Commutative Algebra

September 22, 2018

Contents

Introduction

The study and application of commutative rings with identity (CRW1).

1. AC in calculus. $\mathcal{C}(\mathbb{R}) = \{\text{continuous functions } \mathbb{R} \to \mathbb{R}\}$, $\mathcal{D}(\mathbb{R}) = \{\text{differentiable functions } \mathbb{R} \to \mathbb{R}\}$ are both CRW1's.

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

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

3. AC in CO (combinatorics). A simplicial complex Δ on V. Stanley-Reisner ideal $\mathrm{J}(\Delta) \leq K[v_1, \cdots, v_d]$.

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

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

4. AC in NT (number theory). NT is the study of solutions of polynomial equations over $\mathbb{Z}$. Given an intermediate field $\mathbb{Q} \subseteq K \subseteq \mathbb{C}$, let $R = \{\alpha \in K \mid \exists \text{ monic } f \in \mathbb{Z}[x] \text{ s.t. } f(\alpha) = 0\}$. Then $\mathbb{Z} \subseteq R \subseteq K$ and R is a subring of K. (Chapter 5)

5. AC in AG (algebraic geometry). AG is the study of solution sets for systems of polynomial equations over fields. Let k be a field, $f_1, \cdots, f_m \in k[X_1, \cdots, X_d]$, $V := \mathrm{V}(f_1, \cdots, f_m) = \{\underline{x} \in k^d \mid f_i(\underline{x}) = 0,\ \forall\ i = 1, \cdots, m\}$, where V for "variety", and $\mathrm{I}(V) = \{f \in k[X_1, \cdots, X_d \mid f(\underline{x}) = 0,\ \forall\ \underline{x} \in V\} \leq k[X_1, \cdots, X_d]$.

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

Why modules? b/c in NT, $R = \{\alpha \in K \mid \exists \text{ monic } f \in \mathbb{Z}[x] \text{ s.t. } f(\alpha) = 0\}$ is a subring of K.
Challenge-exercise: prove this by definition. Let $\alpha, \beta \in R$. Then there exist $f, g \in \mathbb{Z}[X]$ monic such that $f(\alpha) = 0 = f(\beta)$. Prove/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 straight forward application of modules.

Why topology? To study geometry, need continuity. Let $V = \mathrm{V}(f_1, \cdots, f_m)$, $W = \mathrm{V}(g_1, \cdots, g_n)$ 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

1.1 Rings and Ring Homomorphisms

Let R be a CRW1.

Fact 1.1. $R = 0$ iff $1_R = 0_R$.

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

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

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

Definition 1.3. A homomorphism of CRW1's is a function $\phi : R \to S$, where R and S are CRW1's, such that

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

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

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

A.K.A. a 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 any $r \in R$.

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

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

(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 CRW1 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 iff 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. $R = \mathbb{F}_3 \times \mathbb{F}_3 \supseteq \{(a,a) \mid a \in \mathbb{F}_3\} =: S$. 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.

1.2 Ideals and Quotient Rings

Definition 1.9. An *ideal* of R is a non-empty subset $\mathfrak{a} \subseteq R$ and a subgroup under addition such that for any $r \in R$ and any $a \in \mathfrak{a}$, $ra \in \mathfrak{a}$.
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 $\cdot$, then for any $a \in \mathfrak{a}$, $-a = (-1_R)a \in \mathfrak{a}$, also, since $\mathfrak{a}$ is closed under $+$, it is automatically closed under $-$.
Thus, A subset $\mathfrak{a} \subseteq R$ is an ideal iff $\mathfrak{a} \neq \emptyset$ and $\mathfrak{a}$ is closed under $+$ and $\cdot$.

Example 1.11. (a) Let $R = \mathbb{Z}$, then ideals of R are $n\mathbb{Z} = \{nm \mid m \in \mathbb{Z}\}$, where $n \in \mathbb{Z}$.
$n\mathbb{Z}$ is prime iff $n = 0$ or $|n|$ is prime.
$n\mathbb{Z}$ is maximal iff $|n|$ is prime.

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

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

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

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

(d) If $A \subseteq R$, then $\langle A \rangle = \bigcap_{A \subseteq I \leq R} I$ and $\langle A \rangle = RAR = AR = RA = \{\sum_{a \in A}^{\text{finite}} r_a a \mid r_a \in R,\ \forall\ a\}$.

Fact 1.12. For any $r_1, \cdots, r_m \in R$, $\langle r_1, \cdots, r_m \rangle$ is the smallest ideal of R containing $r_1, \cdots, r_m$, i.e., for any $\mathfrak{a} \leq R$, $r_1, \cdots, r_m \in \mathfrak{a}$ iff $\langle r_1, \cdots, r_m \rangle \subseteq \mathfrak{a}$. Similarly, $A \subseteq \mathfrak{a}$ iff $\langle A \rangle \subseteq \mathfrak{a}$. For example, 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 CRW1 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.

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

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 diagram commute, where $\overline{\phi}(\bar{r}) = \overline{\phi}(\pi(r)) = \phi(r)$.
Note $\phi(\mathfrak{a}) = 0$ iff $\mathfrak{a} \subseteq \mathrm{Ker}(\phi)$. In particular, if $\mathfrak{a} = \langle A \rangle$, then $\mathfrak{a} \subseteq \mathrm{Ker}(\phi)$ iff $A \subseteq \mathrm{Ker}(\phi)$.

1.3 Prime Ideals and Maximal Ideals

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

(a) $\mathfrak{a}$ is prime iff $R/\mathfrak{a}$ is an integral domain.

(b) $\mathfrak{a}$ is maximal iff $R/\mathfrak{a}$ is a field.

(c) If R is a field, then it is an integral domain. So if $\mathfrak{a}$ is maximal, then $\mathfrak{a}$ is prime.

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

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

In both R and $R/\mathfrak{a}$, maximal ideals are a subset of prime ideals and prime ideals are a proper subset of ideals.
Claim $\frac{R/\mathfrak{a}}{J/\mathfrak{a}} \cong \frac{R}{J}$.

$$\begin{tikzcd} R \arrow[r, two heads, "p"] \arrow[d, two heads, "\pi"] & R/\mathfrak{a} \arrow[r, two heads, "\tau"] & \frac{R/\mathfrak{a}}{J/\mathfrak{a}} \\ R/J \arrow[urr, hook, two heads, dashed, "\exists\,!\,\overline{\phi}"'] & & \end{tikzcd}$$

Clearly $J \subseteq \mathrm{Ker}(\tau \circ p)$, so we can use the UMP.
Since the diagram commutes, $J = \mathrm{Ker}(\pi) = \mathrm{Ker}(\pi \circ p)$.
So the kernel is "modulo out" by π and hence $\overline{\phi}$ is 1-1.
Since $\tau \circ p$ is onto and the diagram commutes, $\overline{\phi}$ is onto.
Note $\overline{\phi}(\bar{r}) = \bar{\bar{r}}$, i.e., $\overline{\phi}(r + J) = (r + \mathfrak{a}) + J/\mathfrak{a}$.

Notation. $\mathrm{Spec}(R) = \{\text{primes ideals of } R\}$, called the *prime spectrum of* R.
$\mathrm{V}(\mathfrak{a}) = \{\mathfrak{p} \in \mathrm{Spec}(R) \mid \mathfrak{p} \supseteq \mathfrak{a}\}$.

