}(R)$. Then by Corollary 2.35, $\operatorname{Spec}(R) = \operatorname{V}(\operatorname{Nil}(R))$ is irreducible.

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

Proposition 2.40. We have the following.

(a) If $Y \subseteq X$ is irreducible, then $\overline{Y} \subseteq X$ with subspace topology is irreducible.

(b) If $\mathscr{C}$ is a chain of irreducible subsets of X, then $\bigcup_{Y \in \mathscr{C}} Y$ 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 $\overline{Y} = V_1 \cup V_2$ with $V_1, V_2 \subseteq \overline{Y}$ closed. Let $i \in \{1, 2\}$. Since V_i is closed in $\overline{Y}$ and $\overline{Y}$ has subspace topology, there exists $\widetilde{V}_i \subseteq X$ closed in X such that $V_i = \widetilde{V}_i \cap \overline{Y}$. Set $V_i' = \widetilde{V}_i \cap Y = (\widetilde{V}_i \cap \overline{Y}) \cap Y = V_i \cap Y$. Since V_i is closed in $\overline{Y}$, $V_i' = V_i \cap Y$ is closed in Y[†]. Then

$$\overline{Y} = V_1 \cup V_2 = (\widetilde{V}_1 \cap \overline{Y}) \cup (\widetilde{V}_2 \cap \overline{Y}) = (\widetilde{V}_1 \cup \widetilde{V}_2) \cap \overline{Y}.$$

Hence $Y \subseteq \overline{Y} \subseteq \widetilde{V}_1 \cup \widetilde{V}_2$. Thus,

$$Y = (\widetilde{V}_1 \cup \widetilde{V}_2) \cap Y = (\widetilde{V}_1 \cap Y) \cup (\widetilde{V}_2 \cap Y) = V_1' \cup V_2'.$$

Since Y is irreducible, $Y = V_1'$ or V_2'. Say $Y = V_1' = V_1 \cap Y$. Then $Y \subseteq V_1 \subseteq \widetilde{V}_1$. Since $\widetilde{V}_1 \subseteq X$ is closed, $\overline{Y} \subseteq \widetilde{V}_1$. Thus, $\overline{Y} = \widetilde{V}_1 \cap \overline{Y} = V_1$.

[†]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

(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 $x_1 \in Z \smallsetminus V_1$ and $x_2 \in Z \smallsetminus V_2$. Hence 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 $x_1 \in Y_1 \smallsetminus V_1$ and $x_2 \in Y_1 \smallsetminus V_2$. Hence $V_1 \cap Y_1 \subsetneq Y_1$ 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 that $(V_1 \cap Y_1) \cup (V_2 \cap Y_1) \subsetneq Y_1$. Hence $Y_1 \not\subseteq V_1 \cup V_2$. 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. Hence Σ has a maximal element.

(d) Let $\mathcal{M}$ be the union of the maximal irreducible subsets of X. We claim that $X = M$. "$\supseteq$". 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), $\overline{Z}$ is irreducible. Also, since $Z \subseteq \overline{Z}$ and Z is maximal irreducible, we have that $Z = \overline{Z}$, i.e., Z is closed. □

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

Proposition 2.42. † Let $X = \operatorname{Spec}(R)$.

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

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

Proof. (a) $\Longleftarrow$ Let $\mathfrak{p} \in \operatorname{Spec}(R)$. Let $V, W \subseteq \mathrm{V}(\mathfrak{p})$ be closed such that $\mathrm{V}(\mathfrak{p}) = V \cup W$. Then $V = \mathrm{V}(\mathfrak{a}) \cap \mathrm{V}(\mathfrak{p})$ and $W = \mathrm{V}(\mathfrak{b}) \cap \mathrm{V}(\mathfrak{p})$ for some $\mathfrak{a}, \mathfrak{b} \leq R$. Since $\mathfrak{p} \in \operatorname{Spec}(R)$,

$$\mathfrak{p} \in \mathrm{V}(\mathfrak{p}) = V \cup W = (\mathrm{V}(\mathfrak{a}) \cap \mathrm{V}(\mathfrak{p})) \cup (\mathrm{V}(\mathfrak{b}) \cap \mathrm{V}(\mathfrak{p})) = \mathrm{V}(\mathfrak{a}+\mathfrak{p}) \cup \mathrm{V}(\mathfrak{b}+\mathfrak{p}) = \mathrm{V}((\mathfrak{a}+\mathfrak{p})(\mathfrak{b}+\mathfrak{p})).$$

Hence $\mathfrak{p} \supseteq (\mathfrak{a}+\mathfrak{p})(\mathfrak{b}+\mathfrak{p})$. Since $\mathfrak{p} \in \operatorname{Spec}(R)$, $\mathfrak{p} \supseteq \mathfrak{a}+\mathfrak{p} \supseteq \mathfrak{a}$ or $\mathfrak{p} \supseteq \mathfrak{b}+\mathfrak{p} \supseteq \mathfrak{b}$. Hence $\mathrm{V}(\mathfrak{p}) \subseteq \mathrm{V}(\mathfrak{a})$ or $\mathrm{V}(\mathfrak{p}) \subseteq \mathrm{V}(\mathfrak{b})$. Hence $\mathrm{V}(\mathfrak{p}) = \mathrm{V}(\mathfrak{a}) \cap \mathrm{V}(\mathfrak{p}) = V$ or $\mathrm{V}(\mathfrak{p}) = \mathrm{V}(\mathfrak{b}) \cap \mathrm{V}(\mathfrak{p}) = W$.

$\Longrightarrow$ Assume $V \subseteq X$ is closed and irreducible. Then $\emptyset \neq V = \mathrm{V}(\mathfrak{a}) = \mathrm{V}(\operatorname{rad}(\mathfrak{a}))$ for some $\mathfrak{a} \leq R$. Hence is suffices to show $\operatorname{rad}(\mathfrak{a}) \in \operatorname{Spec}(R)$. Note that $\mathfrak{r} := \operatorname{rad}(\mathfrak{a}) \lneq R$.

Method 1. Let $x, y \in R$ such that $xy \in \mathfrak{r}$. Then $\mathfrak{r}^2 \subseteq (xR+\mathfrak{r})(yR+\mathfrak{r}) \subseteq \mathfrak{r}$. Hence $\mathrm{V}(\mathfrak{r}) = \mathrm{V}(\mathfrak{r}^2) \supseteq \mathrm{V}((xR+\mathfrak{r})(yR+\mathfrak{r})) \supseteq \mathrm{V}(\mathfrak{r})$. Hence

$$V = \mathrm{V}(\mathfrak{r}) = \mathrm{V}((xR+\mathfrak{r})(yR+\mathfrak{r})) = (\mathrm{V}(xR) \cap \mathrm{V}(\mathfrak{r})) \cup (\mathrm{V}(yR) \cap \mathrm{V}(\mathfrak{r})) = (\mathrm{V}(xR) \cap V) \cup (\mathrm{V}(yR) \cap V).$$

Also, since $\mathrm{V}(xR) \cap V$ and $\mathrm{V}(xR) \cap V$ are closed in V and V is irreducible, we have that $\mathrm{V}(\mathfrak{r}) = \mathrm{V}(xR) \cap V \subseteq \mathrm{V}(xR)$ or $\mathrm{V}(\mathfrak{r}) = \mathrm{V}(yR) \cap V \subseteq \mathrm{V}(yR)$. Then

$$x \in xR \subseteq \operatorname{rad}(xR) = \bigcap_{\mathfrak{p}\in\mathrm{V}(xR)} \mathfrak{p} \subseteq \bigcap_{\mathfrak{p}\in\mathrm{V}(\mathfrak{r})} \mathfrak{p} = \operatorname{rad}(\mathfrak{r}) = \mathfrak{r}$$

by Fact 1.58(c) and (g), or $y \in \mathfrak{r}$ similarly. Hence $\operatorname{rad}(\mathfrak{a}) = \mathfrak{r} \in \operatorname{Spec}(R)$.

Method 2. Assume $\operatorname{rad}(\mathfrak{a}) \supseteq IJ$ for some $I, J \leq R$. Then $\mathrm{V}(I) \cup \mathrm{V}(J) = \mathrm{V}(IJ) \supseteq \mathrm{V}(\operatorname{rad}(\mathfrak{a})) = \mathrm{V}(\mathfrak{a})$. Since $\mathrm{V}(\mathfrak{a}) = V$ is irreducible and

$$\mathrm{V}(\mathfrak{a}) = (\mathrm{V}(\mathfrak{a}) \cap \mathrm{V}(I)) \cup (\mathrm{V}(\mathfrak{a}) \cap \mathrm{V}(J)) = \mathrm{V}(\mathfrak{a}I) \cup \mathrm{V}(\mathfrak{a}J),$$

†This proposition also holds for $\mathrm{V}(\mathfrak{a})$ with subspace topology and with $\operatorname{Min}(\mathrm{V}(\mathfrak{a}))$.

we have that $\mathrm{V}(I) \supseteq \mathrm{V}(\mathfrak{a})$ or $\mathrm{V}(J) \supseteq \mathrm{V}(\mathfrak{a})$. Hence by Proposition 1.32(d), $\operatorname{rad}(\mathfrak{a}) \supseteq \operatorname{rad}(I) \supseteq I$ or $\operatorname{rad}(\mathfrak{a}) \supseteq \operatorname{rad}(J) \supseteq J$.

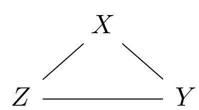
(b) Let V be an irreducible component of $X = \operatorname{Spec}(R)$. Then V is closed by Proposition 2.40(c) and maximal irreducible. Hence by (a), $V = \mathrm{V}(\mathfrak{p})$ for some $\mathfrak{p} \in \operatorname{Spec}(R)$. Let $\mathfrak{q} \in \operatorname{Spec}(R)$ such that $\mathfrak{q}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

Remark. Example 2.34, Corollary 2.35, and Proposition 2.39 follow from Proposition 2.42(a).

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:



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 that

$$I_G = \bigcap_{V \text{ min. v.cover}} P_V = P_{\{X,Y\}} \cap P_{\{Y,Z\}} \cap P_{\{X,Z\}} = \langle X, Y\rangle \cap \langle Y, Z\rangle \cap \langle X, Z\rangle.$$

Hence

$$\operatorname{Min}(k[X,Y,Z]) = \{P_V \mid V \text{ min. v.cover}\} = \{\langle X, Y\rangle, \langle Y, Z\rangle, \langle X, Z\rangle\}.$$

By Fact 1.15, $\operatorname{Min}(R) = \{\langle \overline{X}, \overline{Y}\rangle, \langle \overline{Y}, \overline{Z}\rangle, \langle \overline{X}, \overline{Z}\rangle\}$. Hence the irreducible components of $\operatorname{Spec}(R)$ are $\mathrm{V}(\langle \overline{X}, \overline{Y}\rangle)$, $\mathrm{V}(\langle \overline{X}, \overline{Z}\rangle)$ and $\mathrm{V}(\langle \overline{Y}, \overline{Z}\rangle)$.

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

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

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

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

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

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

(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 $\overline{\{0\}} = \mathrm{V}(0) = \operatorname{Spec}(R)$. 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, $\overline{\{\mathfrak{p}\}} = \mathrm{V}(\mathfrak{a})$ for some $\mathfrak{a} \leq R$ by Proposition 2.42(a). Hence $\mathfrak{a} \subseteq \mathfrak{p}$. Hence $\mathrm{V}(\mathfrak{p}) \subseteq \mathrm{V}(\mathfrak{a}) = \overline{\{\mathfrak{p}\}}$. Since $\overline{\{\mathfrak{p}\}}$ is the smallest closed subset containing $\mathfrak{p}$, we have that $\overline{\{\mathfrak{p}\}} = \mathrm{V}(\mathfrak{p})$.

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

$\Longleftarrow$ Assume $\mathfrak{p} \in$ m-Spec(R). Then by (a), $\overline{\{\mathfrak{p}\}} = \mathrm{V}(\mathfrak{p}) = \{\mathfrak{p}\}$.

(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) $\{1, f, f^2, \cdots\} \subseteq R$ is multiplicatively closed for $f \in R$.

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

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

(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 $\frac{r}{u}, \frac{s}{v} \in U^{-1}R$.
$0_{U^{-1}R} = \frac{0_R}{1_R} = \frac{0}{u}$ and $1_{U^{-1}R} = \frac{1_R}{1_R} = \frac{u}{u}$ for all $u \in U$.
$\frac{r}{u} = 0$ if and only if there exists $u'' \in U$ such that $u''r = 0$.
$\psi : R \to U^{-1}R$ given by $\psi(r) = \frac{r}{1}$ is a well-defined ring homomorphism. ψ is 1-1 if and only if $U \subseteq \operatorname{NZD}(R)$.

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

(b) If $U = R \smallsetminus \mathfrak{p}$ for some $\mathfrak{p} \in \operatorname{Spec}(R)$, 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 $\psi : R \to U^{-1}R$ 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 $u \in U$. Hence localization makes more elements invertible.

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

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

$$\begin{tikzcd} R \arrow[r, "\psi"] \arrow[dr, "\varphi"'] & U^{-1}R \arrow[d, dashed, "\exists!\ \Phi"] \\ & S \end{tikzcd} \qquad \begin{tikzcd} R \arrow[r, "\psi"] \arrow[dr, "\varphi"'] & U^{-1}R \arrow[d, "\Lambda"] \\ & S \end{tikzcd}$$

Proof. Let $\frac{r}{u} = \frac{r'}{u'}$. Then there exists $u'' \in U$ such that $u''(ru' - r'u) = 0$. Since φ is a ring homomorphism, we have that $\varphi(u'')(\varphi(r)\varphi(u') - \varphi(r')\varphi(u)) = 0$. Also, since $\varphi(u'') \in S^\times$, we have that $\varphi(r)\varphi(u') = \varphi(r')\varphi(u)$, i.e., $\varphi(r)\varphi(u)^{-1} = \varphi(r')\varphi(u')^{-1}$ since $\varphi(u), \varphi(u') \in S^\times$. Hence ϕ is well-defined. Since

$$\begin{aligned} \Phi\left(\frac{r}{u} + \frac{s}{v}\right) = \Phi\left(\frac{rv+su}{uv}\right) &= \varphi(rv+su)\varphi(uv)^{-1} = (\varphi(r)\varphi(v) + \varphi(s)\varphi(u)))\varphi(u)^{-1}\varphi(v)^{-1} \\ &= \varphi(r)\varphi(u)^{-1} + \varphi(s)\varphi(v)^{-1} = \Phi\left(\frac{r}{u}\right) + \Phi\left(\frac{s}{v}\right) \end{aligned}$$

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 that Φ is a ring homomorphism.

Suppose there is another ring homomorphism $\Lambda : U^{-1}R \to S$ such that $\Lambda \circ \psi = \varphi$. Then $\varphi(r) = \Lambda(\psi(r)) = \Lambda(\frac{r}{1})$ for $r \in R$. Hence

$$\Lambda\left(\frac{r}{u}\right) = \Lambda\left(\frac{r}{1}\frac{1}{u}\right) = \Lambda\left(\frac{r}{1}\right)\Lambda(\frac{u}{1})^{-1} = \varphi(r)\varphi(u)^{-1} = \Phi\left(\frac{r}{u}\right)$$

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 $U^{-1}\varphi : U^{-1}R \to U^{-1}S$ given by $U^{-1}\varphi(r/u) = \varphi(r)/\varphi(u)$.

$$\begin{tikzcd} R \arrow[rrr, "\psi"] \arrow[ddd, "\varphi"'] & & & U^{-1}R \arrow[ddd, "U^{-1}\varphi"] \\ & r \arrow[r, mapsto] \arrow[d, mapsto] & \frac{r}{1} \arrow[d, mapsto] & \\ & \varphi(r) \arrow[r, mapsto] & \frac{\varphi(r)}{1} & \\ S \arrow[rrr, "\rho"'] & & & U^{-1}S \end{tikzcd}$$

(c) If φ is onto, $U^{-1}\varphi$ is onto.

(d) If φ is 1-1, $U^{-1}\varphi$ is 1-1.

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

$$\begin{tikzcd} R \arrow[rr, "\psi"] \arrow[dr, "\varphi"] \arrow[dd, "\alpha\circ\varphi"'] & & U^{-1}R \arrow[dr, "U^{-1}\varphi"] \arrow[dd] & \\ & S \arrow[rr] \arrow[dl, "\alpha"] & & U^{-1}S \arrow[dl, "\varphi(U)^{-1}\alpha"] \\ T \arrow[rr] & & \varphi(U)^{-1}T \ := \alpha(\varphi(U))^{-1}T & \end{tikzcd}$$

Proof. (b) Let $\frac{r}{u} = \frac{r'}{u'} \in U^{-1}R$. Then there exists $u'' \in U$ such that $u''(ru' - r'u) = 0$. Hence there exists $\varphi(u'') \in \varphi(U)$ such that $\varphi(u'')(\varphi(r)\varphi(u') - \varphi(r')\varphi(u)) = 0$. Hence $\frac{\varphi(r)}{\varphi(u)} = \frac{\varphi(r')}{\varphi(u')} \in U^{-1}S$. Hence $U^{-1}\varphi$ is well-defined. Since

$$\begin{aligned} U^{-1}\varphi\left(\frac{r}{u} + \frac{s}{v}\right) &= U^{-1}\varphi\left(\frac{rv+su}{uv}\right) = \frac{\varphi(rv+su)}{\varphi(uv)} = \frac{\varphi(r)\varphi(v)+\varphi(s)\varphi(u)}{\varphi(u)\varphi(v)} \\ &= \frac{\varphi(r)}{\varphi(u)} + \frac{\varphi(s)}{\varphi(v)} = U^{-1}\varphi\left(\frac{r}{u}\right) + U^{-1}(\varphi)(\frac{s}{v}) \end{aligned}$$

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+ϵ, $\rho(\varphi(U)) \subseteq ((\varphi(U))^{-1}S)^{\times} = (U^{-1}S)^{\times}$. Then the uniqueness follows from Proposition 3.5.

(c) Assume φ is onto. Let $\frac{s}{\varphi(u)} \in U^{-1}S$ with $s \in S$ and $u \in U$. Since $\varphi : R \to S$ 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 φ is 1-1. Let $\frac{r}{u} \in U^{-1}R$ with $r \in R$ and $u \in U$. Then $\frac{r}{u} \in \operatorname{Ker}(U^{-1}\varphi)$ 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 φ is 1-1 if and only if $\frac{r}{u} = 0$ in $U^{-1}R$.

(e) Since $\varphi : R \to S$ and $\alpha : S \to T$ 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 that $U^{-1}(\alpha \circ \varphi)$ and $\varphi(U)^{-1}\alpha$ are well-defined.

$$\begin{tikzcd}
U^{-1}R \arrow[drrr] \arrow[ddd] & & & \\
& \frac{r}{u} \arrow[r, mapsto] \arrow[d, mapsto] & \frac{\varphi(r)}{\varphi(u)} \arrow[d, mapsto] & \varphi(U)^{-1}S \arrow[ddl] \\
& \frac{(\alpha\circ\varphi)(r)}{(\alpha\circ\varphi)(u)} \arrow[r, equal] & \frac{\alpha(\varphi(r))}{\alpha(\varphi(u))} & \\
(\alpha \circ \varphi)(U)^{-1}T & & \alpha(\varphi(U))^{-1}T &
\end{tikzcd}$$

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 $\operatorname{Im}(U^{-1}\varphi) \cong U^{-1}\operatorname{Im}(\varphi)$ given by $\frac{\varphi(r)}{\varphi(u)} \mapsto \frac{i(\pi(r))}{i(\pi(u))} = \frac{\varphi(r)}{\varphi(u)}$.

Proof. We have that

$$\begin{tikzcd}
R \arrow[rr, "\psi"] \arrow[dr, "\pi"] \arrow[dd, "\varphi"'] & & U^{-1}R \arrow[dr, "U^{-1}\pi"] \arrow[dd, "U^{-1}\varphi"' near start] & \\
& \operatorname{Im}(\varphi) \arrow[rr] \arrow[dl, "i"] & & U^{-1}\operatorname{Im}(\varphi) \arrow[dl, "\pi(U)^{-1}i"] \\
S \arrow[rr] & & U^{-1}S &
\end{tikzcd}$$

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

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. $U^{-1}\mathfrak{a} = \{$equivalence classes from $U \times \mathfrak{a}$ 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 $i : U^{-1}\mathfrak{a} \to U^{-1}R$ given by $i(a/u) = a/u$ is a well-defined ring monomorphism. Identify $U^{-1}\mathfrak{a}$ with $\mathrm{Im}(i) \subseteq U^{-1}R$, 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 that $\frac{r}{u} = \frac{vr}{vu} \in U^{-1}\mathfrak{a}$ with $ur \in \mathfrak{a}$ and $vu \in U$.

(c) Let $\pi : R \to \frac{R}{\mathfrak{a}}$ be the natural surjection. Then $U^{-1}\mathfrak{a} = \mathrm{Ker}(U^{-1}\pi) \leq U^{-1}R$ 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 $\varphi : R \to S$ is a ring homomorphism, then $U^{-1}\mathrm{Ker}(\varphi) = \mathrm{Ker}(U^{-1}\varphi) \leq U^{-1}R$ such that $\mathrm{Im}(U^{-1}\varphi) \cong \frac{U^{-1}R}{U^{-1}\mathrm{Ker}(\varphi)}$.

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

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 $\frac{a}{u} \in \mathrm{Ker}(i)$ 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. $\Longrightarrow$ Assume $\frac{r}{u} \in U^{-1}\mathfrak{a}$. Then $\frac{r}{u} = \frac{a}{u'} \in U^{-1}R$ for some $a \in \mathfrak{a}$ and $u \in U$. Hence 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 $vr = u''u'r \in \mathfrak{a}$.

$\Longleftarrow$ 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 that $\frac{r}{u} \in U^{-1}\mathfrak{a}$ 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 that by Proposition 3.7, $\mathrm{Im}(U^{-1}\pi) \cong U^{-1}\mathrm{Im}(\pi) = U^{-1}\frac{R}{\mathfrak{a}}$ given by $\frac{\overline{r}}{\overline{u}} \mapsto \frac{\overline{r}}{\overline{u}}$. Then by (d), $U^{-1}\frac{R}{\mathfrak{a}} \cong \frac{U^{-1}R}{U^{-1}\mathrm{Ker}(\pi)} = \frac{U^{-1}R}{U^{-1}\mathfrak{a}}$ given by $\frac{\overline{r}}{\overline{u}} \leftarrow\!\shortmid \overline{\frac{r}{u}}$.

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

By the first isomorphism theorem, $\operatorname{Im}(U^{-1}\varphi) \cong \frac{U^{-1}R}{\operatorname{Ker}(U^{-1}\varphi)} = \frac{U^{-1}R}{U^{-1}\operatorname{Ker}(\varphi)}$ given by $\frac{\varphi(r)}{\varphi(u)} \leftarrow\!\shortmid \overline{\frac{r}{u}}$.

$$
\begin{tikzcd}
U^{-1}R \arrow[r] \arrow[dr, "U^{-1}\varphi"'] & \frac{U^{-1}R}{\operatorname{Ker}(U^{-1}\varphi)} \arrow[d, dashed] \\
& \operatorname{Im}(U^{-1}\varphi)
\end{tikzcd}
$$

(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 $\frac{a}{u} = \frac{a}{1} \cdot \frac{1}{u} = \psi(a)\frac{1}{u} \in \mathfrak{a} \cdot U^{-1}R$. $\square$

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) $U^{-1}\operatorname{rad}(\mathfrak{a}) = \operatorname{rad}(U^{-1}\mathfrak{a})$.

(e) $U^{-1}\operatorname{Nil}(R) = \operatorname{Nil}(U^{-1}R)$.

(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 that

$$U^{-1}(\mathfrak{a} + \mathfrak{b}) = (\mathfrak{a} + \mathfrak{b}) \cdot U^{-1}R = (\mathfrak{a} \cdot U^{-1}R) + (\mathfrak{b} \cdot U^{-1}R) = (U^{-1}\mathfrak{a}) + (U^{-1}\mathfrak{b}).$$

(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). Hence $(vw)r \in \mathfrak{a} \cap \mathfrak{b}$. 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 that

$$U^{-1}(\mathfrak{a}\mathfrak{b}) = (\mathfrak{a}\mathfrak{b}) \cdot U^{-1}R = (\mathfrak{a} \cdot U^{-1}R)(\mathfrak{b} \cdot U^{-1}R) = (U^{-1}\mathfrak{a})(U^{-1}\mathfrak{b}).$$

(d) $\subseteq$ By Proposition 3.11(e) and 1.63(g),

$$U^{-1}\operatorname{rad}(\mathfrak{a}) = \operatorname{rad}(\mathfrak{a}) \cdot U^{-1}R \subseteq \operatorname{rad}(\mathfrak{a} \cdot U^{-1}R) = \operatorname{rad}(U^{-1}\mathfrak{a}).$$

$\supseteq$ Let $\frac{r}{u} \in \operatorname{rad}(U^{-1}\mathfrak{a})$ 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 $n \geq 1$. Hence there exists $v \in U$ such that $vr^n \in \mathfrak{a}$ by Proposition 3.11(b). Hence $(vr)^n = v^{n-1} \cdot vr^n \in \mathfrak{a}$. Hence $vr \in \operatorname{rad}(\mathfrak{a})$. Thus, $\frac{r}{u} \in U^{-1}\operatorname{rad}(\mathfrak{a})$ 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, $\mathfrak{a} = \langle a_1, \ldots, a_n\rangle R$ for some $n \geq 1$ and $a_1, \ldots, a_n \in R$. Then $U^{-1}\mathfrak{a} = \langle \frac{a_1}{1}, \ldots, \frac{a_n}{1}\rangle U^{-1}R$. 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 $i = 1, \ldots, n$. Hence by Proposition 3.11(b), there exists $v_i \in U$ such that $v_i r a_i \in \mathfrak{b}$ for $i = 1, \ldots, n$. Let $v = v_1 \cdots v_n \in U$. Then $(vr)a_i \in \mathfrak{b}$ for $i = 1, \ldots, n$. Hence $vr \in (\mathfrak{b} : \mathfrak{a})$. Thus, $\frac{r}{u} \in U^{-1}(\mathfrak{b} : \mathfrak{a})$ by Proposition 3.11(b). □

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 ψ.

(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 that $\psi^{-1}(I) \leq R$. We claim that $I = U^{-1}(\psi^{-1}(I))$.

$\supseteq$ 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., $r \in \psi^{-1}(I)$. Hence $i = \frac{r}{u} \in U^{-1}(\psi^{-1}(I))$.

(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 that $U^{-1}\mathfrak{a} = U^{-1}R$ 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). □

Corollary 3.14. Let $\mathfrak{p} \in \operatorname{Spec}(R)$ 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 $\bar{r}/\bar{u} \leftarrow\!\shortmid \overline{r/u}$.

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

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

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. Hence by Corollary 3.14, $R_{\mathfrak{m}}/\mathfrak{m}_{\mathfrak{m}} \cong Q(R/\mathfrak{m}) = R/\mathfrak{m}$. □

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

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

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

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

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

Question. $U \cap \mathfrak{p} = \emptyset$ if and only if $U^{-1}\mathfrak{p} \in \operatorname{Spec}(U^{-1}R)$ 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. $\Longleftarrow$ follows from the definition.

$\Longrightarrow$ Assume $\frac{r}{u} \in U^{-1}\mathfrak{p}$. Then there exists $v \in U$ such that $vr \in \mathfrak{p} \in \operatorname{Spec}(R)$. Hence $v \in \mathfrak{p}$ or $r \in \mathfrak{p}$. Since $v \in U$ and $U \cap \mathfrak{p} = \emptyset$, we have that $v \notin \mathfrak{p}$. Hence $r \in \mathfrak{p}$. ☐

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

$$\begin{aligned} (U^{-1}R)_{U^{-1}\mathfrak{p}} &\xrightarrow{\cong} R_{\mathfrak{p}} \\ \frac{r/1}{s/1} &\longmapsfrom r/s \;\; s \in R \setminus \mathfrak{p} \end{aligned}$$

Proof. We have that

$$\begin{tikzcd}
r \arrow[rrr, mapsto] \arrow[ddd, mapsto] & & & \frac{r}{1} \arrow[ddd, mapsto] \\
& R \arrow[r] \arrow[d, "\psi"] \arrow[dr, "\beta"] & R_{\mathfrak{p}} \arrow[d, dashed, "\exists\varphi"] & \\
& U^{-1}R \arrow[r, "\alpha"] & (U^{-1}R)_{U^{-1}\mathfrak{p}} & \\
r/1 \arrow[rrr, mapsto] & & & \frac{r/1}{1/1}
\end{tikzcd}$$

Let $\beta = \alpha \circ \psi$. By proposition 3.5, to show φ 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 that $x/1 \notin U^{-1}\mathfrak{p}$ by Lemma 3.16. Hence $\frac{x}{1}$ 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 that $\varphi(r/s) = \beta(r)/\beta(s) = \frac{r/1}{s/1}$ for $\frac{r}{s} \in R_{\mathfrak{p}}$.

Let $\frac{r}{s} \in R_{\mathfrak{p}}$. Then $\frac{r}{s} \in \operatorname{Ker}(\varphi)$ 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). Hence φ 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. Hence $\frac{vr}{us} \in R_{\mathfrak{p}}$. 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 that φ is onto. ☐

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

Proof. Take $U = R \smallsetminus \mathfrak{q}$ in Proposition 3.17. □

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. Hence 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 $\mathfrak{p} := (0) \in \operatorname{Spec}(R)$. Hence $Q(U^{-1}R) = (U^{-1}R)_{U^{-1}(0)} \cong R_{(0)} = Q(R)$ by Proposition 3.17. In fact, the map $Q(U^{-1}R) \xleftarrow{\cong} Q(R)$ is given by $\frac{r/1}{s/1} \leftarrow\!\shortmid r/s$.

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

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

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

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

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

Example. (a) If R is an integral domain, then $\operatorname{NZD}(R) = R \smallsetminus \{0\}$ and $\mathrm{Q}(R) = \operatorname{NZD}(R)^{-1}(R) = (R \smallsetminus 0)^{-1}(R) = Q(R)$. Hence 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 $x = \overline{X}$, $y = \overline{Y}$, $z = \overline{Z}$ and $w = \overline{W}$. Since $\langle 0 \rangle R = \langle x, z\rangle \cap \langle y, w\rangle$ is a minimal primary decomposition, $\operatorname{Ass}_R(0) = \{\langle x,z\rangle, \langle y,w\rangle\}$. Hence $\operatorname{ZD}(R) = \bigcup_{\mathfrak{p} \in \operatorname{Ass}_R(0)} \mathfrak{p} = \langle x,z\rangle \cup \langle y,w\rangle$ by Corollary 4.34. Then $U := \operatorname{NZD}(R) = R \smallsetminus \{\langle x,z\rangle \cup \langle y,w\rangle\}$.

By prime correspondence for localization, $\operatorname{Spec}(\mathrm{Q}(R)) = \{U^{-1}\mathfrak{p} \mid \mathfrak{p} \in \operatorname{Spec}(R), \mathfrak{p} \cap U = \emptyset\} = \{U^{-1}\langle x,z\rangle, U^{-1}\langle y,w\rangle\}$. 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),

$$\mathfrak{p}_1 \cap \mathfrak{p}_2 = U^{-1}(\langle x,z\rangle \cap \langle y,w\rangle) = U^{-1}\langle xy, yz, zw, xw\rangle = 0.$$

Hence $\text{m-Spec}(U^{-1}R) = \{\mathfrak{p}_1, \mathfrak{p}_2\}$. Hence $\mathfrak{p}_1 + \mathfrak{p}_2 = U^{-1}R = \mathrm{Q}(R)$. Let $\pi_1 : R \to R/\langle x,z\rangle$ and $\pi_2 : R \to R/\langle y,w\rangle$ be natural surjections. Then by Chinese Remainder Theorem and Proposition 3.17 with $0 \notin \pi_1(R \smallsetminus \langle x,z\rangle \cup \langle y,w\rangle) = \pi_1(U)$ and $0 \notin \pi_2(U)$,

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

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

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

Assume $U \subseteq R$ is multiplicatively closed such that the natural ring homomorphism $\phi : R \to U^{-1}R$ 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 ϕ is 1-1, $r = 0$. Hence $u \in \mathrm{NZD}(R)$. $\square$

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

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

(b) What does $(\varphi^*)^{-1}(\mathfrak{p}) = \{\mathfrak{q} \in \operatorname{Spec}(S) \mid \varphi^*(\mathfrak{q}) = \mathfrak{p}\}$ look like? In general, if $f : Y \to X$ 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 $U = R \smallsetminus \mathfrak{p}$.

$$\begin{tikzcd}
R \arrow[r, "\varphi"] \arrow[d, "\psi"] & S \arrow[d, "\rho"] \\
U^{-1}R \arrow[r, "U^{-1}\varphi"] \arrow[d, "\tau"] & U^{-1}S \arrow[d, "\pi"] \\
Q(R/\mathfrak{p}) \cong \frac{R_\mathfrak{p}}{\mathfrak{p}_\mathfrak{p}} = \frac{U^{-1}R}{U^{-1}\mathfrak{p}U^{-1}R} \arrow[r, "\overline{\pi\circ U^{-1}\varphi}"] & \frac{U^{-1}S}{\mathfrak{p}\cdot U^{-1}S} := \frac{U^{-1}S}{\mathfrak{p}S\cdot U^{-1}S} := \frac{U^{-1}S}{U^{-1}\mathfrak{p}\cdot U^{-1}S} \arrow[d, equal] \\
& \mathcal{F}(\mathfrak{p}) = \frac{S_\mathfrak{p}}{\mathfrak{p}\cdot S_\mathfrak{p}} := \frac{\varphi(U)^{-1}S}{\varphi(U)^{-1}(\mathfrak{p}S)}
\end{tikzcd}$$

Note that $\mathfrak{p} \cdot U^{-1}S$ 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 ρ, 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. φ.

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 $\varphi(p) \subseteq \mathfrak{p}S$. Hence by Construction 1.13, $\overline{\pi \circ (U^{-1}\varphi)}$ is a well-defined ring homomorphism.

$$\begin{tikzcd}
U^{-1}R \arrow[r] \arrow[dr, "\pi\circ(U^{-1}\varphi)"'] & \frac{U^{-1}R}{U^{-1}\mathfrak{p}} \arrow[d, dashed, "\overline{\pi\circ(U^{-1}\varphi)}"] \\
& \mathcal{F}(\mathfrak{p}) = \frac{\varphi(U)^{-1}S}{\varphi(U)^{-1}(\mathfrak{p}S)}
\end{tikzcd}$$

$$\begin{tikzcd}
& R \arrow[rr, "\varphi"] \arrow[dl, "\psi"'] \arrow[dd] & & S \arrow[dl, "\rho"] \arrow[dd, "\epsilon"] \\
U^{-1}R \arrow[rr, "U^{-1}\varphi"] \arrow[dd, "\tau"] & & U^{-1}S \arrow[dd, "\pi"] & \\
& \frac{R}{\mathfrak{p}} \arrow[rr, "\overline{\epsilon\circ\varphi}"] \arrow[dl, "\overline{\tau\circ\psi}"'] & & \frac{S}{\mathfrak{p}S} \arrow[dl, "\overline{\pi\circ\rho}"] \\
\frac{U^{-1}R}{U^{-1}\mathfrak{p}} \arrow[rr, "\overline{\pi\circ(U^{-1}\varphi)}"] & & \frac{\varphi(U)^{-1}S}{\varphi(U)^{-1}(\mathfrak{p}S)} &
\end{tikzcd}$$

Let $\bar{r} \in \frac{R}{\mathfrak{p}}$ with $r \in R$. Then

$$\overline{\pi \circ (U^{-1}\varphi)} \circ (\overline{\tau \circ \psi})(\bar{r}) = \overline{\pi \circ (U^{-1}\varphi)}(\tau \circ \psi(r)) = \overline{\pi \circ (U^{-1}\varphi)}\left(\frac{\overline{r}}{1}\right) = \pi \circ (U^{-1}\varphi)\left(\frac{r}{1}\right) = \frac{\overline{\varphi(r)}}{\varphi(1)} = \frac{\overline{\varphi(r)}}{1}$$

and

$$\overline{\pi \circ \rho} \circ \overline{\epsilon \circ \varphi}(\bar{r}) = \overline{\pi \circ \rho}(\epsilon \circ \rho)(r) = \overline{\pi \circ \rho}(\overline{\phi(r)}) = \pi \circ \rho(\phi(r)) = \overline{\frac{\varphi(1)}{1}}.$$

Hence the diagram on the bottom also commutes.