Fact 1.16. Let $\phi : R \to S$ be a ring homomorphism. Then $\mathrm{Ker}(\phi) \leq R$, $\mathrm{Im}(\phi) \subseteq S$ is a subring and $\mathrm{Im}(\phi) \cong R/\mathrm{Ker}(\phi)$.
If S is an integral domain, then so is $\mathrm{Im}(\phi)$. Hence $\mathrm{Ker}(\phi)$ is prime.
More generally, for any $\mathfrak{b} \leq S$, we have $\phi^{-1}(\mathfrak{b}) = \{x \in R \mid \phi(x) \in \mathfrak{b}\} \leq R$.

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

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

Example. Let $\phi : \mathbb{Z} \to \mathbb{Q}$ be an inclusion map. Note $\mathfrak{q} := (0)\mathbb{Q} \leq \mathbb{Q}$ is maximal, but $\phi^{-1}(\mathfrak{q}) = \phi^{-1}(0) = \mathrm{Ker}(\phi) = 0\mathbb{Z}$, which is not maximal in $\mathbb{Z}$.

Fact 1.17. (a) If $R \neq 0$, then R has a maximal ideal $\mathfrak{m}$. 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, $\mathrm{V}(\mathfrak{a}) = \{\mathfrak{p} \in \mathrm{Spec}(R) \mid \mathfrak{p} \supseteq \mathfrak{a}\} \neq \emptyset$.

(b) Let $\mathfrak{a} \lneq R$. Then $0 \neq R/\mathfrak{a}$ is a CRW1. So $R/\mathfrak{a}$ has a maximal ideal and this ideal corresponds for quoitients, hence it is of the form $\mathfrak{m}/\mathfrak{a}$, where $\mathfrak{m}$ is the maximal ideal of R containing $\mathfrak{a}$.

Definition 1.18. R is *local* if it has a unique maximal ideal $\mathfrak{m}$. A.K.A. *"quasi-local"*. The *residue field* of R is $R/\mathfrak{m}$.
Shorthand, assume $(R, \mathfrak{m}, k)$ is local, where $\mathfrak{m}$ is the unique maximal ideal of R and $k = R/\mathfrak{m}$.
Or assume $(R, \mathfrak{m})$ is local.

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

(b) Let $n \in \mathbb{N}$ and p be prime in $\mathbb{Z}$. Note $0 \neq \mathbb{Z}/\langle p^n \rangle$ has a maximal ideal $\mathfrak{m} = \langle p \rangle/\langle p^n \rangle$, where $\langle p \rangle$ is a 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. So $\langle p \rangle = \langle \mathfrak{m}_1 \rangle$. 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 $\mathrm{Spec}(\mathbb{Z}/\langle p^n \rangle) = \{\langle p \rangle/\langle p^n \rangle\}$.

(c) Let k be a field. Then $R = k[X]/\langle X^n \rangle$ is local with $\mathfrak{m} = \langle X \rangle/\langle X^n \rangle$. In fact, $\mathrm{Spec}(R) = \{\langle X \rangle/\langle X^n \rangle\}$.

(d) Let k be a field and $R = \frac{k[X_1, \cdots, X_d]}{\langle X_1^{a_1}, \cdots, X_d^{a_d} \rangle}$, where $a_i \in \mathbb{N}$ for any $i = 1, \cdots, d$. Then R is local with $\mathfrak{m} = \langle X_1, \cdots, X_d \rangle/\langle X_1^{a_1}, \cdots, X_d^{a_d} \rangle$. In fact, $\mathrm{Spec}(R) = \left\{ \frac{\langle X_1, \cdots, X_d \rangle}{\langle X_1^{a_1}, \cdots, X_d^{a_d} \rangle} \right\}$.

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 $\frac{R/\mathfrak{a}}{\mathfrak{m}/\mathfrak{a}} \cong R/\mathfrak{m}$ canonically isomorphic residue fields. Converse fails in general by Example 1.19.

1.4 Units, Nilradical and Jacobson Radical

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

Proposition 1.22. TFAE.

(i) R is local.

(ii) $R \setminus R^\times \lneq R$.

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

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

Proof. "(i)⇒(ii)". Assume $(R, \mathfrak{m})$ is local. Claim $\mathfrak{m} = R \setminus R^\times$. It suffices to show $R \setminus \mathfrak{m} = R^\times$.
"⊇". Let $u \in R^\times$. Then $\langle u \rangle = R$ and so $u \notin \mathfrak{m} \lneq R$, i.e., $u \in R \setminus \mathfrak{m}$. Hence $R^\times \subseteq R \setminus \mathfrak{m}$.
"⊆". Let $x \in R \setminus R^\times$. 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, $R \setminus R^\times \subseteq \mathfrak{m}$, i.e., $R \setminus \mathfrak{m} \subseteq R^\times$.
"(ii)⇒(iii)". Assume $R \setminus R^\times \lneq R$. Set $\mathfrak{a} = R \setminus R^\times$. Then $R \setminus \mathfrak{a} = R^\times$.
"(iii)⇒(i)". Let $\mathfrak{a} \lneq R$ such that $R \setminus \mathfrak{a} \subseteq R^\times$. Claim, $\mathfrak{a} = R \setminus R^\times$. Clearly $\mathfrak{a} \supseteq R \setminus R^\times$. On the other hand (OTOH), let $a \in \mathfrak{a} \lneq R$, then $a \notin R^\times$ since $\mathfrak{a} \lneq R$, so $a \in R \setminus R^\times$ and hence $\mathfrak{a} \subseteq R \setminus R^\times$. Thus, $\mathfrak{a} = R \setminus R^\times$. Let $\mathfrak{n} \lneq R$ be maximal and $y \in \mathfrak{n}$. Then $y \notin R^\times$. So $y \in R \setminus R^\times = \mathfrak{a}$. Thus, $\mathfrak{n} \subseteq \mathfrak{a} \lneq R$. Since $\mathfrak{n}$ is maximal, $\mathfrak{n} = \mathfrak{a}$. Thus, $\mathfrak{a}$ is the unique maximal ideal in R and so R is local. □

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

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

Definition 1.24. $x \in R$ is *nilpotent* if there exists $n \in \mathbb{N}$ such that $x^n = 0$. Then *nilradical* of R is $\mathrm{Nil}(R) = \mathrm{N}(R) = \mathfrak{N}_R = \mathfrak{N} = \{\text{nilpotent elements of } R\}$.

Example 1.25. In $\mathbb{Z}/\langle p^n \rangle$, $\bar{p}$ is nilpotent. It is similar in $k[x]/\langle x^n \rangle$ and $k[x_1, \cdots, x_n]/\langle x_1^{a_1}, \cdots, x_d^{a_d} \rangle$, where k is a field.

Proposition 1.26. (a) $\mathrm{Nil}(R) \leq R$.

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

(c) $\mathrm{Nil}(R) = R$ iff $R = 0$.

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

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

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

(c) Since $1 \in \operatorname{Nil}(R)$,, there exists $n \in \mathbb{N}$ such that $1 = 1^n = 0$. So $R = 0$.