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

(i) $\mathfrak{p} \in \operatorname{Im}(\varphi^*)$, 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 $\theta : \operatorname{Spec}(\mathcal{F}(\mathfrak{p})) \to (\varphi^*)^{-1}(\mathfrak{p}) \subseteq \operatorname{Spec}(S)$ 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. $\varphi^* : \operatorname{Spec}(S) \to \operatorname{Spec}(R)$.

$$\begin{tikzcd}
R \arrow[r, "\varphi"] \arrow[d, "\psi"] & S \arrow[d, "\rho"] \\
U^{-1}R \arrow[r] \arrow[d, "\tau"] & U^{-1}S \arrow[d, "\pi"] \\
\frac{U^{-1}R}{\mathfrak{p} \cdot U^{-1}R} \arrow[r] & \frac{U^{-1}S}{\mathfrak{p} \cdot U^{-1}S}
\end{tikzcd}$$

Proof. (i)$\Longrightarrow$(ii) Assume there is $\mathfrak{q} \in \operatorname{Spec}(S)$ 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)$\Longrightarrow$(iii). Assume $\mathfrak{p} = \varphi^{-1}(\mathfrak{p}S)$. Note that

$$\mathfrak{p} \cdot U^{-1}S = \mathfrak{p}S \cdot U^{-1}S = \mathfrak{p}S \cdot \varphi(U)^{-1}S = \varphi(U)^{-1}(\mathfrak{p}S).$$

To show that $\varphi(U)^{-1}(\mathfrak{p}S) \neq \varphi(U)^{-1}S$, it is equivalent to show that $\mathfrak{p}S \cap \varphi(U) = \emptyset$ 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)$\Longrightarrow$(i) and well-definedness of θ: It suffices to show that $\varphi^*(\theta(Q)) = \mathfrak{p}$ for $Q \in \operatorname{Spec}(\frac{U^{-1}S}{\mathfrak{p} \cdot U^{-1}S})$, i.e., $\varphi^{-1}(\rho^{-1}(\pi^{-1}(Q))) = \mathfrak{p}$. Let $\mathfrak{q} := \pi^{-1}(Q) \in \operatorname{Spec}(U^{-1}S)$. Then by prime correspondence for quotients, we have that $\mathfrak{p} \cdot U^{-1}S \subseteq \pi^{-1}(Q) = \mathfrak{q}$ and $Q = \frac{\mathfrak{q}}{\mathfrak{p} \cdot U^{-1}S}$. Since $\mathfrak{q} \in \operatorname{Spec}(U^{-1}S)$, by prime correspondence for localization $\operatorname{Spec}(U^{-1}S) \xrightarrow{\rho^{-1}} \operatorname{Spec}(S)$, for $\mathfrak{r} := \rho^{-1}(\mathfrak{q}) = \rho^{-1}(\pi^{-1}(Q)) \in \operatorname{Spec}(S)$ with $\mathfrak{r} \cap \varphi(U) = \emptyset$, we have that

$$\mathfrak{q} = \mathfrak{r} \cdot U^{-1}S = \mathfrak{r} \cdot \varphi(U)^{-1}S = \varphi(U)^{-1}\mathfrak{r}.$$

Hence 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 $x \in R \setminus \mathfrak{p} = U$. Hence $\varphi(x) \in \mathfrak{r} \cap \varphi(U) = \emptyset$, a contradiction. Thus, $\mathfrak{p} = \varphi^{-1}(\mathfrak{r}) = \varphi^{-1}(\rho^{-1}(\pi^{-1}(Q)))$.

By prime correspondence for quotients, π^* is 1-1 and by prime correspondence for localization, ρ^* is 1-1. Since

$$\theta : \operatorname{Spec}(\mathcal{F}(\mathfrak{p})) \xrightarrow{\pi^*} \operatorname{V}(\mathfrak{p} \cdot U^{-1}S) \xrightarrow{\rho^*|_{\text{restriction}}} (\varphi^*)^{-1}(\mathfrak{p}),$$

we have that θ is the restriction of $\rho^* \circ \pi^*$. Hence θ is 1-1.

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

$$\theta\left(\frac{\mathfrak{q} \cdot U^{-1}S}{\mathfrak{p}U^{-1}S}\right) = \rho^{-1}\left(\pi^{-1}(\frac{\mathfrak{q} \cdot U^{-1}S}{\mathfrak{p}U^{-1}S})\right) = \rho^{-1}(\mathfrak{q} \cdot U^{-1}S) = \mathfrak{q}.$$

Thus, θ is onto. □

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 that $U := R \smallsetminus \mathfrak{m} = R^\times$ by Proposition 1.22. Hence $U^{-1}(-) \cong -$, e.g., $\mathcal{F}(\mathfrak{m}) = \frac{U^{-1}S}{\mathfrak{m} \cdot U^{-1}S} \cong \frac{S}{\mathfrak{m} \cdot S}$. □

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 φ (fibre over unique closed point of $\operatorname{Spec}(R)$).

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

Example 3.27. (a) Let $\varphi : R \overset{\subseteq}{\hookrightarrow} R[X_1, \ldots, R_d]$.

(1) If $(R, \mathfrak{m})$ is local, then

$$\mathcal{F}(\mathfrak{m}) \cong \frac{R[X_1, \ldots, X_d]}{\mathfrak{m} \cdot R[X_1, \ldots, X_d]} = \frac{R[X_1, \ldots, X_d]}{\mathfrak{m}[X_1, \ldots, X_d]} \cong \frac{R}{\mathfrak{m}}[X_1, \ldots, X_d].$$

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

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

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 $R \overset{\subseteq}{\hookrightarrow} R[\![X_1, \ldots, X_d]\!]$.

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

(c) Let k be a field and $\varphi : k[X_1, \ldots, X_d] \overset{\subseteq}{\hookrightarrow} k[\![X_1, \ldots, X_d]\!]$.

(1) Let $\mathfrak{m} = \langle X_1, \ldots, X_d \rangle = k[X_1, \ldots, X_d]$ be maximal. Then $\mathfrak{m} \cdot k[\![X_1, \ldots, X_d]\!] = \langle X_1, \ldots, X_d \rangle \leq k[\![X_1, \ldots, X_d]\!]$. Hence with $U = k[X_1, \ldots, X_d] \smallsetminus \mathfrak{m}$,

$$\mathcal{F}(\mathfrak{m}) = \frac{U^{-1}(k[\![X_1, \ldots, X_d]\!])}{\mathfrak{m} \cdot U^{-1}(k[\![X_1, \ldots, X_d]\!])} \cong \frac{k[\![X_1, \ldots, X_d]\!]}{\mathfrak{m} \cdot k[\![X_1, \ldots, X_d]\!]} \cong \frac{k[\![X_1, \ldots, X_d]\!]}{\langle X_1, \ldots, X_d \rangle} \cong k$$

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 weired, 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".
Aternative versions for non-UFD's.

(a) Irreducible factorizations:

Pros	Cons
familiar	don't necessarily exist

.

(b) Primary decompositions:

Pros	Cons
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 $a \in R \smallsetminus \{R^\times \cup 0\}$.*

(a) a has an irreducible factor in R.

(b) There exist irreducible $b_1, \ldots, b_n \in R$ 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, Σ has a maximal element, say $\langle b \rangle$. We claim that $\langle b \rangle$ is irreducible. Since $a \neq 0$ and $b \mid a$, we have that $b \neq 0$. Since $\langle b \rangle \neq R$, $b \notin R^\times$. Suppose $b = cd$ for some $c \in R \smallsetminus R^\times$ and $d \in R$. Since $c \mid b \mid a$, we have that $c \mid a$. 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 Σ, we have that $\langle cd \rangle = \langle b \rangle = \langle c \rangle$. Also, since R is an integral domain, $d \in R^\times$. Hence 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 that $\langle a \rangle \subsetneq \langle a_1 \rangle \subsetneq \langle a_2 \rangle$. 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 $\mathfrak{m} = \langle X^{\mathbb{R}_{>0}}\rangle \lneq A$. Then $\mathfrak{m} \in \text{m-Spec}(R)$ and $A/\mathfrak{m} \cong k$. Let $R = A_{\mathfrak{m}}$. Then $A \smallsetminus \mathfrak{m} \subseteq R^\times$. Since X has no irreducible factors in R, X has no irreducible factorization. Let $r \in R \smallsetminus \{R^\times \cup 0\}$. Then $r = X^\epsilon \cdot f$ for some $\epsilon > 0$ and $f \in R \smallsetminus \{0\}$. Since $X^\epsilon \cdot f = X^{\frac{\epsilon}{2}} \cdot X^{\frac{\epsilon}{2}} \cdot f$. Hence r is not irreducible in R. Thus, R has no irreducible elements.

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

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, $IJ = J = \langle x_1, \ldots, x_n\rangle$ for some $x_1, \ldots, x_n \in J$. Hence $x_n \in IJ$ and then $x_n = \sum_{i=1}^n a_i x_i$ for some $a_1, \ldots, a_n \in I$, 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. Hence $x_n \in \langle x_1, \ldots, x_{n-1}\rangle$, contradicting minimality of n. Hence $n = 1$ or 0. If $n = 1$, similarly, we have that $x_1(1 - a_1) = 0$ for some $a_1 \in I$ with $1 - a_1 \in R^\times$, so $x_1 = 0$, a contradiction. Thus, $n = 0$. □

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 that $\langle c\rangle = \langle b\rangle = \langle cd\rangle = \langle d\rangle\langle c\rangle$. Suppose $d \notin R^\times$. Then $\langle d\rangle \subseteq \mathfrak{m} = \text{Jac}(R)$. Hence by Lemma 4.5, $c = 0$. Hence $b = cd = 0$, a contradiction. Thus, $d \in R^\times$. □

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

(a) a has an irreducible factor in R.

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

Proof. It is similar to the proof of Theorem 4.2. □

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

Example 4.9. Let

$$R = \frac{k[X,Y,Z]_{(X,Y,Z)}}{(X^2 - YZ)} \cong \frac{k[X,Y,Z]_{(X,Y,Z)}}{(X^2 - YZ)_{(X,Y,Z)}} \cong \left(\frac{k[X,Y,Z]}{(X^2 - YZ)}\right)_{(X,Y,Z)}$$

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. Hence R is a local, noetherian and integral domain. Let $x = \overline{X} \in R$, which is irreducible. Let $y = \overline{Y}, z = \overline{Z} \in R$. Since $(x,z) \in \text{V}(x) \smallsetminus \text{V}(y)$ and $(x,y) \in \text{V}(x) \smallsetminus \text{V}(z)$, $\text{V}(x) \neq \text{V}(y)$ and $\text{V}(x) \neq \text{V}(z)$. Also, since $\text{V}(x) = \text{V}(x^2) = \text{V}(yz) = \text{V}(y) \cup \text{V}(z)$, we have that $\text{V}(x)$ is not irreducible in $\text{Spec}(R)$.

Primary decomposition does the job.

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

Example 4.11. We have the following examples.

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

(b) If $\mathfrak{m} \in \operatorname{Spec}(R)$ 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 $y \notin \operatorname{rad}(\mathfrak{q})$. Since $\operatorname{rad}(\mathfrak{m}) = \operatorname{rad}(\mathfrak{m}^n) \subseteq \operatorname{rad}(\mathfrak{q}) \subseteq \operatorname{rad}(\mathfrak{m})$, we have that $\operatorname{rad}(\mathfrak{q}) = \operatorname{rad}(\mathfrak{m}) = \mathfrak{m} \in \text{m-Spec}(R)$. Hence $\langle y, \mathfrak{m}\rangle = R$. As in Proposition 1.46(b), we can show $\langle y, \mathfrak{m}^n\rangle = R$ by Proposition 1.39(a). Hence $1 = zy + \alpha$ 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 $\mathfrak{q} \lneq R$ such that $\operatorname{rad}(\mathfrak{q}) = \mathfrak{m} \in \text{m-Spec}(R)$, then $\mathfrak{q}$ is primary.

Alternating proof of (b). Let $\overline{x}, \overline{y} \in \overline{R} := R/\mathfrak{q}$ such that $\overline{x}\overline{y} = 0$. Let $\mathfrak{p}/\mathfrak{q} \in \operatorname{Spec}(\overline{R})$ with $\mathfrak{p} \in \operatorname{Spec}(R)$ such that $\mathfrak{p} \supseteq \mathfrak{q} \supseteq \mathfrak{m}^n$. Then

$$R \supsetneq \mathfrak{p} = \operatorname{rad}(\mathfrak{p}) \supseteq \operatorname{rad}(\mathfrak{q}) \supseteq \operatorname{rad}(\mathfrak{m}^n) = \mathfrak{m} \in \operatorname{Spec}(R).$$

Hence $\mathfrak{p} = \mathfrak{m}$. Hence $\operatorname{Spec}(\overline{R}) = \{\mathfrak{m}/\mathfrak{q}\}$. Hence $(\overline{R}, \mathfrak{m}/\mathfrak{q})$ is local. If $\overline{y} \in \mathfrak{m}/\mathfrak{q} = \operatorname{Nil}(R/\mathfrak{q})$ by Proposition 1.26(d), done. Assume now $\overline{y} \notin \operatorname{Nil}(R/\mathfrak{q}) = \mathfrak{m}/\mathfrak{q}$. Then $\overline{y} \in \overline{R}^\times$ by Proposition 1.22. Also, since $\overline{x}\overline{y} = 0$ in $\overline{R}$, $\overline{x} = 0$.

(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 $x = \overline{X} \in R$. Then x is irreducible. Note that

$$R/\langle x\rangle = \frac{k[\![X,Y,Z]\!]}{\langle X^2 - YZ\rangle}/\langle x\rangle \cong \frac{k[\![X,Y,Z]\!]}{\langle X, X^2 - YZ\rangle} = \frac{k[\![X,Y,Z]\!]}{\langle X, YZ\rangle} \cong \frac{k[\![Y,Z]\!]}{\langle YZ\rangle}.$$

Let $y = \overline{Y}, z = \overline{Z} \in \frac{k[\![Y,Z]\!]}{\langle YZ\rangle}$. Then $yz = 0$ with $y, z \neq 0$. Hence $y, z \notin (0) = \operatorname{rad}(0) = \operatorname{Nil}(R/\langle x\rangle)$. Thus, $\langle x\rangle$ is not primary.

(c) Let $R = k[X_1, \ldots, X_d]$. Then $I = \langle X_{i_1}^{e_1}, \cdots, X_{i_n}^{e_n}\rangle$ with $e_1, \ldots, e_n \geq 1$ is primary.

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

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

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

Proof. (a) Let $xy \in \langle p^n \rangle$ with $x, y \in R$. If $y \in \operatorname{rad}(\langle p^n \rangle) = \langle p \rangle$, 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 $s \geq 1$, $a_i \in R \smallsetminus \{0\}$ and $f_i \in R$ monomial for $i = 1, \dots, s$ and $g = \sum_{i=1}^{t} b_i g_i$ for some $t \geq 1$, $b_i \in R \smallsetminus \{0\}$ 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, asssume f_s is the largest monomial occuring in $\tilde{f}$ and g_t is the largest monomial occuring in g. Then $f_s g_t$ is the largest monomial occuring in $\tilde{f}g \in I$. Hence $f_s g_t \in I$. Since the monomial $f_s \notin I$, $X_i^{e_i} \nmid f_s$ for $i = 1, \dots, n$. Hence g_t is not a constant in R and hence $X_j \mid g_t$ for some $j \in \{1, \dots, n\}$. Then $g_t \in \langle X_1, \dots, X_n \rangle = \operatorname{rad}(\langle X_1^{e_1}, \dots, X_n^{e_n} \rangle) = \operatorname{rad}(I)$. Hence $g = \sum_{i=1}^{t-1} b_i g_i + b_t g_t$ with $b_t g_t \in \operatorname{rad}(I)$. Induct on t, we have that $b_i g_i \in \operatorname{rad}(I)$ for all $i = 1, \dots, t$. Thus, $g \in \operatorname{rad}(I)$. □

Let $\mathfrak{a} \lneq R$ for the rest of this section.

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 $\mathfrak{p} \in \operatorname{Spec}(R)$, then $\mathfrak{p}$ is irreducible.

(b) If $\mathfrak{a}$ is primary in R, then $\mathfrak{q}$ 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 $\mathfrak{p} \in \operatorname{Spec}(R)$, $\mathfrak{p} \supseteq I$ or $\mathfrak{p} \supseteq J$. Hence $I \supseteq I \cap J = \mathfrak{p} \supseteq I$ 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 $\operatorname{rad}(\mathfrak{a}) = \langle X, Y \rangle \in \operatorname{m-Spec}(R)$, but $\mathfrak{a}$ is not irreducible since $\mathfrak{a} = \langle X, Y^2 \rangle \cap \langle X^2, Y \rangle$. □

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 that $(0 : y) \subseteq (0 : y^2) \subseteq (0 : y^3) \subseteq \cdots$. 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 $xs = z = y^n t$ for some $s \in R$ and $t \in R$. Hence $y^{n+1} t = xys = 0$, i.e., $t \in (0 : y^{n+1}) = (0 : y^n)$. Hence $z = y^n t = 0$. Hence $\langle x \rangle \cap \langle y^n \rangle = 0 = \mathfrak{a}$. Also, since $\mathfrak{a}$ is irreducible and $\langle x \rangle \neq 0$, we have that $\langle y^n \rangle = 0$, i.e., $y^n = 0$. Hence $y \in \operatorname{rad}(0) = \operatorname{rad}(\mathfrak{a})$. 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 $(0) \lneq R/\mathfrak{a}$ 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 $\mathfrak{a} \leq \tilde{I}, \tilde{J} \leq R$ ($\mathfrak{a} \leq \tilde{I} \cap \tilde{J}$). Hence $\tilde{I} \cap \tilde{J} = \mathfrak{a}$. Also, since $\mathfrak{a}$ is irreducible, $\tilde{I} = \mathfrak{a}$ or $\tilde{J} = \mathfrak{a}$. Hence $I = \frac{\tilde{I}}{\mathfrak{a}} = 0$ or $J = \frac{\tilde{J}}{\mathfrak{a}} = 0$. □

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 $\Sigma = \{\mathfrak{b} \lneq R \mid \mathfrak{b}$ does not have a irreducible decomposition$\}$. Since $\mathfrak{a} \in \Sigma$, $\Sigma \neq \emptyset$. Since R is noetherian, Σ 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 that $I, J \notin \Sigma$. Hence there exists $m \geq n \geq 1$ and irreducible $J_1, \dots, J_m \lneq R$ such that $I = \bigcap_{i=1}^n J_i$ and $J = \bigcap_{i=n+1}^m J_i$. Thus, $\mathfrak{q} = I \cap J = \bigcap_{i=1}^m J_i$, contradicting $\mathfrak{q} \in \Sigma$. ☐

Example 4.18. We have the following examples.

(a) Let R be a UFD and $a \in R \smallsetminus \{R^\times \cup 0\}$ has a prime factorization $a = up_1^{e_1} \cdots p_n^{e_n}$ 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. Hence $\mathfrak{a} = \bigcap_{i=1}^n J_i$ 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 $\operatorname{rad}(J_i) = \operatorname{rad}(J_j)$ for $1 \leq i, j \leq n$.

Proof. (c) $\Longleftarrow$ Assume that $\operatorname{rad}(J_i) = \operatorname{rad}(J_j)$ for $1 \leq i, j \leq n$. Let $xy \in \mathfrak{a}$ with $x, y \in R$. If $y \in \operatorname{rad}(\mathfrak{a})$, done. Assume that

$$y \notin \operatorname{rad}(\mathfrak{a})^{\dagger} = \operatorname{rad}\left(\bigcap_{i=1}^n J_i\right) = \bigcap_{i=1}^n \operatorname{rad}(J_i) = \operatorname{rad}(J_i)$$

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 that $x \in J_i$ for $i = 1, \dots, n$. Hence $x \in \bigcap_{i=1}^n J_i = \mathfrak{a}$.

$\Longrightarrow$ Assume that $\mathfrak{a}$ is primary. Induct on n. The base case $n = 2$ is the important case. Suppose $\operatorname{rad}(J_1) \neq \operatorname{rad}(J_2)$. Then we have that there exist $a \in \operatorname{rad}(J_1) \smallsetminus \operatorname{rad}(J_2)$ and $b \in \operatorname{rad}(J_2) \smallsetminus \operatorname{rad}(J_1)$. Hence $a, b \notin \operatorname{rad}(J_1) \cap \operatorname{rad}(J_2) = \operatorname{rad}(J_1 \cap J_2) = \operatorname{rad}(\mathfrak{a})$ and $ab \in \operatorname{rad}(J_1) \cap \operatorname{rad}(J_2) = \operatorname{rad}(\mathfrak{a})$, contradicting $\operatorname{rad}(\mathfrak{a}) \in \operatorname{Spec}(R)$ by Proposition 4.19. ☐

Proposition 4.19. If $\mathfrak{q} \lneq R$ is primary, then $\operatorname{rad}(\mathfrak{q}) \in \operatorname{Spec}(R)$. In particular, $\operatorname{rad}(\mathfrak{q})$ is the unique smallest prime ideal of R containing $\mathfrak{q}$.

Proof. Since $\mathfrak{q} \leq R$, $\operatorname{rad}(\mathfrak{q}) \lneq R$. Let $xy \in \operatorname{rad}(\mathfrak{q})$ 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 $y^m \in \operatorname{rad}(\mathfrak{q})$. Hence $x \in \operatorname{rad}(\mathfrak{q})$ or $y \in \operatorname{rad}(\operatorname{rad}(\mathfrak{q})) = \operatorname{rad}(\mathfrak{q})$ by Fact 1.58(c). Hence $\operatorname{rad}(\mathfrak{q}) \in \operatorname{Spec}(R)$. The minimality follows from the definition of prime ideal and equivalent definition of primary ideal. ☐

Definition 4.20. If $\mathfrak{q} \lneq R$ is primary and $\mathfrak{p} = \operatorname{rad}(\mathfrak{q})$, 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 $\operatorname{rad}(\mathfrak{q}) = \langle p \rangle \in \operatorname{Spec}(\mathbb{Z})$ 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 $\operatorname{rad}(\mathfrak{q}) = \mathfrak{m} \in \operatorname{Spec}(R)$ by the proof of Example 4.11(b).

†Not try to assume $x \notin \mathfrak{a}$.

(c) Let $R = k[X_1, \ldots, X_d]$ and $\mathfrak{q} = \langle X_{i_1}^{e_1}, \ldots, X_{i_n}^{e_n} \rangle$ with $e_1, \cdots, e_n \geq 1$. Then $\mathfrak{q}$ is primary with $\mathrm{rad}(\mathfrak{q}) = \langle X_{i_1}, \ldots, X_{i_n} \rangle \in \mathrm{Spec}(R)$.

Proposition 4.22. Let $\mathfrak{q}_1, \ldots, \mathfrak{q}_n \lneq R$ 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). □

Definition 4.23. A primary decomposition $\mathfrak{a} = \bigcap_{i=1}^n \mathfrak{q}_i$ is *minimal* if

(a) $\mathrm{rad}(\mathfrak{q}_i) \neq \mathrm{rad}(\mathfrak{q}_j)$ 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 $j = 1, \ldots, n$.

Example 4.24. (a) Let $n \in \mathbb{Z}$ and $n = p_1^{e_1} \cdots p_m^{e_m}$ such that $p_1, \ldots, p_m$ are distinct primes and $e_1, \ldots, e_m \geq 1$. 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 $\mathrm{rad}(\mathfrak{q}_i) = \mathfrak{p}_i$ for $i = 1, \ldots, n$.

(a) The *associated primes* of $\mathfrak{a}$ are $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$. Write it as

$$\mathrm{Ass}_R(\mathfrak{a}) = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}.$$

(b) The *minimal (associated) primes* of $\mathfrak{a}$ are the minimal elements of $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$ w.r.t. $\subseteq$. Write it as

$$\mathrm{Min}(\mathfrak{a}) = \min\{\mathrm{Ass}_R(\mathfrak{a}))\} = \min\{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}.$$

(c) The *embedded primes* of $\mathfrak{a}$ are the non-minimal associated primes of $\mathfrak{a}$, i.e., $\mathrm{Ass}_R(\mathfrak{a}) \smallsetminus \mathrm{Min}(\mathfrak{a})$.

Example 4.26. Let $R = k[X, Y]$ and $\mathfrak{a} = \langle X^2, XY \rangle$. Then $\mathrm{Ass}_R(\mathfrak{a}) = \{\langle X \rangle, \langle X, Y \rangle\}$, $\mathrm{Min}(\mathfrak{a}) = \{\langle X \rangle\}$ and the embedded prime(s) of $\mathfrak{a}$ is $\{\langle X, Y \rangle\}$.

Goals: $\mathrm{Ass}_R(\mathfrak{a})$ is independent of the minimal primary decomposition, so $\mathrm{Min}(\mathfrak{a})$ is also independent of the minimal primary decomposition. $\mathrm{Ass}_R(\mathfrak{a}) = \mathrm{Ass}_R(R/\mathfrak{a})$[†] 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 $\mathrm{rad}(\mathfrak{q}_i) = \mathrm{rad}(\mathfrak{q}_j)$ for some $i, j \in \{1, \ldots, n\}$ with $i \neq j$, then $\mathfrak{q}_i \cap \mathfrak{q}_j$ is $\mathfrak{p}$-primary where $\mathfrak{p} := \mathrm{rad}(\mathfrak{q}_i)$ 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 that $\mathfrak{p}_i = \mathrm{rad}(\mathfrak{q}_i) \neq \mathrm{rad}(\mathfrak{q}_j) = \mathfrak{p}_j$ 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 $j \in \{1, \ldots, n\}$, 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. □

[†]By definition of *associated prime* from module theory, $\mathrm{Ass}_R(R/\mathfrak{a}) = \mathrm{Spec}(R) \cap \{\mathrm{Ann}_R(\bar{x}) \mid \bar{x} \in R/\mathfrak{a}\}$.

Let $\mathfrak{a} = \bigcap_{i=1}^n \mathfrak{q}_i$ be a minimal primary decomposition such that $\mathrm{rad}(\mathfrak{q}_i) = \mathfrak{p}_i$ for $i = 1, \ldots, n$.

Proposition 4.28. Re-order the $\mathfrak{q}_i$'s if necessary to assume without loss of generality, $\mathrm{Min}(\mathfrak{a}) = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_m\}$. Then the irreducible components of $\mathrm{V}(\mathfrak{a})$ with subspace topology are $\mathrm{V}(\mathfrak{p}_1), \ldots, \mathrm{V}(\mathfrak{p}_m)$.

Proof. We claim that $\mathrm{Min}(\mathrm{V}(\mathfrak{a})) = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_m\}$. Then $\mathrm{V}(\mathfrak{p}_1), \ldots, \mathrm{V}(\mathfrak{p}_m)$ are all maximal irreducible subset of $\mathrm{V}(\mathfrak{a})$ by Proposition 2.42.

"$\subseteq$". Let $\mathfrak{p} \in \mathrm{Min}(\mathrm{V}(\mathfrak{a}))$. Then $\mathfrak{p} \supseteq \mathfrak{a} = \bigcap_{i=1}^n \mathfrak{q}_i$. Hence $\mathfrak{p} \supseteq \mathrm{rad}(\mathfrak{a}) = \mathrm{rad}(\bigcap_{i=1}^n \mathfrak{q}_i) = \bigcap_{i=1}^n \mathrm{rad}(\mathfrak{q}_i) = \bigcap_{i=1}^n \mathfrak{p}_i = \bigcap_{j=1}^m \mathfrak{p}_j$ since there exists $j_i \in \{1, \ldots, m\}$ such that $\mathfrak{p}_{j_i} \subseteq \mathfrak{p}_i$ for $i = m+1, \ldots, n$. Since $\mathfrak{p} \in \mathrm{Spec}(R)$, $\mathfrak{p} \supseteq \mathfrak{p}_k \supseteq \bigcap_{j=1}^m \mathfrak{p}_j = \mathrm{rad}(\mathfrak{a}) \supseteq \mathfrak{a}$ for some $k \in \{1, \ldots, m\}$. Also, since $\mathfrak{p}_k \in \mathrm{Spec}(R)$ by Proposition 4.19 and $\mathfrak{p} \in \mathrm{Min}(\mathrm{V}(\mathfrak{a}))$, we have that $\mathfrak{p} = \mathfrak{p}_k$.

"$\supseteq$". Fix $j \in \{1, \ldots, m\}$. Suppose there exists $\mathfrak{p} \in \mathrm{Spec}(R)$ such that $\mathfrak{a} \subseteq \mathfrak{p} \subsetneq \mathfrak{p}_j$. Then $\mathfrak{a}R_{\mathfrak{p}_j} \subseteq \mathfrak{p}R_{\mathfrak{p}_j} \subsetneq \mathfrak{p}_j R_{\mathfrak{p}_j}$ by prime correspondence for localization. For $i = 1, \ldots, m$ with $i \neq j$, since $\mathfrak{p}_i \not\subseteq \mathfrak{p}_j$, we have that $\mathfrak{p}_i \cap (R \setminus \mathfrak{p}_j) \neq \emptyset$ and then $\mathfrak{p}_i R_{\mathfrak{p}_j} = R_{\mathfrak{p}_j}$ by Proposition 3.13(c). Hence we have that

$$\begin{aligned} \mathfrak{a}R_{\mathfrak{p}_j} &= (R \setminus \mathfrak{p}_j)^{-1}\mathfrak{a} = (R \setminus \mathfrak{p}_j)^{-1}\left(\bigcap_{i=1}^m \mathfrak{p}_i\right) = \bigcap_{i=1}^m (R \setminus \mathfrak{p}_j)^{-1}\mathfrak{p}_i \\ &= \bigcap_{i=1}^m \mathfrak{p}_i R_{\mathfrak{p}_j} = \left(\bigcap_{i=1, i\neq j}^m R_{\mathfrak{p}_j}\right) \bigcap \mathfrak{p}_j R_{\mathfrak{p}_j} = \mathfrak{p}_j R_{\mathfrak{p}_j} \end{aligned}$$

by Proposition 3.12(a), a contradiction. Thus, $\mathfrak{p}_j \in \mathrm{Min}(\mathrm{V}(\mathfrak{a}))$. ◻

Proposition 4.29. Let $\mathfrak{q} \lneq R$ be $\mathfrak{p}$-primary and $x \in R$. Then

$$(\mathfrak{q} : x) = \begin{cases} R & \text{if } x \in \mathfrak{q} \\ \mathfrak{q} & \text{if } x \notin \mathfrak{p} \\ \mathfrak{p}\text{-primary} & \text{if } x \notin \mathfrak{q} \end{cases}.$$

Proof. If $x \in \mathfrak{q}$, then $1 \in (\mathfrak{q} : x)$, so $(\mathfrak{q} : x) = R$.

Assume $x \notin \mathfrak{p} = \mathrm{rad}(\mathfrak{q})$. Note that $(\mathfrak{q} : x) \supseteq \mathfrak{q}$ 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 $x \in \mathrm{rad}(\mathfrak{q})$. 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 $y \in \mathrm{rad}(\mathfrak{q}) = \mathfrak{p}$. Hence by assumption, $y \in \mathfrak{p}$. Then $\mathfrak{q} \subseteq (\mathfrak{q} : x) \subseteq \mathfrak{p}$. Hence $\mathfrak{p} = \mathrm{rad}(\mathfrak{q}) \subseteq \mathrm{rad}(\mathfrak{q} : x) \subseteq \mathrm{rad}(\mathfrak{p}) = \mathfrak{p}$. Hence $\mathrm{rad}(\mathfrak{q} : x) = \mathfrak{p}$. Next, let $ab \in (\mathfrak{q} : x)$ with $a, b \in R$. If $b \in \mathrm{rad}(\mathfrak{q} : x)$, then $(\mathfrak{q} : x)$ is $\mathfrak{p}$-primary, done. Assume $b \notin \mathrm{rad}(\mathfrak{q} : x) = \mathfrak{p} = \mathrm{rad}(\mathfrak{q})$. Since $ab \in (\mathfrak{q} : x)$, $ax \cdot b = abx \in \mathfrak{q}$. Also, since $\mathfrak{q}$ is primary and $b \notin \mathrm{rad}(\mathfrak{q})$, $ax \in \mathfrak{q}$, i.e., $a \in (\mathfrak{q} : x)$. Thus, $(\mathfrak{q} : x)$ is $\mathfrak{p}$-primary. ◻

Proposition 4.30.

$$\mathrm{Ass}_R(\mathfrak{a}) := \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\} = \mathrm{Spec}(R) \cap \{\mathrm{rad}(\mathfrak{a} : x) \mid x \in R\}^{\dagger}.$$

Hence $\mathrm{Ass}_R(\mathfrak{a})$ is independent of the minimal primary decomposition.

$^{\dagger}\mathrm{Ass}_R(\mathfrak{a}) = \mathrm{Spec}(R) \cap \{\mathrm{rad}(\mathfrak{a} : x) \mid x \notin \mathfrak{a}\}$.

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). Hence $\mathrm{rad}(\mathfrak{a} : x) = \mathrm{rad}(\bigcap_{i=1}^n (\mathfrak{q}_i : x)) = \bigcap_{i=1}^n \mathrm{rad}(\mathfrak{q}_i : x) = \bigcap_{i=1, x\notin \mathfrak{q}_i}^n \mathfrak{p}_i$ by Proposition 4.29, where the intersection of empty ideals is the R.

"$\supseteq$". Let $\mathfrak{p} \in \mathrm{Spec}(R) \cap \{\mathrm{rad}(\mathfrak{a} : x) \mid x \in R\}$. Then $\mathfrak{p} \in \mathrm{Spec}(R)$ and there exists $x \in R$ such that $\mathfrak{p} = \mathrm{rad}(\mathfrak{a} : x) = \bigcap_{i=1, x\notin \mathfrak{q}_i}^n \mathfrak{p}_i$ which is not an empty intersection since $\mathfrak{p} \neq R$. Hence 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, $\bigcap_{i=1, i\neq j}^n \mathfrak{q}_i \not\subseteq \mathfrak{q}_j$. Hence 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 $x \notin \mathfrak{q}_j$. Hence $\mathrm{rad}(\mathfrak{a} : x) = \bigcap_{i=1, x\notin \mathfrak{q}_i}^n \mathfrak{p}_i = \mathfrak{p}_j$. Hence $\mathfrak{p}_j \in \mathrm{Spec}(R) \cap \{\mathrm{rad}(\mathfrak{a} : x) \mid x \in R\}$. $\square$

Theorem 4.31. *If R is noetherian, then*

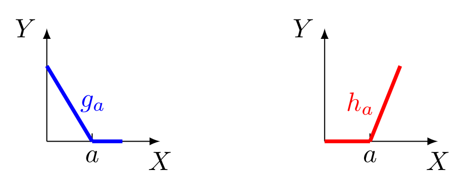
$$\begin{aligned}\mathrm{Ass}_R(\mathfrak{a}) := \{\mathfrak{p}_1, \dots, \mathfrak{p}_n\} &= \mathrm{Spec}(R) \cap \{(\mathfrak{a} : x) \mid x \in R\} \\ &= \mathrm{Spec}(R) \cap \{\mathrm{Ann}_R(\overline{x}) \mid \overline{x} \in R/\mathfrak{a}\} =: \mathrm{Ass}_R(R/\mathfrak{a}).\end{aligned}$$

Proof. Proof of the first equality. "$\supseteq$". Let $\mathfrak{p} \in \mathrm{Spec}(R)$ such that $\mathfrak{p} = (\mathfrak{a} : x)$ for some $x \in R$. Then $\mathfrak{p} = \mathrm{rad}(\mathfrak{p}) = \mathrm{rad}(\mathfrak{a} : x)$. Hence 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 $\mathrm{rad}(\mathfrak{q}_j) = \mathfrak{p}_j$, 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 that $\mathfrak{a}_j \mathfrak{p}_j^0 = \mathfrak{a}_j \supsetneq \mathfrak{a}$. Since $\mathfrak{a}_j \mathfrak{p}_j^{l-1} \not\subseteq \mathfrak{a}$, there exists $x \in \mathfrak{a}_j \mathfrak{p}_j^{l-1} \smallsetminus \mathfrak{a} \subseteq \mathfrak{a}_j \smallsetminus \mathfrak{a} = (\bigcap_{i=1, i\neq j}^n \mathfrak{q}_i) \smallsetminus \mathfrak{q}_j$, i.e., $x \in \mathfrak{q}_i$ for $1 \leq i \leq n$ with $i \neq j$ and $x \notin \mathfrak{q}_j$. Hence by the proof of Proposition 4.30, $(\mathfrak{a} : x) \subseteq \mathrm{rad}(\mathfrak{a} : x) = \mathfrak{p}_j$. 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 that $\mathfrak{p}_j \subseteq (\mathfrak{a} : x)$. Hence $\mathfrak{p}_j = (\mathfrak{a} : x)$. $\square$

Example 4.32. If R is not noetherian, then $\mathfrak{a} \lneq R$ may not have a primary decomposition. Let $R = \mathcal{C}([0,1]) = \{\text{continuous } f : [0,1] \to \mathbb{R}\}$ with pointwise operations. We claim that $0 \leq R$ does not have a primary decomposition.