(d) "$\subseteq$". Let $x \in \operatorname{Nil}(R)$. Then there exists $n \in \mathbb{N}$ such that $x^n = 0 \in \mathfrak{p}$ for any $\mathfrak{p} \in \operatorname{Spec}(R)$. So $x \in \mathfrak{p}$ for any $p \in \operatorname{Spec}(R)$. Thus, $x \in \bigcap_{\mathfrak{p}\in\operatorname{Spec}(R)} \mathfrak{p}$.
"$\supseteq$". Let $x \in R \setminus \operatorname{Nil}(R)$. 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 any $k \in \mathbb{N}$. So $(0) \in \Sigma$ and then $\Sigma \neq \emptyset$. Let $\mathscr{C} \subseteq \Sigma$ be chain. Then we have $\mathfrak{q} := \bigcup_{\mathfrak{a}\in\mathscr{C}} \mathfrak{a} \leq R$. Suppose $x^n \in \mathfrak{q}$ for some $n \in \mathbb{N}$. Then $x^n \in \mathfrak{a}$ for some $\mathfrak{a} \in \mathscr{C} \subseteq \Sigma$, contradicting $\mathfrak{a} \in \Sigma$. So $x^n \notin \mathfrak{q}$ for any $n \in \mathbb{N}$ 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.
Claim I is prime. Suppose $I = R$. Then $x \in R = I$, contradicting $I \in \Sigma$. So $I \lneq R$. Let $r, s \in R \setminus I$. Then $I \subsetneq \langle r, I\rangle \leq R$ and $I \subsetneq \langle s, I\rangle \leq R$. By the maximality of I in Σ, we have $\langle r, I\rangle, \langle s, I\rangle \notin \Sigma$. So there exists $m, n \in \mathbb{N}$ such that $x^m \in \langle r, I\rangle$ and $x^n \in \langle s, I\rangle$. Then $x^m = ar + i$ for some $a \in R$ and $i \in I$, and $x^n = bs + j$ for some $b \in R$ and $j \in I$. So $x^{m+n} = x^m x^n = (ar+i)(bs+j) = abrs + (\underbrace{arj + bsi + ij}_{\in I}) \in \langle rs, I\rangle$. Hence $\langle rs, I\rangle \notin \Sigma$. Also, since $I \in \Sigma$, $rs \notin I$. Thus, $I \in \operatorname{Spec}(R)$ such that $x \notin I$.

$\square$

Example. Let k be a field and $R = \frac{k[X_1,\cdots,X_d]}{(X_1^{a_1},\cdots,X_d^{a_d})} \neq 0$, where $a_i \in \mathbb{N}$ for any $i = 1, \cdots, d$. Then $\operatorname{Nil}(R) = \frac{\langle X_1,\cdots,X_d\rangle}{\langle X_1^{a_1},\cdots,X_d^{a_d}\rangle}$.

Proof. Method 1: Since $\operatorname{Spec}(R) = \left\{\frac{\langle X_1,\cdots,X_d\rangle}{\langle X_1^{a_1},\cdots,X_d^{a_d}\rangle}\right\}$, $\operatorname{Nil}(R) = \bigcap_{\mathfrak{p}\in\operatorname{Spec}(R)} \mathfrak{p} = \frac{\langle X_1,\cdots,X_d\rangle}{\langle X_1^{a_1},\cdots,X_d^{a_d}\rangle}$.
Method 2: Since $\overline{X}_i \in \operatorname{Nil}(R) \leq R$ for each $i = 1, \cdots, d$, we have $\overline{\langle X_1, \cdots, X_d\rangle} = \langle \overline{X}_1, \cdots, \overline{X}_d\rangle \subseteq \operatorname{Nil}(R) \subsetneq R$. Also, since $\overline{\langle X_1, \cdots, X_d\rangle}$ is maximal, we have $\operatorname{Nil}(R) = \overline{\langle X_1, \cdots, X_d\rangle}$. $\square$

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

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

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

1.5 Operations on Ideals

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

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. (a) $\mathfrak{a} + \mathfrak{b} \subseteq \mathfrak{c}$ iff $\mathfrak{a} \cup \mathfrak{b} \subseteq \mathfrak{c}$.

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

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

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

Proof. (c) Set $I = \{a + b \mid a \in \mathfrak{a}, b \in \mathfrak{b}\} \leq R$ (Check). For any $a \in \mathfrak{a}$, $a = a + 0 \in I$ and for any $b \in \mathfrak{b}$, $b = 0 + b \in I$. So $\mathfrak{a} \cup \mathfrak{b} \subseteq I$. By (a), $\mathfrak{a} + \mathfrak{b} \subseteq I$. OTOH, for any $a + b \in I$ with $a \in \mathfrak{a}$ and $b \in \mathfrak{b}$, $a, b \in \mathfrak{a} \cup \mathfrak{b} \subseteq \mathfrak{a} + \mathfrak{b} \leq R$. So $a + b \in \mathfrak{a} + \mathfrak{b}$.

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

(e) By (d).

(f) By (c).

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

□

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 any $S \subseteq R$, $\mathrm{V}(S) = \{\mathfrak{p} \in \mathrm{Spec}(R) \mid \mathfrak{p} \supseteq S\}$.

Proposition 1.32. Let $S \subseteq R$.

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

(b) $\mathfrak{a} = R$ iff $\mathrm{V}(\mathfrak{a}) = \emptyset$.

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

(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 $\mathrm{V}(S) \supseteq \mathrm{V}(T)$ by definition.

(a) "$\supseteq$". Since $S \subseteq \langle S \rangle$, $\mathrm{V}(S) \supseteq \mathrm{V}(\langle S \rangle)$ by (d).
"$\subseteq$". Let $\mathfrak{p} \in \mathrm{V}(S)$. Then $\mathfrak{p} \supseteq S$. So $\mathfrak{p} \supseteq \langle S \rangle$ and then $\mathfrak{p} \in \mathrm{V}(\langle S \rangle)$. Hence $\mathrm{V}(S) \subseteq \mathrm{V}(\langle S \rangle)$.

(b) "$\Rightarrow$". Let $\mathfrak{a} = R$. Then $\mathfrak{p} \not\supseteq \mathfrak{a}$ for any $\mathfrak{p} \in \mathrm{Spec}(R)$. So $\mathrm{V}(\mathfrak{a}) = \emptyset$.
"$\Leftarrow$". Let $\mathrm{V}(\mathfrak{a}) = \emptyset$. Suppose $\mathfrak{a} \neq R$, then there exists $\mathfrak{m} \leq R$ maximal such that $\mathfrak{m} \supseteq \mathfrak{a}$. Also, since $\mathfrak{m} \in \mathrm{Spec}(R)$, we have $\mathfrak{m} \in \mathrm{V}(\mathfrak{a})$, contradicting $\mathrm{V}(\mathfrak{a}) = \emptyset$.

(c) $\mathfrak{a} \subseteq \mathrm{Nil}(R)$ iff $\mathfrak{p} \supseteq \mathfrak{a}$ for all $\mathfrak{p} \in \mathrm{Spec}(R)$ iff $\mathrm{V}(\mathfrak{a}) = \mathrm{Spec}(R)$.

□

Proposition 1.33. (a) $\mathrm{V}(\mathfrak{a} + \mathfrak{b}) = \mathrm{V}(\mathfrak{a} \cup \mathfrak{b}) = \mathrm{V}(\mathfrak{a}) \cap \mathrm{V}(\mathfrak{b})$.

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

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 $\mathfrak{p} \supseteq \mathfrak{a} \cup \mathfrak{b}$ iff $\mathfrak{p} \supseteq \mathfrak{a}$ and $\mathfrak{p} \supseteq \mathfrak{b}$. So $\mathrm{V}(\mathfrak{a} \cup \mathfrak{b}) = \mathrm{V}(\mathfrak{a}) \cap \mathrm{V}(\mathfrak{b})$.