(a) For $a \in [0,1]$, define $\Phi_a : R \to \mathbb{R}$ by $\Phi_a(f) = f(a)$. Then Φ_a is a well-defined ring epimorphism. Hence $\frac{R}{\mathrm{Ker}(\Phi_a)} \cong \mathbb{R}$. Hence $\{f \in R \mid f(a) = 0\} = \mathrm{Ker}(\Phi_a) \in \text{m-Spec}(R) \subseteq \mathrm{Spec}(R)$.

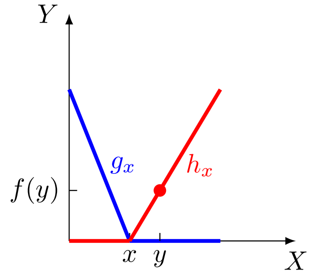
(b) We claim that $0 \notin \mathrm{Spec}(R)$. For $a \in (0,1)$, there exist $g_a, h_a \in R$ such that $g_a h_a = 0$ but $g_a, h_a \neq 0$.



(c) We claim that $\mathrm{Nil}(R) = 0$. Let $f \in \mathrm{Nil}(R)$. 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) We claim that $(0 : f) = \mathrm{rad}(0 : f)$ for $f \in R$. "$\subseteq$". Done. "$\supseteq$". Let $g \in \mathrm{rad}(0 : f)$. Then $g^m \cdot f = 0$ for some $m \geq 1$. Hence $g^m f^m = 0$. Hence $gf \in \mathrm{Nil}(R) = 0$ by (c), i.e., $g \in (0 : f)$.

(e) We claim that $(0 : f) \notin \operatorname{Spec}(R)$ for $f \in R$. Suppose $(0 : f) \in \operatorname{Spec}(R)$. Then $(0 : f) \neq R$, i.e., $f \neq 0$. Hence 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 $g_x h_x = 0 \in (0 : f) \in \operatorname{Spec}(R)$.



Hence $g_x \in (0 : f)$ or $h_x \in (0 : f)$, i.e., $g_x f = 0$ or $h_x f = 0$. Since $h_x(y)f(y) > 0$, $h_x f \neq 0$. Hence $g_x f = 0$. Also, since $g_x(a) \neq 0$ for $0 < a < x < y$, we have that $f(a) = 0$ for $0 < a < x < y$. Since $x \in (0, y)$ is arbitrary, $f(a) = 0$ for $0 < a < y$. Since f is continuous, $f(y) = \lim_{a \to y^-} f(a) = 0$, 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 $\operatorname{Spec}(R) \not\ni (0 : f_1) = \operatorname{rad}(0 : f_1) = \operatorname{rad}(\mathfrak{q}_1) \in \operatorname{Spec}(R)$, a contradiction.

(f) Note that

$$0 = \{f \in R \mid f(a) = 0, \forall a \in [0, 1]\} = \bigcap_{a \in [0,1]} \underbrace{\{f \in R \mid f(a) = 0\}}_{\in \operatorname{Spec}(R),\ \therefore \text{ primary}}$$
$$= \bigcap_{a \in [0,1]} \operatorname{Ker}(\Phi_a) = \bigcap_{a \in [0,1] \cap \mathbb{Q}} \operatorname{Ker}(\Phi_a) = \cdots$$

cannot be pruned to a minimal primary decomposition.

Proposition 4.33.

$$\{x \in R \mid (\mathfrak{a} : x) \neq \mathfrak{a}\} = \bigcup_{i=1}^n \mathfrak{p}_i = \bigcup_{\mathfrak{p} \in \operatorname{Ass}_R(\mathfrak{a})} \mathfrak{p}.$$

Proof. We claim that $\{x \in R \mid (\mathfrak{a} : x) \neq \mathfrak{a}\} = \bigcup_{y \notin \mathfrak{a}} \operatorname{rad}(\mathfrak{a} : y)$. "$\subseteq$". Then $x \in R$ such that $(\mathfrak{a} : x) \neq \mathfrak{a}$. Hence $(\mathfrak{a} : x) \supsetneq \mathfrak{a}$. Then there exists $z \in (\mathfrak{a} : x) \smallsetminus \mathfrak{a}$, i.e., $z \notin \mathfrak{a}$ and $xz \in \mathfrak{a}$, i.e., $z \notin \mathfrak{a}$ and $x \in (\mathfrak{a} : z) \subseteq \operatorname{rad}(\mathfrak{a} : z) \subseteq \bigcup_{y \notin \mathfrak{a}} \operatorname{rad}(\mathfrak{a} : y)$. "$\supseteq$". Let $x \in \operatorname{rad}(\mathfrak{a} : y)$ 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 that $x^0 y = y \notin \mathfrak{a}$. Then $x^n y \in \mathfrak{a}$ but $x^{n-1} y \notin \mathfrak{a}$. Hence $x^{n-1} y \in (\mathfrak{a} : x)$. Hence $(\mathfrak{a} : x) \neq \mathfrak{a}$.

We claim that $\bigcup_{y \notin \mathfrak{a}} \operatorname{rad}(\mathfrak{a} : y) = \bigcup_{i=1}^n \mathfrak{p}_i$. "$\subseteq$". Let $y \notin \mathfrak{a} = \bigcap_{i=1}^n \mathfrak{q}_i$. Then by the proof of Proposition 4.30,

$$\operatorname{rad}(\mathfrak{a} : y) = \bigcap_{i=1, y \notin \mathfrak{q}_i}^n \mathfrak{p}_i = \bigcap_{i=1}^n \mathfrak{p}_i \subseteq \bigcup_{i=1}^n \mathfrak{p}_i.$$

"$\supseteq$". By Proposition 4.30, there exists $y_i \notin \mathfrak{a}$ such that $\mathfrak{p}_i = \operatorname{rad}(\mathfrak{a} : y_i)$ for $i = 1, \ldots, i$. Hence $\bigcup_{y \notin \mathfrak{a}} \operatorname{rad}(\mathfrak{a} : y) \supseteq \bigcup_{i=1}^n \mathfrak{p}_i$. $\square$

Corollary 4.34. Set $\mathfrak{a} = 0$ in Proposition 4.33, we get

$$\operatorname{ZD}(R) = \{x \in R \mid (0 : x) \neq 0\} = \bigcup_{i=1}^{n} \mathfrak{p}_i = \bigcup_{\mathfrak{p} \in \operatorname{Ass}_R(0)} \mathfrak{p}.$$

Summary 4.35. Let R be noetherian and $\mathfrak{a} = 0$. Then $\operatorname{ZD}(R) = \bigcup_{i=1}^{n} \mathfrak{p}_i = \bigcup_{\mathfrak{p} \in \operatorname{Ass}_R(0)} \mathfrak{p}$. (Use with prime avoidence to get useful information about ideals and $\operatorname{NZD}(R)$.)

$$\operatorname{Nil}(R) = \operatorname{rad}(0) = \operatorname{rad}\left(\bigcap_{i=1}^{n} \mathfrak{q}_i\right) = \bigcap_{i=1}^{n} \mathfrak{p}_i = \bigcap_{\mathfrak{p} \in \operatorname{Min}(0)} \mathfrak{p}.$$

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 $x = \overline{X}, y = \overline{Y} \in R$. Then $\langle 0\rangle R = \langle x\rangle \cap \langle x^2, y\rangle$ is a minimal primary decomposition. Hence $\operatorname{ZD}(R) = \langle x\rangle \cup \langle x, y\rangle = \langle x, y\rangle$. For $f \in R$ with constant term 0, we have that $f = xf_1 + yf_2$ for some $f_1, f_2 \in R$, then $xf = x^2 f_1 + xyf_2 = 0$. Hence $f \in \operatorname{ZD}(R)$.

Proposition 4.36. We have that

$$\operatorname{Min}(\mathfrak{a}) = \min\{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\} = \operatorname{Min}(\operatorname{V}(\mathfrak{a})).$$

In particular,

$$\operatorname{Min}(0) = \operatorname{Min}(\operatorname{V}(0)) = \operatorname{Min}(\operatorname{Spec}(R)) = \operatorname{Min}(R).$$

Proof. It follows from the proof of Proposition 4.28. □

Lemma 4.37. Let $U \subseteq R$ be multiplicatively closed and $\mathfrak{q} \subsetneq R$ be $\mathfrak{p}$-primary. Let $\psi : R \to U^{-1}R$ 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 $U^{-1}\mathfrak{q} \subsetneq U^{-1}R$ 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 $\mathfrak{p} = \operatorname{rad}(\mathfrak{q})$ and U is multiplicatively closed, there exists $n \geq 1$ such that $u^n \in \mathfrak{q} \cap U$. Hence 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 $\frac{x}{u}, \frac{y}{v} \in U^{-1}R$ $\frac{x}{u} \cdot \frac{y}{v} \in U^{-1}\mathfrak{q}$. If $\frac{y}{v} \in \operatorname{rad}(U^{-1}\mathfrak{q})$, then $U^{-1}\mathfrak{q}$ is primary. Assume $\frac{y}{v} \notin \operatorname{rad}(U^{-1}\mathfrak{q})$. Since $\frac{xy}{uv} \in U^{-1}\mathfrak{q}$, there exists $w \in U$ such that $x(wy) = wxy \in \mathfrak{q}$. Since $\frac{y}{v} \notin \operatorname{rad}(U^{-1}\mathfrak{q}) = U^{-1}\operatorname{rad}(\mathfrak{q}) = U^{-1}\mathfrak{p}$ by Proposition 3.12(d), $wy \notin \mathfrak{p} = \operatorname{rad}(\mathfrak{q})$. Also, since $\mathfrak{q}$ is primary, $x \in \mathfrak{q}$. Hence $\frac{x}{u} \in U^{-1}\mathfrak{q}$. Hence $U^{-1}\mathfrak{q}$ is primary.

Since $\mathfrak{q} \subseteq \mathfrak{p} = \operatorname{rad}(\mathfrak{q}) \in \operatorname{Spec}(R)$, by Proposition 3.12(d), we have that $\operatorname{rad}(U^{-1}\mathfrak{q}) \subseteq \operatorname{rad}(U^{-1}\mathfrak{p}) = U^{-1}\operatorname{rad}(\mathfrak{p}) = U^{-1}\mathfrak{p} = U^{-1}\operatorname{rad}(\mathfrak{q}) = \operatorname{rad}(U^{-1}\mathfrak{q})$. Hence $\operatorname{rad}(U^{-1}\mathfrak{q}) = U^{-1}\mathfrak{p}$.

We claim that $\psi^{-1}(U^{-1}\mathfrak{q}) = \mathfrak{q}$. "$\supseteq$". By Proposition 1.63(a). "$\subseteq$". Let $x \in \psi^{-1}(U^{-1}\mathfrak{q})$. Then $\frac{x}{1} = \psi(x) \in U^{-1}\mathfrak{q}$. Hence there exists $u \in U$ such that $xu \in \mathfrak{q}$. Since $U \cap \mathfrak{p} = \emptyset$, $u \notin \mathfrak{p} = \operatorname{rad}(\mathfrak{q})$. Also, since $\mathfrak{q}$ is primary, $x \in \mathfrak{q}$. □

Theorem 4.38 (Second uniqueness theorem)**.** *(a) Let $\mathfrak{q} = \mathfrak{q}_i$ be $\mathfrak{p}$-primary for some $i \in \{1, \ldots, n\}$ with $\mathfrak{p} \in \operatorname{Min}(\mathfrak{a})$. Then $\mathfrak{q} = \psi^{-1}(\mathfrak{a}_\mathfrak{p})$*†*, where $\psi : R \to R_\mathfrak{p}$ and $U = R \smallsetminus \mathfrak{p}$, so $\mathfrak{q}$ is independent of choice of minimal primary decomposition.*

†That is, $\mathfrak{q}$ is the kernel of the ring homomorphism $R \to (R/\mathfrak{a})_\mathfrak{p}$.

(b) If $\Lambda = \langle \mathfrak{p}_{i_1}, \ldots, \mathfrak{p}_{i_m}\rangle$ is an "isolated" subset of $\mathrm{Ass}_R(\mathfrak{a}) = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$, then $\bigcap_{j=1}^m \mathfrak{q}_{i_j} = \Psi^{-1}(U^{-1}\mathfrak{a})$, where $\Psi : R \to U^{-1}R$ and $U = R \smallsetminus \{\mathfrak{p}_{i_1} \cup \cdots \cup \mathfrak{p}_{i_m}\}$. Hence $\bigcap_{j=1}^m \mathfrak{q}_{i_j}$ is independent of choice of minimal primary decomposition.

Proof. (b) By Proposition 3.12(b) and Lemma 4.37, we have that $\Psi^{-1}(U^{-1}\mathfrak{a}) = \Psi^{-1}(U^{-1}(\bigcap_{i=1}^n \mathfrak{q}_i)) = \Psi^{-1}(\bigcap_{i=1}^n U^{-1}\mathfrak{q}_i) = \bigcap_{i=1}^n \Psi^{-1}(U^{-1}\mathfrak{q}_i) = \bigcap_{i=1,\mathfrak{p}_i\cap U=\emptyset}^n \mathfrak{q}_i = \bigcap_{j=1}^m \mathfrak{q}_{i_j}$ since Λ is "isolated".

(a) It follows from (b) since $\{\mathfrak{p}\}$ is "isolated" for $\mathfrak{p} \in \mathrm{Min}(\mathfrak{a})$. $\square$

Definition 4.39. $\Lambda \subseteq \mathrm{Ass}_R(\mathfrak{a})$ is "*isolated*" if it is "closed under subsets", i.e., if $\mathfrak{p}, \mathfrak{p}' \in \mathrm{Ass}_R(\mathfrak{a})$ 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 $\mathfrak{p} = \langle X_{i_1}, \cdots, X_{i_m}\rangle \subsetneq k[X_1, \ldots, X_d]$, then $\mathfrak{p}^n$ is $\mathfrak{p}$-primary for $n \geq 1$.

Proof. (b) Note that $\langle X_{i_1}^{a_1}, \ldots, X_{i_m}^{a_m}\rangle$ is $\mathfrak{p}$-primary for $a_1, \ldots, a_m \geq 1$ by Example 4.12(c). Let $\Lambda = \{\underline{a} \in \mathbb{N}^m \mid a_1 + \cdots + a_m = m + n - 1\}$. Set $\mathfrak{p}_{\underline{a}} = \langle X_{i_1}^{a_1}, \ldots, X_{i_m}^{a_m}\rangle$ for $\underline{a} \in \Lambda$. We claim that $\mathfrak{p}^n = \bigcap_{\underline{a}\in\Lambda} \mathfrak{p}_{\underline{a}}$, then by Proposition 4.22, $\mathfrak{p}^n$ is $\mathfrak{p}$-primary.

"$\subseteq$". Let $\Lambda_0 = \{\underline{e} \in \mathbb{Z}_{\geq 0}^m \mid e_1 + \cdots + e_m = n\}$. For $n \geq 1$,

$$\mathfrak{p}^n = (\langle X_{i_1}\rangle + \cdots + \langle X_{i_m}\rangle)^n = \sum_{\underline{e}\in\Lambda_0} \langle X_{i_1}^{e_1} \cdots X_{i_m}^{e_m}\rangle.$$

Suppose that $X_{(i)}^{\underline{e}} := X_{i_1}^{e_1} \cdots X_{i_m}^{e_m} \in \mathfrak{p}^n \smallsetminus \mathfrak{p}_{\underline{a}}$ for some $\underline{e} \in \Lambda_0$ and $\underline{a} \in \Lambda$. Then $a_i \geq e_i + 1$ for $i = 1, \ldots, m$. Hence $m+n-1 = \sum_{i=1}^m a_i \geq m + \sum_{i=1}^m e_i = m+n$, a contradiction. Hence $X_{(i)}^{\underline{e}} \in \mathfrak{p}_{\underline{a}}$ 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 $R' := k[X_{i_1}, \ldots, X_{i_m}] \subseteq k[X_1, \ldots, X_d]$ and $\mathfrak{p}' = (X_{i_1}, \ldots, X_{i_m})R'$. Set $\mathfrak{p}'_{\underline{a}} = \langle X_{i_1}^{a_1}, \ldots, X_{i_m}^{a_m}\rangle R'$ 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 $\{\mathrm{lcm}(f_1, \ldots, f_q) \mid f_j$ is a generator of $\mathfrak{p}_{\underline{a}_j}$ with $\underline{a}_j \in \Lambda$ for $j = 1, \ldots, q\}$, we have that 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 $\mathfrak{p} \in \mathrm{Spec}(R)$. For example, let $R = \frac{k[X,Y,Z]}{\langle XY - Z^2\rangle}$ and $x = \overline{x}, y = \overline{Y}, z = \overline{Z} \in R$, then $\mathfrak{p} := \langle x, z\rangle \in \mathrm{Spec}(R)$, but $\mathfrak{p}^2$ is not $\mathfrak{p}$-primary since $xy = z^2 \in \mathfrak{p}^2$ but $x \notin \mathfrak{p}^2$ and $y \notin \mathfrak{p} = \mathrm{rad}(\mathfrak{p}^2)$.

Definition 4.42. Let $\mathfrak{p} \in \mathrm{Spec}(R)$ and $\psi : R \to R_{\mathfrak{p}}$. Then for $n \geq 1$, the n^{th} *symbolic power* of $\mathfrak{p}$ is

$$\mathfrak{p}^{(n)} = \psi^{-1}((\mathfrak{p}^n)_{\mathfrak{p}}) = \psi^{-1}\left((\mathfrak{p}_{\mathfrak{p}})^n\right).$$

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.

(a) Let $\mathfrak{m} \in \text{m-Spec}(R)$ and $\psi : R \to R_{\mathfrak{m}}$. Since $\mathfrak{m}^n$ is $\mathfrak{m}$-primary by Example 4.11(b) and $\mathfrak{m} \cap (R \smallsetminus \mathfrak{m}) = \emptyset$, 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 $\mathfrak{p} = \langle X_{i_1}, \cdots, X_{i_m} \rangle \lneq k[X_1, \ldots, X_d]$. Since $\mathfrak{p}^n$ is $\mathfrak{p}$-primary by Discussion 4.40(b) and $\mathfrak{p} \cap (R \smallsetminus \mathfrak{p}) = \emptyset$, 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 $\mathfrak{p} = \langle x, z \rangle$. We claim that $\mathfrak{p}^{(2)} = \langle x \rangle$. "$\supseteq$". Since $y \notin \mathfrak{p}$ and $xy = z^2 \in \mathfrak{p}^2$, we have that $x = \frac{x}{1} = \frac{xy}{y} \in (\mathfrak{p}^2)_\mathfrak{p}$ in $R_\mathfrak{p}$. Hence $x \in \psi^{-1}(\mathfrak{p}^2)_\mathfrak{p}) = \mathfrak{p}^{(2)}$. "$\subseteq$". Let $a \in \mathfrak{p}^{(2)}$. Then $a = \frac{a}{1} = \psi(a) \in (\mathfrak{p}^2)_\mathfrak{p}$. Hence there exists $b \in R \smallsetminus \mathfrak{p}$ 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 that 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 $\mathfrak{p} \in \operatorname{Spec}(R)$, 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 $\mathfrak{p}_i = \operatorname{rad}(\mathfrak{q}_i)$ for $i = 1, \ldots, m$, then $\mathfrak{p}_j = \mathfrak{p}$ and $\mathfrak{q}_j = \mathfrak{p}^{(n)}$ for some $j \in \{1, \ldots, m\}$.

Proof. Since $\operatorname{rad}(\mathfrak{p}^n) = \mathfrak{p}$, $\operatorname{Min}(\mathfrak{p}^n) = \{\mathfrak{p}\}$. Hence $\mathfrak{p} = \operatorname{rad}(\mathfrak{q}_j) = \mathfrak{p}_j$ for some $j \in \{1, \ldots, m\}$. Then by the second uniqueness theorem, $\mathfrak{q}_j = \psi^{-1}((\mathfrak{p}_j^n)_{\mathfrak{p}_j}) = \psi^{-1}((\mathfrak{p}^n)_\mathfrak{p}) = \mathfrak{p}^{(n)}$. □

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 $\mathfrak{p} = \langle x, z \rangle \in \operatorname{Spec}(R)$. Then by Example 4.44(c), $\mathfrak{p}^{(2)} = \langle x \rangle$. Note that $\mathfrak{p}^2 = \langle x \rangle \cap \langle x^2, z, y \rangle$ with $\operatorname{rad}(\langle x \rangle) = \langle x, z \rangle = \mathfrak{p}$ since $z^2 = xy$, and with $\operatorname{rad}(\langle x^2, z, y \rangle) = \langle x, y, z \rangle \in \text{m-Spec}(R)$ 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 $R = \mathbb{C}[X_1, \ldots, X_d]$ and $\mathfrak{p} \in \operatorname{Spec}(R)$ (Zariski).

$$\mathfrak{p}^{(2)} = \left\{ f \in \mathfrak{p} \;\middle|\; \frac{\partial f}{\partial x_i} \in \mathfrak{p}, \forall i = 1, \ldots, d \right\},$$

$$\mathfrak{p}^{(n)} = \left\{ f \in \mathfrak{p} \;\middle|\; \frac{\partial^i f}{\partial \underline{x}} \in \mathfrak{p}, \text{ all partials of order } i = 1, \ldots, n-1 \right\}, \forall n \geq 3.$$

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 $R \times M \to M$ 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 $n = 1, 2, 3, \cdots$, let $R^n = \left\{ \begin{bmatrix} r_1 \\ \vdots \\ r_n \end{bmatrix} \middle| \, r_1, \ldots, r_n \in R \right\}$ 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 $\varphi : R \to S$ 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 $y_1, \ldots, y_n \in M$ such that $M = \langle y_1, \ldots, y_n\rangle$.

Fact 5.6. (a) Let $Y \subseteq M$. Then

$$\langle Y\rangle = \left\{ \sum_{y\in Y}^{\text{finite}} r_y y \;\middle|\; r_y \in R, \forall y \right\} = \sum_{y\in Y} \langle y\rangle.$$

(b) If $y_1, \ldots, y_n \in M$, then

$$\langle y_1, \ldots, y_n\rangle = \left\{ \sum_{i=1}^{n} r_i y_i \;\middle|\; r_1, \ldots, r_n \in R \right\}.$$

Example 5.7. Submodules of a finitely generated R-module may not be finitely generated. Note that $R := k[X_1, X_2, \cdots] = \langle 1\rangle$ is a finitely generated R-module, but $\mathfrak{m} = \langle X_1, X_2, \cdots\rangle \subseteq R$ 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 $r_0, \ldots, r_{n-1} \in R$ such that $s^n + r_{n-1}s^{n-1} + \cdots + r_0 = 0$.

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 $(\frac{r}{s})^n + c_{n-1}(\frac{r}{s})^{n-1} + \cdots + c_1(\frac{r}{s}) + c_0 = 0$ for some $n \geq 1$ and $c_0, \ldots, c_{n-1} \in R$. Hence $\frac{r^n + c_{n-1}r^{n-1}s + \cdots + c_1 rs^{n-1} + c_0 s^n}{s^n} = 0$, i.e.,

$$r^n = -(c_{n-1}r^{n-1}s + \cdots + c_1 rs^{n-1} + c_0 s^n) = -s(c_{n-1}r^{n-1} + \cdots + c_1 rs^{n-2} + c_0 s^{n-1}).$$

Hence $s \mid r^n$. Since $(r,s) = 1$, $(r^n, s) = 1$. Hence $s = \pm 1$. Thus, $\frac{r}{s} = \pm r \in \mathbb{Z}$. □

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 $y_1, \ldots, y_n \in S$. Define the *subring* of S generated over R by $y_1, \ldots, y_n$ by

$$R[y_1, \ldots, y_n] = \bigcap_{\substack{R \subseteq T \subseteq S, \\ y_1, \ldots, y_n \in T}} T,$$

where the intersection is taken over all intermediate subrings $R \subseteq T \subseteq S$ such that $y_1, \ldots, y_n \in T$.

Fact 5.11. Let $y_1, \ldots, y_n \in S$.

(a) $R[y_1, \ldots, y_n] = \{f(y_1, \ldots, y_n) \in S \mid f \in R[Y_1, \ldots, Y_n]\}$.

(b) $\psi : R[Y_1, \ldots, Y_n] \to S$ given by $\psi(f) = f(y_1, \ldots, y_n)$ is a well-defined ring homomorphism with $\operatorname{Im}(\psi) = R[y_1, \ldots, y_n]$ and $\overline{Y_1}, \ldots, \overline{Y_n} \in R[Y_1, \ldots, Y_n]/\operatorname{Ker}(\psi) \cong R[y_1, \ldots, y_n]$. Hence if $y_1, \ldots, y_n$ have no polynomial relations, then $\operatorname{Ker}(\psi) = 0$ and hence $R[Y_1, \ldots, Y_n] \cong R[y_1, \ldots, y_n]$.

(c) Let $T \subseteq S$ be a subring. Then $R[y_1, \ldots, y_n] \subseteq T$ if and only if $R \subseteq T$ and $y_1, \ldots, y_n \in T$.

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)$\Longrightarrow$(ii). Method 1. Assume s is integral over R. Then $s^n + r_{n-1}s^{n-1} + \cdots + r_0 = 0$ for some $n \geq 1$ and $r_0, \ldots, r_{n-1} \in R$. We claim that $R[s] = R\langle 1, s, \ldots, s^{n-1} \rangle$.

$\supseteq$ It is straightforward.

$\subseteq$ It suffices to show $s^m \in R\langle 1, s, \ldots, s^{n-1} \rangle$ for $m = n, n+1, \cdots$. Use induction on m. Base case: $s^n = -\sum_{i=0}^{n-1} r_i s^i \in R\langle 1, s, \ldots, s^{n-1} \rangle$. Inductive step: assume $m \geq n+1$ and $s^k \in R\langle 1, s, \ldots, s^{n-1} \rangle$ for $0 \leq k \leq m-1$. Then

$$s^m = s^n s^{m-n} = -\sum_{i=0}^{n-1} r_i s^{i+m-n} \in R\langle s^{m-n}, \ldots, s^{m-1} \rangle \subseteq R\langle 1, s, \ldots, s^{n-1} \rangle$$

by inductive hypothesis.

Method 2. Assume s is integral over R. Then there exists $f \in R[x]$ monic such that $f(s) = 0$. Let $g \in R[x]$. Write $g(x) = f(x)q(x) + r(x)$ with $q, r \in R[x]$, where $r = 0$ or $\deg(r) < \deg(f)$. Then $g(s) = f(s)q(s) + r(s) = r(s)$. This implies $R[s]$ is finitely generated by $1, s, \dots, s^{\deg(f)-1}$ as an R-module.

(ii)$\Longrightarrow$(iii) Use $T = R[s]$.

(iii)$\Longrightarrow$(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 $\sum_{i=1}^n \delta_{ij} s y_i = sy_j = \sum_{i=1}^n a_{ij} y_i$, 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 $(\det(B)(\delta_{ij}))\vec{y} = \operatorname{adj}(B)B\vec{y} = \vec{0}$, † 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 $1 = \sum_{j=1}^n c_j y_j$. Hence $\det(\delta_{ij}s - a_{ij}) = \det(B)\cdot 1 = \det(B)\sum_{j=1}^n c_j y_j = \sum_{j=1}^n c_j \det(B) y_j = 0$, i.e.,

$$0 = \det(\delta_{ij}s - a_{ij}) = \begin{vmatrix} s-a_{11} & -a_{12} & \cdots & -a_{1n} \\ -a_{21} & s-a_{22} & \cdots & -a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ -a_{n1} & -a_{n2} & \cdots & s-a_{nn} \end{vmatrix} = s^n + c_{n-1}s^{n-1} + \cdots + c_1 s + c_0,$$

where $c_0, \dots, c_{n-1} \in R$ since they are built from $a_{ij} \in R$. ☐

Theorem 5.14. *$s_1, \dots, s_n \in S$ are integral over R if and only if $R[s_1, \dots, s_n]$ is a finitely generated R-module.*

Proof. $\Longrightarrow$ 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. We claim that $C = A\langle b_i c_j \mid i = 1, \dots, m, j = 1, \dots, n\rangle$.

$\supseteq$ 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 that for $j = 1, \dots, n$, $\beta_j = \sum_{i=1}^m \alpha_{ij} b_i$ for some $\alpha_{1j}, \dots, \alpha_{mj} \in A$. Hence $c = \sum_{j=1}^n (\sum_{i=1}^m \alpha_{ij} b_i) c_j = \sum_{i=1}^m \sum_{j=1}^n \alpha_{ij} b_i c_j$.

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. Hence $R[s_1, s_2]$ is a finitely generated R-module by our result. Continuing in this fashion, we have that $R[s_1, \dots, s_n]$ is a finitely generated R-module.

$\Longleftarrow$ follows from Proposition 5.13 by considering the intermediate subring $R \subseteq R[s_1, \dots, s_n] \subseteq S$. ☐

Theorem 5.15. *Let $\overline{R} := \{s \in S \mid s \text{ is integral over } R\}$. Then $R \subseteq \overline{R} \subseteq S$ is an intermediate subring. Hence for $s, s' \in S$ integral over R, the elements $s \pm s'$ and ss' are integral over R.*

Proof. $R \subseteq \overline{R}$ is straightforward. Since s, s' are integral over R, $T := R[s, s']$ is a finitely generated R-module by Theorem 5.14. Hence $s \pm s', ss'$ are integral over R by Proposition 5.13(iii). Hence $s \pm s', ss' \in \overline{R}$. Since $R \subseteq S$ is a subring, $1_S = 1_R \in \overline{R}$. Hence by subring test, $\overline{R} \subseteq S$ is a subring. ☐

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)$\Longrightarrow$(ii) of

† $A \operatorname{adj}(A) = \operatorname{adj}(A)A = \det(A)(\delta_{ij})$ for $A \in \mathrm{Mat}_n(R)$. When A is invertible, $\operatorname{adj}(A)$ is unique.

Proposition 5.13, we have that

$$\begin{aligned}R[s,s'] &= R[s][s'] = R[s]\langle 1, s', \ldots, s'^{n-1}\rangle = R\langle 1, s, \ldots, s^{m-1}\rangle\langle 1, s', \ldots, s'^{n-1}\rangle\\ &= R\langle 1, s', \ldots, s'^{n-1}, s, ss', \ldots, ss'^{n-1}, \ldots, s^{m-1}, s^{m-1}s', s^{m-1}s'^{n-1}\rangle,\end{aligned}$$

which has mn generators. Hence by the proof (iii)$\Longrightarrow$(i) of Proposition 5.13, we have that 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. $\overline{R} = \{s \in S \mid s \text{ is integral over } R\}$ is the *integral closure* of R in S.
If $\overline{R} = S$, then S is *integral* over R. If $\overline{R} = R$, then R is *integrally closed* in S.

Example 5.17. (a) $\mathbb{Z}[i]$ is integral over $\mathbb{Z}$ with $\overline{\mathbb{Z}} = \mathbb{Z}[i]$.

(b) $\mathbb{Z}$ is integrally closed in $\mathbb{Q}$ with $\overline{\mathbb{Z}} = \mathbb{Z}$.

(c) $\overline{\mathbb{Z}} = \mathbb{Z}[i]$ in $\mathbb{Q}(i)$.

Definition 5.18. Let $\varphi : R \to S$ be a ring homomorphism. Then φ is *integral* if $\mathrm{Im}(\varphi) \subseteq S$ is an integral extension.

Theorem 5.19. *The following are equivalent.*

(i) S is a finitely generated R-module.

(ii) $S = R[s_1, \ldots, s_n]$ for some $s_1, \ldots, s_n$ and is integral over R.

(iii) $S = R[s_1, \ldots, s_n]$ for some $s_1, \ldots, s_n$ integral over R.

Proof. (i)$\Longrightarrow$(ii) Assume $S = R\langle s_1, \ldots, s_n\rangle$. Then $S = R\langle s_1, \ldots, s_n\rangle \subseteq R[s_1, \ldots, s_n] \subseteq S$. Hence $S = R[s_1, \ldots, s_n]$. Note that there exists an intermediate subring $R \subseteq R[s_1, \ldots, s_n] := T \subseteq S$ such that T is a finitely generated R-module. Then $s_1, \ldots, s_n \in S$ are integral over R by Proposition 5.13. Since $\overline{R} \subseteq S$ is a subring by Theorem 5.15, $S = R[s_1, \ldots, s_n] \subseteq \overline{R} \subseteq S$ by Fact 5.11(c). Hence $\overline{R} = S$.

(ii)$\Longrightarrow$(iii) is trivial.

(iii)$\Longrightarrow$(i) follows from Theorem 5.14. □

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. Hence $t^n + s_{n-1}t^{n-1} + \cdots + s_0 = 0$ for some $n \geq 1$ and $s_0, \ldots, s_{n-1} \in S$. Hence t is integral over $R[s_0, \ldots, s_{n-1}]$. Hence $R[s_0, \ldots, s_{n-1}, t] = R[s_0, \ldots, s_{n-1}][t]$ is a finitely generated $R[s_0, \ldots, s_{n-1}]$-module by Proposition 5.13. Since S is integral over R and $s_0, \ldots, s_{n-1} \in S$, $s_0, \ldots, s_{n-1}$ are integral over R. Hence $R[s_0, \ldots, s_{n-1}]$ is a finitely generated R-module by Theorem 5.14. Thus, $R[s_0, \ldots, s_{n-1}, t]$ 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). □

Corollary 5.21. If $\overline{R}$ is an integral closure of R in S, then $\overline{R}$ is integrally closed in S, i.e., $\overline{\overline{R}} = \overline{R}$.

Proof. Let $s \in \overline{\overline{R}}$. Then $s \in S$ be integral over $\overline{R}$. Hence $R \subseteq \overline{R} \subseteq \overline{R}[s]$ are integral extensions by Theorem 5.15. Hence $R \subseteq \overline{R}[s]$ is an integral extension by Corollary 5.20. Hence s is integral over R, i.e., $s \in \overline{R}$. □

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 $R/\mathfrak{a} \to S/\mathfrak{b}$ 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

$$\begin{tikzcd}
R \arrow[r, "\subseteq", "p"'] \arrow[d, "\tau"] \arrow[dr, "\rho"'] & S \arrow[d, "\pi"] \\
R/\mathfrak{a} \arrow[r, hook, dashed, "\exists!\ \bar{\rho}"'] & S/\mathfrak{b} \\
\bar{r} \arrow[r, mapsto] & \bar{r}
\end{tikzcd}$$

Since $\mathrm{Ker}(\rho) = \mathrm{Ker}(\pi) \cap R = \mathfrak{b} \cap R = \mathfrak{a}$, by the first isomorphism, $R/\mathfrak{a} \cong \mathrm{Im}(\bar{\rho}) \subseteq S/\mathfrak{b}$.

Let $\bar{s} \in S/\mathfrak{b}$. Then s is integral over R since S is integral over R. Hence s satisfies $X^n + \sum_{i=0}^{n-1} a_i X^i$ for some $a_0, \ldots, a_{n-1} \in R$. Hence $\bar{s}$ satisfies $X^n + \sum_{i=0}^{n-1} \bar{a}_i X^i$ for some $\bar{a}_0, \ldots, \bar{a}_{n-1} \in R/\mathfrak{a} \cong \mathrm{Im}(\bar{\rho})$.