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

□

Remark. You can define $\mathfrak{a}_1 + \cdots + \mathfrak{a}_n$ inductively and same properties as above hold for finite sums.

Definition 1.34. $\sum_\lambda \mathfrak{a}_\lambda = \langle \bigcup_{\lambda \in \Lambda} \mathfrak{a}_\lambda \rangle = \bigcap_{\bigcup_{\lambda \in \Lambda} \mathfrak{a}_\lambda \subseteq I \leq R} I$.

Fact 1.35. (a) $\sum_{\lambda \in \Lambda} \mathfrak{a}_\lambda \subseteq \mathfrak{c}$ iff $\bigcup_{\lambda \in \Lambda} \mathfrak{a}_\lambda \subseteq \mathfrak{c}$.

(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 any $\lambda \in \Lambda$, then $\sum_{\lambda \in \Lambda} \mathfrak{a}_\lambda = \langle \bigcup_{\lambda \in \Lambda} S_\lambda \rangle$.

Fact 1.36. (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) $\bigcap_{\lambda \in \Lambda} \mathrm{V}(\mathfrak{a}_\lambda) = \emptyset$ iff $\sum_{\lambda \in \Lambda} \mathfrak{a}_\lambda = R$.

Definition 1.37. $\mathfrak{ab} = \langle N \rangle = \bigcap_{N \subseteq I \leq R} R$, where $N = \{ab \mid a \in \mathfrak{a}, b \in \mathfrak{b}\}$.

Fact 1.38. Let $\mathfrak{ab} = \langle N \rangle$.

(a) $\mathfrak{ab} \subseteq \mathfrak{c}$ iff $N \subseteq \mathfrak{c}$.

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

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

(d) If $\mathfrak{a} = \langle S \rangle$ and $\mathfrak{b} = \langle T \rangle$, then $\mathfrak{ab} = \langle st \mid s \in S, t \in T \rangle$.

(e) If $\mathfrak{a} = \langle x_1, \cdots, x_m \rangle$ and $\mathfrak{b} = \langle y_1, \cdots, y_n \rangle$, then $\mathfrak{ab} = \langle x_i y_j \mid i = 1, \cdots, m, j = 1, \cdots, n \rangle$.

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

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

(f) To show $\mathfrak{ab} \subseteq \mathfrak{a} \cap \mathfrak{b}$, it suffices to show $ab \in \mathfrak{a} \cap \mathfrak{b}$ for any $a \in \mathfrak{a}$ and $b \in \mathfrak{b}$. For any $a \in \mathfrak{a} \leq R$, we have $ab \in \mathfrak{a}$ for any $b \in \mathfrak{b}$. For any $b \in \mathfrak{b} \leq R$, we have $ab \in \mathfrak{b}$ for any $a \in \mathfrak{a}$. So $ab \in \mathfrak{a} \cap \mathfrak{b}$ for any $a \in \mathfrak{a}$ and $b \in \mathfrak{b}$.

□

Proposition 1.39. (a) $\mathrm{V}(\mathfrak{ab}) = \mathrm{V}(\mathfrak{a} \cap \mathfrak{b}) = \mathrm{V}(\mathfrak{a}) \cup \mathrm{V}(\mathfrak{b})$.

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

Proof. (a)

- Let $\mathfrak{p} \in \mathrm{Spec}(R)$. Claim $\mathfrak{p} \supseteq \mathfrak{ab}$ iff $\mathfrak{p} \supseteq \mathfrak{a}$ or $\mathfrak{p} \supseteq \mathfrak{b}$. "$\Leftarrow$". Let $\mathfrak{p} \supseteq \mathfrak{a}$ or $\mathfrak{p} \supseteq \mathfrak{b}$. Then $\mathfrak{p} = \mathfrak{p}R \supseteq \mathfrak{a}R \supseteq \mathfrak{ab}$ or $\mathfrak{p} = R\mathfrak{p} \supseteq R\mathfrak{b} \supseteq \mathfrak{ab}$. "$\Rightarrow$". 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 $\mathfrak{p} \supseteq \mathfrak{ab}$ iff $\mathfrak{p} \supseteq \mathfrak{a}$ or $\mathfrak{p} \supseteq \mathfrak{b}$. So $\mathrm{V}(\mathfrak{ab}) = \mathrm{V}(\mathfrak{a}) \cup \mathrm{V}(\mathfrak{b})$.

- 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 $\mathfrak{p} \supseteq \mathfrak{ab}$. Let $x \in \mathfrak{a} \cap \mathfrak{b}$. Then $x \in \mathfrak{a}$ and $x \in \mathfrak{b}$. So $x^2 = x \cdot x \in \mathfrak{ab} \subseteq \mathfrak{p}$. Since $\mathfrak{p}$ is prime, $x \in \mathfrak{p}$. So $\mathfrak{p} \supseteq \mathfrak{a} \cap \mathfrak{b}$ 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) $\mathrm{V}(\mathfrak{a}) \cup \mathrm{V}(\mathfrak{b}) = \mathrm{Spec}(R)$ iff $\mathrm{V}(\mathfrak{ab}) = \mathrm{Spec}(R)$ iff $\mathfrak{ab} \subseteq \mathrm{Nil}(R)$ and similarly for $\mathfrak{a} \cap \mathfrak{b}$.

□

Proposition 1.40. (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) If $\mathfrak{a} + \mathfrak{b} = R$, i.e., $\mathfrak{a}$ and $\mathfrak{b}$ are "coprime" and "co-maximal", then $\mathfrak{a} \cap \mathfrak{b} = \mathfrak{ab}$.
The converse holds if R is a PID and $\mathfrak{a}, \mathfrak{b} \neq 0$.

Proof. (c) "$\supseteq$". We always have $\mathfrak{a} \cap \mathfrak{b} \supseteq \mathfrak{ab}$.
"$\subseteq$". Assume $\mathfrak{a} + \mathfrak{b} = R$.
Method 1: Note $1 = a + b$ for some $a \in \mathfrak{a}$ and $b \in \mathfrak{b}$. Let $x \in \mathfrak{a} \cap \mathfrak{b}$. Then $x \in \mathfrak{b}$ and $x \in \mathfrak{a}$. So $x = 1 \cdot x = (a+b)x = ax + bx = ax + xb \in \mathfrak{ab}$. Hence $\mathfrak{a} \cap \mathfrak{b} \subseteq \mathfrak{ab}$.
Method 2: Note $\mathfrak{a} \cap \mathfrak{b} = R(\mathfrak{a} \cap \mathfrak{b}) = (\mathfrak{a} + \mathfrak{b})(\mathfrak{a} \cap \mathfrak{b}) = \mathfrak{a}(\underbrace{\mathfrak{a} \cap \mathfrak{b}}_{\subseteq \mathfrak{b}}) + \mathfrak{b}(\underbrace{\mathfrak{a} \cap \mathfrak{b}}_{\subseteq \mathfrak{a}}) \subseteq \mathfrak{ab}$ by (a) and (b).
Conversely, assume R is a PID and $\mathfrak{a}, \mathfrak{b} \neq 0$. Write $\mathfrak{a} = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_n^{e_n} R$ and $\mathfrak{b} = \mathfrak{p}_1^{f_1} \cdots \mathfrak{p}_n^{f_n} R$ with $e_i, f_i \geq 0$ for any $i = 1, \cdots, n$, and $\{\mathfrak{p}_1, \cdots, f\mathfrak{p}_n\} \subseteq \mathrm{Spec}(R)$ non-associates. Assume $\mathfrak{a} \cap \mathfrak{b} = \mathfrak{ab}$. Since R is a PID, $\mathfrak{a} \cap \mathfrak{b} = \mathrm{lcm}(\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_n^{e_n}, \mathfrak{p}_1^{f_1} \cdots \mathfrak{p}_n^{f_n})R = \mathfrak{p}_1^{\max\{e_1, f_1\}} \cdots \mathfrak{p}_n^{\max\{e_n, f_n\}}$. By the fact 1.38(e), $\mathfrak{ab} = \mathfrak{p}_1^{e_1+f_1} \cdots \mathfrak{p}_n^{e_n+f_n}$. So $\max\{e_i, f_i\} = e_i + f_i$, i.e, $e_i = 0$ or $f_i = 0$ for any $i = 1, \cdots, n$. In other words, for any $\mathfrak{p} \in \mathrm{Spec}(R)$, either $\mathfrak{a} \not\subseteq \mathfrak{p}R$ or $\mathfrak{b} \not\subseteq \mathfrak{p}R$. So $\mathrm{V}(\mathfrak{a}) \cap \mathrm{V}(\mathfrak{b}) = \emptyset$ for any $\mathfrak{p} \in \mathrm{Spec}(R)$. Thus, $\mathfrak{a} + \mathfrak{b} = R$.