(b) Let $\frac{s}{u} \in U^{-1}S$ with $s \in S$ and $u \in U$. Then s is integral over R. Hence $s^n + a_{n-1}s^{n-1} + \cdots + a_0 = 0$ for some $a_0, \ldots, a_{n-1} \in R$. Hence

$$0 = \frac{s^n + a_{n-1}s^{n-1} + \cdots + a_1 s + a_0}{u^n} = \left(\frac{s}{u}\right)^n + \left(\frac{a_{n-1}}{u}\right)\left(\frac{s}{u}\right)^{n-1} + \cdots + \left(\frac{a_1}{u^{n-1}}\right)\left(\frac{s}{u}\right) + \left(\frac{a_0}{u^n}\right)$$

for some $\frac{a_0}{u^n}, \frac{a_1}{u^{n-1}}, \ldots, \frac{a_{n-1}}{u} \in U^{-1}R$. □

Discussion 5.23. Let $\mathfrak{p} \in \mathrm{Spec}(R)$. When does there exist $\mathfrak{q} \in \mathrm{Spec}(S)$ such that $\mathfrak{p} = \mathfrak{q} \cap R$? i.e., when is the induced map $\mathrm{Spec}(S) \to \mathrm{Spec}(R)$ 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. $\Longrightarrow$ Assume R is a field. Let $0 \neq s \in S$. Then s is integral over R since S is integral over R. Hence 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 $a_0, \ldots, a_{n-1} \in R$. 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. Hence $a_0 \neq 0$. 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, $s \in S^\times$.

$\Longleftarrow$ Assume S is a field. Let $0 \neq r \in R \subseteq S$. Then $r^{-1} \in S$. Note that 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 $a_0, a_1, \ldots, a_{n-1} \in R$. Hence $r^{-1} + \underbrace{a_{n-1} + \cdots + a_1 r^{n-2} + a_0 r^{n-1}}_{\in R} = 0$. Hence $r^{-1} \in R$. □

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 $\varphi : k[X] \to k[X]/(X^2)$, we have an induced ring homomorphism $\varphi|_k : k \to k[X]/(X^2)$. 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. Hence we regard $R := k$ as a subring of $S := k[X]/(X^2)$. Let $x = \overline{X} \in S$. Then x is integral over k since $x^2 = 0$. Hence $S = k[x]$ 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 $\varphi : k[X] \to k[\epsilon]$ given by $f \mapsto f(\epsilon)$ is a ring epimorphism with $\mathrm{Ker}(\varphi) = (X^2)$, so $k[X]/(X^2) \cong k[\epsilon] = k\epsilon + k$.

Corollary 5.25. Let $\mathfrak{q} \in \mathrm{Spec}(S)$ 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. $\mathrm{Spec}(S) \to \mathrm{Spec}(R)$ *given by* $\mathfrak{q} \mapsto \mathfrak{q} \cap R$ *is a surjection, i.e., for* $\mathfrak{p} \in \mathrm{Spec}(R)$, *there exists* $\mathfrak{q} \in \mathrm{Spec}(S)$ *such that* $\mathfrak{p} = \mathfrak{q} \cap R$.

Proof. Let $U = R \smallsetminus \mathfrak{p}$. Consider

$$\begin{tikzcd}
\mathfrak{p} & & & \\
& R \arrow[r, "\subseteq"] \arrow[d, "\psi"] & S \arrow[d, "\rho"] & \\
& U^{-1}R \arrow[r, "\subseteq"] & U^{-1}S & \\
\mathfrak{p}_{\mathfrak{p}} = R_{\mathfrak{p}} \cap Q \arrow[uuu, mapsto] & & & Q \arrow[lll, mapsto]
\end{tikzcd}$$

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 $0 \neq R \subseteq S$, $0 \neq R_{\mathfrak{p}} = U^{-1}R \subseteq U^{-1}S$. Hence 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. Hence $Q \cap R_{\mathfrak{p}} = \mathfrak{p}_{\mathfrak{p}}$. Consider $\psi : R \to U^{-1}R$. Since $U \cap \mathfrak{p} = \emptyset$, by Proposition 3.13, we have that

$$\mathfrak{p} \cdot U^{-1}(U^{-1}R) = \mathfrak{p} \cdot U^{-1}R \neq U^{-1}R = U^{-1}(U^{-1}R).$$

Hence 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 $Q \in \mathrm{Spec}(U^{-1}S)$, $\mathfrak{q} \in \mathrm{Spec}(S)$ by Fact 1.16. $\square$

Proposition 5.27. Let $\mathfrak{q}, \mathfrak{q}' \in \mathrm{Spec}(S)$ 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 $\mathfrak{p} = \mathfrak{q} \cap R = \mathfrak{q}' \cap R \in \mathrm{Spec}(R)$ by Fact 1.16. Let $U = R \smallsetminus \mathfrak{p}$. By prime correspondence for localization,

$$\mathrm{Spec}(U^{-1}S) \leftrightarrow \{\gamma \in \mathrm{Spec}(S) \mid \gamma \cap (R \smallsetminus \mathfrak{p}) = \emptyset\} = \{\gamma \in \mathrm{Spec}(S) \mid \gamma \cap R \subseteq \mathfrak{p}\}$$

given by $U^{-1}\gamma \leftarrow\!\shortmid \gamma$. Hence $U^{-1}\mathfrak{q}, U^{-1}\mathfrak{q}' \in \mathrm{Spec}(U^{-1}S)$. Hence $U^{-1}\mathfrak{q} \cap R_{\mathfrak{p}}, U^{-1}\mathfrak{q}' \cap R_{\mathfrak{p}} \in \mathrm{Spec}(R_{\mathfrak{p}})$.

$$\begin{tikzcd}
\mathfrak{p} \arrow[ddd, mapsto] & & & \mathfrak{q}, \mathfrak{q}' \arrow[lll, mapsto] \arrow[ddd, mapsto] \\
& R \arrow[r, "\subseteq"] \arrow[d, "\psi"] & S \arrow[d, "\rho"] & \\
& U^{-1}R \arrow[r, "\subseteq"] & U^{-1}S & \\
\mathfrak{p}_{\mathfrak{p}} & & & U^{-1}\mathfrak{q}, U^{-1}\mathfrak{q}'
\end{tikzcd}$$

Since $U^{-1}\mathfrak{q}, U^{-1}\mathfrak{q}' \supseteq U^{-1}\mathfrak{p} = \mathfrak{p}_\mathfrak{p}$ and $R_\mathfrak{p} \supseteq \mathfrak{p}_\mathfrak{p}$,

$$R_\mathfrak{p} \supsetneq U^{-1}\mathfrak{q} \cap R_\mathfrak{p}, U^{-1}\mathfrak{q}' \cap R_\mathfrak{p} \supseteq \mathfrak{p}_\mathfrak{p} \in \text{m-Spec}(R_\mathfrak{p}).$$

Hence $U^{-1}\mathfrak{q} \cap R_\mathfrak{p} = \mathfrak{p}_\mathfrak{p} = U^{-1}\mathfrak{q}' \cap R_\mathfrak{p}$.[†] Since $R \subseteq S$ is an integral extension, $U^{-1}R \subseteq U^{-1}S$ is an integral extension by Proposition 5.22(b). Hence 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. ☐

Theorem 5.28 (Going up theorem). *Let $\mathfrak{p}_1 \subseteq \cdots \subseteq \mathfrak{p}_n$ be a chain in* $\operatorname{Spec}(R)$ *and $\mathfrak{q}_1 \subseteq \cdots \subseteq \mathfrak{q}_m$ ($m < n$) be a chain in* $\operatorname{Spec}(S)$ *such that $\mathfrak{p}_i = \mathfrak{q}_i \cap R$ for $i = 1, \ldots, m$. Then there exists a chain $\mathfrak{q}_\mathfrak{m} \subseteq \cdots \subseteq \mathfrak{q}_n$ in* $\operatorname{Spec}(S)$ *such that $\mathfrak{q}_i \cap R = \mathfrak{p}_i$ for $i = 1, \ldots, n$.*

Proof. By induction on $n - m$. It suffices to consider the case $n = 2$ and $m = 1$. Need to find $\mathfrak{q}_2 \in \mathrm{V}(\mathfrak{q}_1) \subseteq \operatorname{Spec}(S)$ such that $\mathfrak{q}_2 \cap R = \mathfrak{p}_2$. Consider

$$\begin{tikzcd}
\mathfrak{p}_2 & & & \mathfrak{q}_2 \arrow[lll, mapsto] \\
& R \arrow[r, "\subseteq"'] \arrow[d, "\pi"] & S \arrow[d, "\tau"'] & \\
& R/\mathfrak{p}_1 \arrow[r, "\subseteq"] & S/\mathfrak{q}_1 & \\
\mathfrak{p}_2/\mathfrak{p}_1 \arrow[uuu, mapsto] & & & \mathfrak{q}_2/\mathfrak{q}_1 \arrow[lll, mapsto] \arrow[uuu, mapsto]
\end{tikzcd}$$

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 $\mathfrak{p}_2/\mathfrak{p}_1 \in \operatorname{Spec}(R/\mathfrak{p}_1)$ by prime correspondence for quotients, there exists $\mathfrak{q}_2/\mathfrak{q}_1 \in \operatorname{Spec}(S/\mathfrak{q}_1)$ such that $(\mathfrak{q}_2/\mathfrak{q}_1) \cap (R/\mathfrak{p}_1) = \mathfrak{p}_2/\mathfrak{p}_1$ by Theorem 5.26.

Note that $x + \mathfrak{p}_1 \in (R \cap \mathfrak{q}_2)/\mathfrak{p}_1$ 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). Hence $(\mathfrak{q}_2 \cap R)/\mathfrak{p}_1 = \mathfrak{p}_2/\mathfrak{p}_1$. Thus, $\mathfrak{q}_2 \cap R = \mathfrak{p}_2$ by prime correspondence for quotients. ☐

Example 5.29. Integral assumption is crucial.

(a) $\mathbb{Z} \subseteq \mathbb{Q}$. Let $0 \subseteq 2\mathbb{Z}$ be a chain in $\operatorname{Spec}(\mathbb{Z})$, Note that 0 is a (unique) chain in $\operatorname{Spec}(\mathbb{Q}) = \{0\}$.

(b) $\mathbb{Z} \subseteq \mathbb{Z}[X]$. Let $0 \subseteq 2\mathbb{Z}$ be a chain in $\operatorname{Spec}(\mathbb{Z})$ and $\langle 2X - 1\rangle$ be a chain in $\operatorname{Spec}(\mathbb{Z}[X])$ since $\frac{\mathbb{Z}[X]}{(2X-1)} \cong \mathbb{Z}_2$[†] $= \mathbb{Z}[\frac{1}{2}] \subseteq \mathbb{Q}$ given by $\overline{X} \mapsto \frac{1}{2}$ and $\mathbb{Z}[\frac{1}{2}]$ is an integral domain. Note that $\mathbb{Z} \cap \langle 2X - 1\rangle = 0$. Suppose there exists $Q \in \operatorname{Spec}(\mathbb{Z}[X])$ such that $\langle 2X - 1\rangle \subseteq Q$ and $\mathbb{Z} \cap Q = 2\mathbb{Z}$. Then $2, 2x - 1 \in Q$. Hence $1 \in Q$, i.e., $Q = \mathbb{Z}[X]$, a contradiction.

This example also shows the need for integral assumption in Proposition 5.27 because

(1) $0, \langle 2X - 1\rangle \in \operatorname{Spec}(\mathbb{Z}[X])$ and $\mathbb{Z} \cap 0 = 0 = \mathbb{Z} \cap \langle 2X - 1\rangle$, but $0 \subsetneq \langle 2X - 1\rangle$;

(2) $\langle 2\rangle, \langle 2, X\rangle \in \operatorname{Spec}(\mathbb{Z}[X])$ 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 $\overline{R}$ 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 $\overline{U^{-1}R} = U^{-1}\overline{R}$.

[†] $U^{-1}\mathfrak{q} \cap R_\mathfrak{p} = U^{-1}\mathfrak{q} \cap U^{-1}R = U^{-1}(\mathfrak{q} \cap R) = U^{-1}\mathfrak{p} = \mathfrak{p}_\mathfrak{p} = U^{-1}\mathfrak{p} = U^{-1}(\mathfrak{q}' \cap R) = U^{-1}\mathfrak{q}' \cap U^{-1}R = U^{-1}\mathfrak{q}' \cap R_\mathfrak{p}$.

[†] $\mathbb{Z}_2$ is the localization of $\mathbb{Z}$ away from 2 while $\mathbb{Z}_{(2)}$ is the localization of $\mathbb{Z}$ at 2.

Proof. "$\supseteq$". Since $R \subseteq \overline{R} \subseteq S$ with $R \subseteq \overline{R}$ integral, we have that $U^{-1}R \subseteq U^{-1}\overline{R} \subseteq U^{-1}S$ with $U^{-1}R \subseteq U^{-1}\overline{R}$ integral by Proposition 5.22(b). Hence $U^{-1}\overline{R} \subseteq \overline{U^{-1}R}$.

"$\subseteq$". Let $\frac{s}{u} \in \overline{U^{-1}R} \subseteq U^{-1}S$. Then

$$0 = \left(\frac{s}{u}\right)^n + \left(\frac{a_{n-1}}{v_{n-1}}\right)\left(\frac{s}{u}\right)^{n-1} + \cdots + \left(\frac{a_1}{v_1}\right)\left(\frac{s}{u}\right) + \left(\frac{a_0}{v_0}\right)$$

in $U^{-1}S$ for some $a_0, \ldots, a_{n-1} \in R$ and $v_0, \ldots, v_{n-1} \in U$. Let $v := v_0 \cdots v_{n-1} \in U$ and multiply the equation by $(uv)^n$,

$$0 = (vs)^n + \underbrace{\left(u\frac{v}{v_{n-1}}a_{n-1}\right)}_{b_{n-1}\in R}(vs)^{n-1} + \cdots + \underbrace{\left(u^{n-1}\frac{v^{n-1}}{v_1}a_1\right)}_{b_1\in R}(vs) + \underbrace{\left(u^n\frac{v^n}{v_0}a_0\right)}_{b_0\in R}$$

in $U^{-1}R$. Hence there exists $w \in U \subseteq R$ such that

$$0 = w^n \cdot 0 = (wvs)^n + (\underbrace{wb_{n-1}}_{\in R})(wvs)^{n-1} + \cdots + (\underbrace{w^{n-1}b_1}_{\in R})(wvs) + (\underbrace{w^n b_0}_{\in R}).$$

Hence $wvs \in \overline{R}$. Thus, $\frac{s}{u} = \frac{wvs}{wvu} \in U^{-1}\overline{R}$. $\square$

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 that $Q(R) = k(X, Y) = Q(k[X, Y])$. Since X, Y satisfies $Z^2 - X^2, Z^2 - Y^2 \in R[Z]$, respectively, we have that 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.

We claim that $R \cong \frac{k[U,V,W]}{\langle V^2 - UW\rangle}$. Let $\varphi : k[U, V, W] \to k[X, Y]$ be a ring homomorphism given by $U \mapsto X^2$, $V \mapsto XY$ and $W \mapsto Y^2$. Then $\mathrm{Im}(\varphi) = k[X^2, XY, Y^2]$ and $\langle V^2 - UW\rangle \subseteq \mathrm{Ker}(\varphi)$. Let $f \in \mathrm{Ker}(\varphi)$. 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 φ is a ring homomorphism, $((XY)^2 - X^2Y^2)\varphi(q) + \varphi(r) = 0$, i.e., $\varphi(r) = 0$. Note that $r = aV + b$ for some $a, b \in k[U, W]$. Hence $a(X^2, Y^2)XY + b(X^2, Y^2) = 0$. Hence $a = 0 = b$, i.e., $r = 0$. Hence $f \in \langle V^2 - UW\rangle$.

Example. If S is noetherian, then R is not necessarily noetherian. Let $\overline{\mathbb{Q}}$ be the algebraic closure of $\mathbb{Q}$ in $\mathbb{C}$ and $R := \mathbb{Q} + X\overline{\mathbb{Q}}[X] \subseteq \overline{\mathbb{Q}}[X] =: S$. Note that $R \subseteq S$ is an integral extension since $\overline{\mathbb{Q}}$ is algebraic over $\mathbb{Q} \subseteq R$ and $X \in R$, but R is not noetherian since $[\overline{\mathbb{Q}} : \mathbb{Q}] = \infty$.

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 that $R \smallsetminus \mathfrak{m} \subseteq \mathrm{NZD}(R)$. Hence $R \subseteq R_{\mathfrak{m}} \subseteq Q(R)$ 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 $\mathfrak{m} \in \text{m-Spec}(R)$. Hence $I \cap (R \smallsetminus \mathfrak{m}) \neq \emptyset$, 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, $x = 1 \cdot x \in R$. ☐

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

(iv) $R_{\mathfrak{m}}$ is integrally closed for $\mathfrak{m} \in \text{m-Spec}(R)$.

Proof. (i)$\Longrightarrow$(ii) Assume R is integrally closed. Let $U \subseteq R$ be multiplicatively closed with $0 \notin U$. Since R is an integral domain and $0 \notin U$, $U \subseteq \mathrm{NZD}(R)$. Hence $R \subseteq U^{-1}R \subseteq Q(R) =: S$ are subrings. By Proposition 5.30, $\overline{U^{-1}R} = U^{-1}\overline{R} = U^{-1}R$ since R is integral closed in $Q(R)$. Hence $U^{-1}R$ is integrally closed in $U^{-1}S = Q(R)$. Also, since $Q(U^{-1}R) = Q(R)$[†], $U^{-1}R$ is integrally closed.

(ii)$\Longrightarrow$(iii) and (iii)$\Longrightarrow$(iv) Done.

(iv)$\Longrightarrow$(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 $x \in \overline{R}$, where $\overline{R}$ 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 $\mathfrak{m} \in \text{m-Spec}(R)$. Hence $x \in \overline{R_{\mathfrak{m}}} = R_{\mathfrak{m}}$ for $\mathfrak{m} \in \text{m-Spec}(R)$. Thus, by Lemma 5.33, $x \in \bigcap_{\mathfrak{m}\in\text{m-Spec}(R)} R_{\mathfrak{m}} = R$. ☐

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 $a_0, \ldots, a_{n-1} \in \mathfrak{a}$.

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 $\overline{R}$ be the integral closure of R in S and $\mathfrak{a} \leq R$. Then $\bar{\mathfrak{a}} = \mathrm{rad}(\mathfrak{a}\overline{R}) \leq \overline{R}$. Hence $\bar{\mathfrak{a}}$ 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 $a_0, \ldots, a_{n-1} \in \mathfrak{a}$. Hence $s^n = -(a_{n-1}s^{n-1} + \cdots + a_0) \in \mathfrak{a}\bar{\mathfrak{a}} \subseteq \mathfrak{a}\overline{R}$. Hence $s \in \mathrm{rad}(\mathfrak{a}\overline{R})$.

"$\supseteq$". Let $t \in \mathrm{rad}(\mathfrak{a}\overline{R})$. Then $t^n \in \mathfrak{a}\overline{R}$ for some $n \geq 1$. Hence $t^n = \sum_{i=1}^m \alpha_i s_i$ for some $m \geq 1$, $\alpha_1, \ldots, \alpha_m \in \mathfrak{a}$ and $s_1, \ldots, s_m \in \overline{R}$. Let $T := R[s_1, \ldots, s_m] \subseteq \overline{R} \subseteq S$. Then $t^n \in \mathfrak{a}T$. Hence $t^nT \subseteq \mathfrak{a}T$. Since $s_1, \ldots, s_m$ 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 that t^n is integral over $\mathfrak{a}$. Hence $(t^n)^\ell + b_{\ell-1}(t^n)^{\ell-1} + \cdots + b_0 = 0$ for some $\ell \geq 1$ and $b_0, \ldots, b_{\ell-1} \in \mathfrak{a}$. Hence t is integral over $\mathfrak{a}$. ☐

[†]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 $c_0, \ldots, c_{m-1} \in \operatorname{rad}(\mathfrak{a})$.

Proof. Let $s_1 := s, s_2, \ldots, s_m$ 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 $i = 1, \ldots, m$. Since $g(X) = (X - s_1)\cdots(X - s_m)$ and $\bar{\mathfrak{a}} \leq \overline{R}$ by Lemma 5.37, $c_0, \ldots, c_{m-1} \in \bar{\mathfrak{a}} = \operatorname{rad}(\mathfrak{a}\overline{R}) = \operatorname{rad}(\mathfrak{a}R) = \operatorname{rad}(\mathfrak{a})$. □

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* $\operatorname{Spec}(R)$ *and $\mathfrak{q}_1 \supseteq \cdots \supseteq \mathfrak{q}_m$ $(m < n)$ be a chain in* $\operatorname{Spec}(S)$ *such that $\mathfrak{q}_i \cap R = \mathfrak{p}_i$ for $i = 1, \ldots, m$. Then there exists a chain $\mathfrak{q}_m \supseteq \cdots \supseteq \mathfrak{q}_n$ in* $\operatorname{Spec}(S)$ *such that $\mathfrak{q}_i \cap R = \mathfrak{p}_i$ for $i = 1, \ldots, n$.*

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 $\operatorname{Spec}(R)$ and $\mathfrak{q} \in \operatorname{Spec}(S)$ such that $\mathfrak{q} \cap R = \mathfrak{p}$. Since S is an integral domain, $S \smallsetminus \mathfrak{q} \subseteq \operatorname{NZD}(S)$. Hence $S_\mathfrak{q} \supseteq S \supseteq R$. We claim that $(\mathfrak{p}'S_\mathfrak{q}) \cap R = \mathfrak{p}'$, then (if and only if) there exists $Q' \in \operatorname{Spec}(S_\mathfrak{q})$ such that $Q' \cap R = \mathfrak{p}'$ by Theorem 3.24, so (if and only if) there exists $\mathfrak{q} \supseteq \mathfrak{q}' \in \operatorname{Spec}(S)$ such that $\mathfrak{q}' \cap R = \mathfrak{p}'$[†] by prime correspondence for localization.

"$\supseteq$". By 1.63(a).

"$\subseteq$". Let $0 \neq x \in (\mathfrak{p}'S_\mathfrak{q}) \cap R$. Then $x \in \mathfrak{p}'S_\mathfrak{q} = \mathfrak{p}'(S \smallsetminus \mathfrak{q})^{-1}S = (S \smallsetminus \mathfrak{q})^{-1}(\mathfrak{p}'S)$. Hence $x = \frac{s}{v}$ for some $s \in \mathfrak{p}'S$ and $v \in S \smallsetminus \mathfrak{q}$. Since $R \subseteq S$ is integral, $\overline{R} = S$, where $\overline{R}$ is the integral closure of R in S. Hence $s \in \mathfrak{p}'S \subseteq \operatorname{rad}(\mathfrak{p}'S) = \operatorname{rad}(\mathfrak{p}'\overline{R}) = \overline{\mathfrak{p}'}$ 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, $u_0, \ldots, u_{r-1} \in \operatorname{rad}(\mathfrak{p}') = \mathfrak{p}'$. Since $0 \neq x = \frac{s}{v}$ and R is an integral domain, $v = sx^{-1}$ in $Q(R)$. Note that 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 that $t_0, \ldots, t_{r-1} \in \operatorname{rad}(\langle 1\rangle R) = R$. Suppose $x \notin \mathfrak{p}'$. Since $u_i = t_ix^{r-i} \in \mathfrak{p}' \in \operatorname{Spec}(R)$, $t_i \in \mathfrak{p}'$ for $i = 0, \ldots, r-1$. Hence $v^r = -(t_{r-1}v^{r-1} + t_{r-2}v^{r-2} + \cdots + t_0) \in \mathfrak{p}'S \subseteq \mathfrak{p}S = (\mathfrak{q} \cap R)S \subseteq \mathfrak{q}S = \mathfrak{q} \in \operatorname{Spec}(S)$. Hence $v \in \mathfrak{q}$, a contradiction. Thus, $x \in \mathfrak{p}'$. □

Theorem 5.40 (Noether normalization)**.** *Let k be a field and $k \subseteq R := k[x_1, \ldots, x_n]$ be a subring.*

(a) There exist an intermediate subring $k \subseteq S \subseteq R$ and $y_1, \ldots, y_d \in R$ such that $S = k[y_1, \ldots, y_d] \cong k[Y_1, \ldots, Y_d]$, a polynomial ring, with $d \leq n$ and R integral over S. Hence $R = S[x_1, \ldots, x_n]$ is a finitely generated S-module. Moreover, y_i is a polynomial in x_j's with coefficients in k for $i = 1, \ldots, d$.

(b) If $|k| = \infty$, then we can take some d and $y_i = \sum_{j=1}^n a_{ij}x_j$ for some $a_{i1}, \ldots, a_{in} \in k$ for $i = 1, \ldots, d$.

[†]For $\Longrightarrow$, take $\mathfrak{q}' = Q' \cap S$, then $\mathfrak{q}' \cap R = (Q' \cap S) \cap R = Q' \cap R = \mathfrak{p}'$. For $\Longleftarrow$, 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.

(In fact, d is uniquely determined and is the Krull dimension of R.)

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 $k[Z_1, \dots, Z_m] \overset{n}{\twoheadrightarrow} k[z_1, \dots, z_m]$ 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 $n = 1$: $R = k[x] \overset{n}{\twoheadleftarrow} k[X]$. 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 $S = R = k[x_1, \dots, x_n] \underset{\cong}{\overset{n}{\longleftarrow}} k[X_1, \dots, X_n]$. 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 $k[X_1, \dots, X_n] \overset{n}{\twoheadrightarrow} k[x_1, \dots, x_n]$. Then there exists $0 \neq F \in k[X_1, \dots, X_n]$ such that $n(F) = 0$. Let $e = \deg(F)$ and write $F = F_0 + F_1 + \cdots + F_e$, 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 $\underline{b} = (b_1, \dots, b_n) \in \mathbb{Z}^n_{\geq 0}$, $(w_1 + \lambda_1 x_n)^{b_1} \cdots (w_{n-1} + \lambda_{n-1} x_n)^{b_{n-1}} \cdot x_n^{b_n} = \lambda_1^{b_1} \cdots \lambda_{n-1}^{b_{n-1}} x_n^{|\underline{b}|} +$ lower degree terms in x_n, where $|\underline{b}| = b_1 + \cdots + b_n$. Note that for $i = 0, \dots, e$,

$$\begin{aligned} F_i(w_1 + \lambda_1 x_n, \dots, w_{n-1} + \lambda_{n-1} x_n, x_n) &= \sum_{|\underline{b}| = i} a_{\underline{b}} (\lambda_1^{b_1} \cdots \lambda_{n-1}^{b_{n-1}}) x_n^i + \text{lower degree terms in } x_n \\ &= F_i(\lambda_1, \dots, \lambda_{n-1}, 1) x_n^i + \text{lower degree terms in } x_n. \end{aligned}$$

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

$$\begin{aligned} G(w_1, \dots, w_{n-1}, x_n) &= F(x_1 - \lambda_1 x_n + \lambda_1 x_n, \dots, x_{n-1} - \lambda_{n-1} x_n + \lambda_{n-1} x_n, x_n) \\ &= F(x_1, \dots, x_{n-1}, x_n) = n(F) = 0. \end{aligned}$$

Since $F_e(\lambda_1, \dots, \lambda_{n-1}, 1) \neq 0$, x_n satisfies a monic $\frac{G(w_1, \dots, w_{n-1}, X_n)}{F_e(\lambda_1, \dots, \lambda_{n-1}, 1)} \in k[w_1, \dots, w_{n-1}][X_n]$. Hence x_n is integral over $k[w_1, \dots, w_{n-1}]$. Hence

$$R = k[x_1, \dots, x_{n-1}, x_n] = k[x_1 - \lambda x_n, \dots, x_{n-1} - \lambda_{n-1} x_n, x_n] = k[w_1, \dots, w_{n-1}][x_n]$$

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 $\underline{b} = (b_1, \dots, b_n) \in \mathbb{Z}^n_{\geq 0}$ and $e_1, \dots, e_{n-1} \gg 1$,

$$(w_1 + x_n^{e_1})^{b_1} \cdots (w_{n-1} + x_n^{e_{n-1}})^{b_{n-1}} \cdot x_n^{b_n} = x_n^{\sum_{i=1}^n e_i b_i} + \text{lower degree terms in } x_n.$$

Write $F = \sum_{j=1}^m a_j \underline{x}^{\underline{b}_j}$ for some $m \geq 1$ and distinct $\underline{x}^{\underline{b}_j} := x_1^{b_{j_1}} \cdots x_n^{b_{j_n}}$ and $a_j \neq 0$ for $j = 1, \ldots, m$. Let $A_i = \max\{b_{1_i}, \ldots, b_{m_i}\} - \min\{b_{1_i}, \ldots, b_{m_i}\}$ for $i = 1, \ldots, n$. Choose $e_{i-1} > A_i e_i + \cdots + A_n e_n$ for $i = 2, \ldots, n$. Re-order $a_1 \underline{x}^{\underline{b}_1}, \ldots, a_m \underline{x}^{\underline{b}_m}$ such that $\underline{b}_1 \succcurlyeq \cdots \succcurlyeq \underline{b}_m$ is in reverse lexicographical order. Then $\sum_{i=1}^n e_i b_{1_i} > \sum_{i=1}^n e_i b_{2_i} > \cdots > \sum_{i=1}^n e_i b_{m_i}$. Let

$$\begin{aligned} G(w_1, \ldots, w_{n-1}, x_n) &= F(w_1 + x_n^{e_1}, \ldots, w_{n-1} + x_n^{e_{n-1}}, x_n) \\ &= a_1 x_n^{\sum_{i=1}^n e_i b_{1_i}} + \text{lower degree terms in } x_n. \end{aligned}$$

Let $w_i := x_i - x_n^{e_i}$ for $i = 1, \ldots, n-1$. Then $G(w_1, \ldots, w_{n-1}, x_n) = F(x_1, \ldots, x_{n-1}, x_n) = n(F) = 0$. Since $a_1 \neq 0$, x_n satisfies a monic $\frac{G(w_1, \ldots, w_{n-1}, X_n)}{a_1} \in k[w_1, \ldots, w_{n-1}][X_n]$. Hence x_n is integral over $k[w_1, \ldots, w_{n-1}]$. Hence

$$R = k[x_1, \ldots, x_{n-1}, x_n] = k[x_1 - x_n^{e_1}, \ldots, x_{n-1} - x_n^{e_{n-1}}, x_n] = k[w_1, \ldots, w_{n-1}][x_n]$$

is integral over $k[w_1, \ldots, w_{n-1}]$ by Theorem 5.19. □

Theorem 5.41 (Hilbert Nullstellensatz, version 1)**.** *Let $k \subseteq K := k[x_1, \ldots, x_n]$ 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 $y_1, \ldots, y_d \in K$ such that $S = k[y_1, \ldots, y_d] = k[Y_1, \ldots, Y_d] \subseteq K$ and K is integral over $k[Y_1, \ldots, Y_d]$. Since K is a field, by Proposition 5.24, $k[Y_1, \ldots, Y_d]$ is a field. Hence $d = 0$. Then $S = k$. Hence $K = k[x_1, \ldots, x_n]$ 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. Hence $K = k$. □

Theorem 5.42 (Hilbert Nullstellensatz, version 2)**.** *Let k be an algebraically closed field, $R = k[X_1, \ldots, X_n]$ and $\mathfrak{m} \in \text{m-Spec}(R)$. Then there exists $\underline{a} \in k^n$ such that $\mathfrak{m} = \langle X_1 - a_1, \ldots, X_n - a_n \rangle$.*

Proof. Set $K = R/\mathfrak{m} = k[x_1, \ldots, x_n] \hookleftarrow k$, where $x_i = \overline{X_i} \in R/\mathfrak{m}$ for $i = 1, \ldots, n$. Since k is algebraically closed and $k \hookrightarrow K$ is a subfield, by Hilbert Nullstellensatz, version 1(b), $k \hookrightarrow k[x_1, \ldots, x_n] = R/\mathfrak{m}$ is onto. Since $x_i \in R/\mathfrak{m}$, there exists $a_i \in k$ such that $a_i \mapsto x_i$ for $i = 1, \ldots, n$. Hence $x_i - a_i = 0$ in $R/\mathfrak{m}$, i.e., $X_i - a_i \in \mathfrak{m}$ for $i = 1, \ldots, n$. Then $\mathfrak{m} \supseteq \langle X_1 - a_1, \ldots, X_n - a_n \rangle$. Since $\mathfrak{m}, \langle X_1 - a_1, \ldots, X_n - a_n \rangle \in \text{m-Spec}(R)$, $\mathfrak{m} = \langle X_1 - a_1, \ldots, X_n - a_n \rangle$. □

Theorem 5.43 (Hilbert Nullstellensatz, version 3)**.** *Let k be an algebraically closed field, $\mathfrak{a} \lneq R = k[X_1, \ldots, X_n]$. Then $\mathrm{Z}(\mathfrak{a}) := \{\underline{a} \in k^n \mid F(\underline{a}) = 0, \forall F \in \mathfrak{a}\} \neq \emptyset$.*

Proof. Since $\mathfrak{a} \neq R$, by Hilbert Nullstellensatz, version 2, $\mathfrak{a} \subseteq \mathfrak{m} := \langle X_1 - a_1, \ldots, X_n - a_n \rangle$ 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 $g_1, \ldots, g_n \in R$. Hence $F(\underline{a}) = \sum_{i=1}^n g_i(\underline{a})(a_i - a_i) = 0$. Thus, $\underline{a} \in \mathrm{Z}(\mathfrak{a})$. □

Theorem 5.44 (Hilbert Nullstellensatz, version 4)**.** *Let k be an algebraically closed field, $\mathfrak{a} \lneq R = k[X_1, \ldots, X_n]$ and $Z = \mathrm{Z}(\mathfrak{a})$. Let $I = \mathrm{I}(Z) = \{F \in R \mid F(\underline{a}) = 0, \forall \underline{a} \in Z\} \leq R$. Then $I = \mathrm{rad}(\mathfrak{a})$.*

Proof. "$\supseteq$". Since

$$I = \mathrm{I}(Z) = \mathrm{I}(\mathrm{Z}(\mathfrak{a})) = \{F \in R \mid F(\underline{a}) = 0, \forall \underline{a} \in \mathrm{Z}(\mathfrak{a})\} \supseteq \mathfrak{a},$$

$\mathrm{rad}(\mathfrak{a}) \subseteq \mathrm{rad}(I) = I$.

"$\subseteq$". Let $F \in R \smallsetminus \mathrm{rad}(\mathfrak{a})$. Then $F \notin \mathrm{rad}(\mathfrak{a}) = \bigcap_{\mathfrak{p} \in \mathrm{V}(\mathfrak{a})} \mathfrak{p}$ by Fact 1.58. Hence there exists $\mathfrak{p} \in \mathrm{V}(\mathfrak{a})$ such that $F \notin \mathfrak{p}$. Set $\overline{R} = R/\mathfrak{p} = k[x_1, \ldots, x_n]$, an integral domain, where $x_i = \overline{X_i} \in R/\mathfrak{p}$ for $i = 1, \ldots, n$. Since $F \notin \mathfrak{p}$, $f := \overline{F} \neq 0$ in $\overline{R}$. Then $0 \neq \overline{R} \subseteq \overline{R}_f = \overline{R}[1/f] = k[x_1, \ldots, x_n, 1/f]$. Hence there exists $\mathfrak{m} \in \text{m-Spec}(\overline{R}_f)$. Consider $k \hookrightarrow \overline{R}_f/\mathfrak{m} = k[\overline{x_1}, \ldots, \overline{x_n}, \overline{1/f}]$, 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 $i = 1, \ldots, n$. Since $\mathfrak{a} \subseteq \mathfrak{p}$, $\mathfrak{a} \cdot \overline{R} = 0$. Hence $\mathfrak{a} \cdot \overline{R}_f/\mathfrak{m} = 0$. Then $G(\underline{a}) = \bar{g}(\overline{x_1}, \ldots, \overline{x_n}) = \bar{g} = 0$ in $\overline{R}_f/\mathfrak{m}$ for all $G \in \mathfrak{a}$. Hence $\underline{a} \in \mathrm{Z}(\mathfrak{a}) = Z$. Also, since $F(\underline{a}) = \overline{f}(\overline{x_1}, \ldots, \overline{x_n}) = \overline{f} \neq 0$ in $\overline{R}_f/\mathfrak{m}$, we have that $F \notin \mathrm{I}(Z) = I$. $\square$