□

Remark. You can do this for $\mathfrak{a}_1, \cdots, \mathfrak{a}_n$, where $n \in \mathbb{Z}^{\geq 3}$.

Example 1.41. Let $R = k[x, y]$, $\mathfrak{a} = \langle x \rangle$ and $\mathfrak{b} = \langle y \rangle$. Then $\mathfrak{a} \cap \mathfrak{b} = \langle xy \rangle = \mathfrak{ab}$ by the fact 1.38(e). But $\mathfrak{a} + \mathfrak{b} = \langle x, y \rangle \subsetneq R$. So the converse in (c) fails for any non-PID.

Definition 1.42. Let $n \in \mathbb{N}$. 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, let $R = \mathbb{F}_2[x, y]$ 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 $n \in \mathbb{N}$ and $N = \{a_1 \cdots a_n \mid a_i \in \mathfrak{a},\ \forall\, i = 1, \cdots, n\}$.

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

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

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

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

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

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

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

Proposition 1.46 (CRT)**.** Let $\mathfrak{a}_1, \cdots, \mathfrak{a}_n \leq R$.

(a) The function $\phi : R \to (R/\mathfrak{a}_1) \times \cdots \times (R/\mathfrak{a}_n)$ given by $\phi(x) = (\bar{x}, \cdots, \bar{x}) = (x + \mathfrak{a}_1, \cdots, x + \mathfrak{a}_n)$ is a well-defined ring homomorphism.

(b) If $\mathfrak{a}_i + \mathfrak{a}_j = R$ for any $1 \leq i \neq j \leq R$, i.e., $\{\mathfrak{a}_1, \cdots, \mathfrak{a}_n\}$ are pairwise co-prime, then $\bigcap_{i=1}^n \mathfrak{a}_i = \mathfrak{a}_1 \cdots \mathfrak{a}_n$ and $\mathfrak{a}_i + (\bigcap_{j\neq i} \mathfrak{a}_j)R = R$ for any $i = 1, \cdots, n$.

(c) ϕ is surjective iff $\mathfrak{a}_i + \mathfrak{a}_j = R$ for any $1 \leq i \neq j \leq n$.

(d) $\mathrm{Ker}(\phi) = \mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_n$.

(e) If $\mathfrak{a}_i + \mathfrak{a}_j = R$ for any $1 \leq i \neq j \leq n$ and $\bigcap_{i=1}^n \mathfrak{a}_i = 0$, then $R \cong (R/\mathfrak{a}_1)R \cap \cdots \times (R/\mathfrak{a}_n)R$.

Proof. (b) Let $i \in \{1, \cdots, r\}$. To show $\mathfrak{a}_i + (\bigcap_{j\neq i})R = R$. It suffices to show $\mathrm{V}(\mathfrak{a}_i) \cap \Big(\bigcup_{j\neq i} \mathrm{V}(\mathfrak{a}_j)\Big) = \mathrm{V}(\mathfrak{a}_i) \cap \mathrm{V}\left(\bigcap_{j\neq i} \mathfrak{a}_j\right) = \mathrm{V}(\mathfrak{a}_i + \bigcap_{j\neq i} \mathfrak{a}_j) = \emptyset$. Suppose $\mathrm{V}(\mathfrak{a}_i) \cap \Big(\bigcup_{j\neq i} \mathrm{V}(\mathfrak{a}_j)\Big) \neq \emptyset$. 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 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 $\mathfrak{a}_n + (\mathfrak{a}_1 \cdots \mathfrak{a}_{n-1})R = \mathfrak{a}_n + (\bigcap_{j=1}^{n-1} \mathfrak{a}_j)R = R$. So by proposition 1.40(c), we have $\bigcap_{i=1}^n \mathfrak{a}_i = (\bigcap_{i=1}^{n-1} \mathfrak{a}_i) \cap \mathfrak{a}_n = (\mathfrak{a}_1 \cdots \mathfrak{a}_{n-1}) \cap \mathfrak{a}_n = (\mathfrak{a}_1 \cdots \mathfrak{a}_{n-1})\mathfrak{a}_n = \mathfrak{a}_1 \cdots \mathfrak{a}_n$.

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

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 any $1 \leq i \neq j \leq n$.

"⇐". Assume $\mathfrak{a}_i + \mathfrak{b}_j = R$ for any $1 \leq i \neq j \leq n$. By (b), $\mathfrak{a}_1 + (\bigcap_{j=2}^n \mathfrak{a}_j)R = R$. So $a_1 + y = 1$ with $a_1 \in \mathfrak{a}_1$ and $y \in \bigcap_{j=2}^n \mathfrak{a}_j$, i.e., $1 - y = a_1 \in \mathfrak{a}_1$ and $y \in \mathfrak{a}_j$ for any $2 \leq j \leq n$. Then $\phi(y) = (\bar{y}, \bar{y}, \cdots, \bar{y}) = (y + \mathfrak{a}_1, y + \mathfrak{a}_2, \cdots, y + \mathfrak{a}_n) = (1 + \mathfrak{a}_1, 0 + \mathfrak{a}_2, \cdots, 0 + \mathfrak{a}_n) = (\bar{1}, \bar{0}, \cdots, \bar{0})$. Similarly, for any $j = 1, \cdots, n$, 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 $(\bar{r}_1, \cdots, \bar{r}_n) \in \frac{R}{\mathfrak{a}_1} \times \cdots \times \frac{R}{\mathfrak{a}_n}$, $(\bar{r}_1, \cdots, \bar{r}_n) = \sum_{j=1}^n r_j(\bar{0}, \cdots, \bar{0}, \underset{\uparrow j\text{th}}{\bar{1}}, \bar{0}, \cdots, \bar{0}) = \sum_{j=1}^n r_j \phi(y_j) = \phi(\sum_{j=1}^n r_j y_j)$. So ϕ is surjective.

$\square$

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

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

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

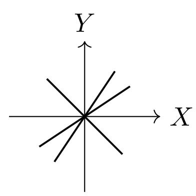
Proof. (b) Assume $\mathfrak{p} = \mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_n \supseteq \mathfrak{a}_1 \cdots \mathfrak{a}_n$. Since $\mathfrak{p} \in \operatorname{Spec}(R)$, there exists some $i \in \{1, \cdots, n\}$ such that $\mathfrak{p} \supseteq \mathfrak{a}_i$. Then $\mathfrak{a}_i \subseteq \mathfrak{p} = \mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_n \subseteq \mathfrak{a}_i$. So $\mathfrak{p} = \mathfrak{a}_i$.

(a) Follow from (b) directly.

$\square$

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

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



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

Example 1.49. If $|k| < \infty$, then fail. For example, let $V = k^2 = \bigcup_{v \in k^2} \{v\} = \bigcup_{0 \neq v \in k^2} \operatorname{span}\{v\}$ with $0 \neq \operatorname{span}(v) \lneq k^2 = V$.
Same technique shows that can't replace $V_1, \cdots, V_n$ with $V_1, V_2, \cdots$, over $\mathbb{Q}$.

Theorem 1.50 (More general version)**.** *Let $\mathfrak{b}_1, \cdots, \mathfrak{b}_n \leq R$. Assume*

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

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

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

Proof. (1) For any $i = 1, \cdots, n$, 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, $\mathfrak{a} \cap \bigcup_{i=1}^n \mathfrak{b}_i = \bigcup_{i=1}^n (\mathfrak{a} \cap \mathfrak{b}_i) \lneq \mathfrak{a}$. So $\mathfrak{a} \not\subseteq \bigcup_{i=1}^n \mathfrak{b}_i$.

(2) Induct on n. Base case $n = 1$, done. Base case $n = 2$. Let $a_i \in \mathfrak{a} \setminus \mathfrak{b}_i$ for any $i = 1, 2$. Then $a_1 + a_2 \in \mathfrak{a}$. Suppose $\mathfrak{a} \subseteq \mathfrak{b}_1 \cup \mathfrak{b}_2$. Then $a_1 + a_2 \in \mathfrak{b}_1 \cup \mathfrak{b}_2$, say $a_1 + a_2 \in \mathfrak{b}_2$. Since $a_1 \in \mathfrak{a} \subseteq \mathfrak{b}_1 \cup \mathfrak{b}_2$ and $a_1 \notin \mathfrak{b}_1$, $a_1 \in \mathfrak{b}_2$. So $a_2 = (a_1 + a_2) - a_1 \in \mathfrak{b}_2$, a contradiction.
Induct on $n \geq 3$. Let $\mathfrak{a} \not\subseteq \mathfrak{b}_i$ for any $i = 1, \cdots, n$. Assume $\mathfrak{a} \not\subseteq \bigcup_{i \neq j} \mathfrak{b}_i$ for any $j = 1, \cdots, n$, there exists $a_j \in \mathfrak{a} \backslash \{\bigcup_{i \neq j} \mathfrak{b}_i\}$. BWOC, suppose $\mathfrak{a} \subseteq \bigcup_{i=1}^n \mathfrak{b}_i$. Then $a_j \in \bigcup_{i=1}^n \mathfrak{b}_i \backslash \{\bigcup_{i \neq j} \mathfrak{b}_i\} = \mathfrak{b}_j$ for any $j = 1, \cdots, n$. Note $a_1 \cdots a_{n-1} + a_n \in \mathfrak{a} \subseteq \bigcup_{i=1}^n \mathfrak{b}_i$. So there exists $l \in \{1, \cdots, n\}$ such that $a_1 \cdots a_{n-1} + a_n \in \mathfrak{b}_l$. Suppose $l = n$. Since $a_n \in \mathfrak{b}_n$, $a_1 \cdots a_{n-1} \in \mathfrak{b}_n$. Since $n \geq 3$, we have $\mathfrak{b}_n \in \operatorname{Spec}(R)$ 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 $a_n \in \mathfrak{b}_l$, a contradiction.

□

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

Fact (Avoidence for monomial ideals)**.** Let A be CRW1$\neq 0$ and $\mathfrak{a}, \mathfrak{b}_1, \cdots, \mathfrak{b}_n$ be monomial ideals of $A[X_1, \cdots, X_d]$. If $\mathfrak{a} \subseteq \bigcup_{i=1}^n \mathfrak{b}_i$, then $\mathfrak{a} \subseteq \mathfrak{b}_i$ for some $i \in \{1, \cdots, n\}$.

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

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

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

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

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)

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

Fact 1.54. Let $S \subseteq R$.

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

(f) $\mathfrak{b} \subseteq \mathfrak{a}$ iff $(\mathfrak{a} : \mathfrak{b}) = R$.

(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) Let $r \in (\mathfrak{a} : \mathfrak{b})$ and $b \in \mathfrak{b}$. Then $br \in \mathfrak{a}$. So all generators of $(\mathfrak{a} : \mathfrak{b})\mathfrak{b}$ is in $\mathfrak{a}$.

(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 any $s \in S$. Let $s \in \langle S \rangle$. Then $s = \sum_i^{\text{finite}} a_i s_i$ for some $a_i \in R$ and $s_i \in S$ for each i. So $rs = r(\sum_i^{\text{finite}} a_i s_i) = \sum_i^{\text{finite}} a_i(rs_i) \in R$. Hence $r \in (\mathfrak{a} : \langle S \rangle)$.

(h) Follow from (e) and (g).

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

$\square$

Example 1.55. Let $R = k[X, Y]$. Since for $\underline{p}, \underline{q} \in \mathbb{N}^2$, we have $(\langle \underline{X}^{\underline{p}} \rangle : \underline{X}^{\underline{q}}) = \langle \underline{X}^{(p-q)^+} \rangle$, then

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

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

Definition 1.56. The *radical* of $\mathfrak{a} \leq R$ is $\operatorname{rad}(\mathfrak{a}) = \mathrm{r}(\mathfrak{a}) = \sqrt{\mathfrak{a}} = \{x \in R \mid x^n \in \mathfrak{a},\ \forall\, n \gg 0\} = \{x \in R \mid x^n \in \mathfrak{a}$ for some $n \in \mathbb{N}\}$.

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

Example 1.57. $\operatorname{rad}(\langle X^2Y, XY^2 \rangle) = \text{m-rad}(\langle X^2Y, XY^2 \rangle) = \langle \operatorname{red}(f) \mid f \in \{X^2Y, XY^2\} \rangle = \langle XY \rangle$ in $k[X, Y]$.

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 $\operatorname{rad}(\mathfrak{a}) \subseteq \operatorname{rad}(\mathfrak{b})$.

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

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

(e) $\operatorname{rad}(\mathfrak{a}) = R$ iff $\mathfrak{a} = R$.

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

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

(h) $\operatorname{rad}(\bigcap_{i=1}^n \mathfrak{p}_i^{e_i}) = \bigcap_{i=1}^n \mathfrak{p}_i$, where $\mathfrak{p}_i \in \operatorname{Spec}(R)$ and $e_i \in \mathbb{N}$ for any $i = 1, \cdots, n$.

(i) $\mathfrak{a} + \mathfrak{b} = R$ iff $\operatorname{rad}(\mathfrak{a}) + \operatorname{rad}(\mathfrak{b}) = R$.

Proof. (a) Let $r \in R$. Then $r \in \pi^{-1}(\operatorname{Nil}(R/\mathfrak{a}))$ iff $\pi(r) \in \operatorname{Nil}(R/\mathfrak{a})$ iff $\bar{r}^n = 0$ in $R/\mathfrak{a}$ for some $n \in \mathbb{N}$ iff $r^n \in \mathfrak{a}$ for some $n \in \mathbb{N}$ iff $r \in \operatorname{rad}(\mathfrak{a})$.

(b) It is clear.

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

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

(e) $\mathfrak{a} = R$ iff $1 \in \mathfrak{a}$ iff $1^n \in \mathfrak{a}$ iff $\operatorname{rad}(\mathfrak{a}) = R$.

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

(g) Note $\operatorname{Nil}(R/\mathfrak{a}) = \bigcap_{\mathfrak{p} \in \operatorname{Spec}(R/\mathfrak{a})} \mathfrak{p} = \bigcap_{\mathfrak{p} \in \operatorname{V}(\mathfrak{a})} \mathfrak{p}/\mathfrak{a}$ by 3IT/4IT. Then by (a) and the property of preimage, $\operatorname{rad}(\mathfrak{a}) = \pi^{-1}(\operatorname{Nil}(R/\mathfrak{a})) = \pi^{-1}(\bigcap_{\mathfrak{p} \in \operatorname{V}(\mathfrak{a})} \mathfrak{p}/\mathfrak{a}) = \bigcap_{\mathfrak{p} \in \operatorname{V}(\mathfrak{a})} \pi^{-1}(\mathfrak{p}/\mathfrak{a}) = \bigcap_{\mathfrak{p} \in \operatorname{V}(\mathfrak{a})} \mathfrak{p}$.

(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 each $i = 1, \cdots, n$. Then by (d), $\operatorname{rad}(\bigcap_{i=1}^n \mathfrak{p}_i^{e_i}) = \bigcap_{i=1}^n \operatorname{rad}(\mathfrak{p}_i^{e_i}) = \bigcap_{i=1}^n \operatorname{rad}(\mathfrak{p}_i) = \bigcap_{i=1}^n \mathfrak{p}_i$.

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

Example 1.59. (b) If $\operatorname{rad}(\mathfrak{a}) \subseteq \operatorname{rad}(\mathfrak{b})$, we can have $\mathfrak{a} \not\subseteq \mathfrak{b}$. For example, in $R = \mathbb{Z}$, $\langle 2 \rangle = \operatorname{rad}(\langle 2 \rangle) = \operatorname{rad}(\langle 4 \rangle) = \langle 2 \rangle$, but $\langle 2 \rangle \not\subseteq \langle 4 \rangle$.

(c) We can have $\mathfrak{a} \subsetneq \operatorname{rad}(\mathfrak{a})$. For example, in $R = \mathbb{Z}$, $\langle 4 \rangle \subsetneq \langle 2 \rangle = \operatorname{rad}(\langle 4 \rangle)$.

(d) We can have $\operatorname{rad}(\bigcap_{i=1}^\infty \mathfrak{a}_i) \neq \bigcap_{i=1}^\infty \operatorname{rad}(\mathfrak{a}_i)$. For example, in $R = k[X_1, X_2, \cdots]$, let $\mathfrak{a}_1 = \langle X_1 \rangle$, $\mathfrak{a}_2 = \langle X_1^2, X_2^2 \rangle$, $\cdots$, $\mathfrak{a}_n = \langle X_1^n, \cdots, X_n^n \rangle$, $\cdots$, then $\bigcap_{i=1}^\infty \mathfrak{a}_i = 0$, so $\operatorname{rad}(\bigcap_{i=1}^\infty \mathfrak{a}_i) = \operatorname{rad}(0) = 0$, but since $\langle X_i \rangle, \langle X_1, \cdots, X_n \rangle \in \operatorname{Spec}(\mathfrak{a})$ for each $i \in \mathbb{N}$, then by (f), $\bigcap_{i=1}^\infty \operatorname{rad}(\mathfrak{a}_i) = \bigcap_{i=1}^\infty \operatorname{rad}(\langle X_1, \cdots, X_i \rangle) = \bigcap_{i=1}^\infty \langle X_1, \cdots, X_i \rangle = \langle X_1 \rangle \neq 0$.

(f) We may have $\operatorname{rad}(\mathfrak{a} + \mathfrak{b}) \supsetneq \operatorname{rad}(\mathfrak{a}) + \operatorname{rad}(\mathfrak{b})$. For example, in $R = k[X, Y]$, let $\mathfrak{a} = \langle X + Y^2 \rangle$ 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 $R = \mathbb{F}_2[X, Y]$, $\mathfrak{a} = \langle X, Y \rangle$, $\mathfrak{b}_1 = \langle X, X^2, XY, Y^2 \rangle$, $\mathfrak{b}_2 = \langle X+Y, X^2, XY, Y^2 \rangle$, and $\mathfrak{b}_3 = \langle Y, X^2, XY, Y^2 \rangle$. Then $\mathfrak{a} = \mathfrak{b}_1 \cup \mathfrak{b}_2 \cup \mathfrak{b}_3$, but $\mathfrak{b}_i \subsetneq \mathfrak{a}$ for any $i = 1, 2, 3$.

(b) $\frac{\mathbb{F}_2[X,Y]}{\langle X^2,XY,Y^2\rangle} \geq \langle \overline{X}, \overline{Y}\rangle \cong \mathbb{F}_2^2$. Let $\mathfrak{b}_1 = \langle \overline{X}, \overline{Y}\rangle$, $\mathfrak{b}_2 = \langle \overline{X} + \overline{Y}\rangle$ and $\mathfrak{b}_3 = \langle Y\rangle$. Then $\langle \overline{X}, \overline{Y}\rangle = \mathfrak{b}_1 \cup \mathfrak{b}_2 \cup \mathfrak{b}_2$ with $\mathfrak{b}_i \subsetneq \langle \overline{X}, \overline{Y}\rangle$ for any $i = 1, 2, 3$.

1.6 Extensions and Contractions

Definition 1.61. Let $f : R \to S$ be a ring homomorphism. Let $\mathfrak{a} \leq R$ and $\mathfrak{b} \leq S$. The *extension* of $\mathfrak{a}$ along f is $\mathfrak{a}^e = \mathfrak{a}S = \langle f(\mathfrak{a})\rangle S = f(\mathfrak{a})S = \{\sum_i^{\text{finite}} f(a_i)s_i \mid a_i \in \mathfrak{a},\ s_i \in S,\ \forall\ i\} \leq S$. The *contraction* of $\mathfrak{b}$ along f is $\mathfrak{b}^c = f^{-1}(\mathfrak{b}) \leq R$.

Example 1.62. (a) Let R be an integral domain with 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 $0Q(R) = 0$ and for $0 \neq \mathfrak{a} \leq R$, we have $\mathfrak{a}Q(R) = Q(R)$.

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

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

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

Proposition 1.63. Let $f : R \to S$ be a ring homomorphism and $\mathfrak{b}, \mathfrak{b}_1, \mathfrak{b}_2 \leq S$.

(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 $f^{-1}(\mathfrak{a}S) = f^{-1}(2S) = f^{-1}(S) = R \supsetneq \langle 2\rangle R = \mathfrak{a}$.

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 $f^{-1}(\mathfrak{b}) = f^{-1}(f^{-1}(\mathfrak{b})S)$.

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

Example for $f^{-1}(\mathfrak{b}_1) + f^{-1}(\mathfrak{b}_2) \subsetneq f^{-1}(\mathfrak{b}_1 + \mathfrak{b}_2)$. 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 $f^{-1}(\mathfrak{b}_1) = 0 = f^{-1}(\mathfrak{b}_2)$ and so $f^{-1}(\mathfrak{b}_1) + f^{-1}(\mathfrak{b}_2) = 0$, but $\mathfrak{b}_1 + \mathfrak{b}_2 = S$, $f^{-1}(\mathfrak{b}_1 + \mathfrak{b}_2) = R \neq 0$.

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

(e) $(\mathfrak{a}_1\mathfrak{a}_2)S = (\mathfrak{a}_1 S)(\mathfrak{a}_2 S)$ and $f^{-1}(\mathfrak{b}_1)f^{-1}(\mathfrak{b}_2) \subseteq f^{-1}(\mathfrak{b}_1\mathfrak{b}_2)$.
Example of $f^{-1}(\mathfrak{b}_1)f^{-1}(\mathfrak{b}_2) \subsetneq f^{-1}(\mathfrak{b}_1\mathfrak{b}_2) \subseteq f^{-1}(\mathfrak{b}_1 \cap \mathfrak{b}_2) = f^{-1}(\mathfrak{b}_1) \cap f^{-1}(\mathfrak{b}_2)$. Let $f : R = k[X] \to S = k[X]/(X(X-1)) = k[X]/(X^2 - X) \cong k[X]/\langle X\rangle \times k[X]/\langle X-1\rangle \cong k \times k$ by CRT. Note in $k \times k$, $(1,0) = (1,0)^2$. Let $\mathfrak{b}_1 = \langle \overline{X}\rangle S = \mathfrak{b}_2$. Then $\mathfrak{b}_1\mathfrak{b}_2 = \langle \overline{X}^2\rangle S = \langle \overline{X}\rangle S = \mathfrak{b}_1$. So $f^{-1}(\mathfrak{b}_1\mathfrak{b}_2) = f^{-1}(\mathfrak{b}_1) = f^{-1}(\langle \overline{X}\rangle S) = \langle X\rangle R \supsetneq \langle X^2\rangle R = f^{-1}(\mathfrak{b}_1)f^{-1}(\mathfrak{b}_2)$.

(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 $f : R = k[X] \to S = k[X]/\langle X\rangle \cong k$. Let $\mathfrak{a}_1 = \langle X^2\rangle R$ 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 $(\mathfrak{b}_1 : \mathfrak{b}_2) = (\langle X\rangle : \langle X-1\rangle) = \langle X\rangle$, $f^{-1}(\mathfrak{b}_1) = 0 = f^{-1}(\mathfrak{b}_2)$. So $f^{-1}(\mathfrak{b}_1 : \mathfrak{b}_2) = f^{-1}(\langle X\rangle) = 0 \subsetneq R = (0 : 0) = (f^{-1}(\mathfrak{b}_1) : f^{-1}(\mathfrak{b}_2))$.

(g) $\mathrm{rad}(\mathfrak{a})S \subseteq \mathrm{rad}(\mathfrak{a}S)$ and $f^{-1}(\mathrm{rad}(\mathfrak{b})) = \mathrm{rad}(f^{-1}(\mathfrak{b}))$.
Example of $\mathrm{rad}(\mathfrak{a})S \subseteq \mathrm{rad}(\mathfrak{a}S)$. Let $f : R = k[X] \to S = k[X]/\langle X^2\rangle$ and $\mathfrak{a} = 0R$. Then $\mathrm{rad}(\mathfrak{a})S = \mathrm{rad}(0R)S = 0S = 0 \subsetneq \langle \overline{X}\rangle S = \mathrm{rad}(0S) = \mathrm{rad}(\mathfrak{a}S)$.

Proof. (a)
- Note $\mathfrak{a} \subseteq f^{-1}(f(\mathfrak{a})) \subseteq f^{-1}(\mathfrak{a}S)$. So we have equality iff f is bijective.
- 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. So we have equality iff f is onto.
- The set of generators of $(\langle T\rangle R)S$ over S is $\{f(\sum_i^{\text{finite}} t_i r_i) = \sum_i^{\text{finite}} f(t_i)f(r_i) \mid t_i \in T,\ r_i \in S,\ \forall\ i\} \subseteq \langle f(T)\rangle S$. The 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)
- "$\subseteq$". Since $\mathfrak{a} \subseteq f^{-1}(\mathfrak{a}S)$, $\mathfrak{a}S \subseteq f^{-1}(\mathfrak{a}S)S$. "$\supseteq$". The set of generators of $f^{-1}(\mathfrak{a}S)S$ over S is $\{f(x) \mid x \in f^{-1}(\mathfrak{a}S)\} = f(f^{-1}(\mathfrak{a}S)) \subseteq \mathfrak{a}S$.
- "$\subseteq$". Since $\mathfrak{b} \supseteq f^{-1}(\mathfrak{b})S$, $f^{-1}(\mathfrak{b}) \supseteq f^{-1}(f^{-1}(\mathfrak{b})S)$. "$\subseteq$". Let $x \in f^{-1}(\mathfrak{b})$. Then $f(x) = f(x)\cdot 1 \in \langle f(f^{-1}\mathfrak{b})\rangle S = f^{-1}(\mathfrak{b})S$. So $x \in f^{-1}(f^{-1}(\mathfrak{b}))$.

(c) "$\supseteq$". Since $\mathfrak{a}_1 + \mathfrak{a}_2 \supseteq \mathfrak{a}_1, \mathfrak{a}_2$, $(\mathfrak{a}_1 + \mathfrak{a}_2)S \supseteq \mathfrak{a}_1 S, \mathfrak{a}_2 S$. So $(\mathfrak{a}_1 + \mathfrak{a}_2)S \supseteq \mathfrak{a}_1 S + \mathfrak{a}_2 S$. "$\subseteq$". The 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 $\mathfrak{a}_1 \cap \mathfrak{a}_2 \subseteq \mathfrak{a}_1, \mathfrak{a}_2$, $(\mathfrak{a}_1 \cap \mathfrak{a}_2)S \subseteq \mathfrak{a}_1 S, \mathfrak{a}_2 S$. So $(\mathfrak{a}_1 \cap \mathfrak{a}_2)S \subseteq \mathfrak{a}_1 S \cap \mathfrak{a}_2 S$.
- $x \in f^{-1}(\mathfrak{b}_1 \cap \mathfrak{b}_2)$ iff $f(x) \in \mathfrak{b}_1 \cap \mathfrak{b}_2$ iff $f(x) \in \mathfrak{b}_1, \mathfrak{b}_2$ iff $x \in f^{-1}(\mathfrak{b}_1), f^{-1}(\mathfrak{b}_2)$ iff $x \in f^{-1}(\mathfrak{b}_1) \cap f^{-1}(\mathfrak{b}_2)$.

(e) "$\subseteq$". The set of generators of $(\mathfrak{a}_1\mathfrak{a}_2)S$ over S is $\{f(\sum_i^{\text{finite}} \alpha_i\beta_i) = \sum_i^{\text{finite}} f(\alpha_i)f(\beta_i) \mid \alpha_i \in \mathfrak{a}_1,\ \beta_i \in \mathfrak{a}_2,\ \forall\ i\} \subseteq (\mathfrak{a}_1 S)(\mathfrak{a}_2 S)$. "$\supseteq$". $(\mathfrak{a}_1 S)(\mathfrak{a}_2 S) = (f(\mathfrak{a}_1)S)(f(\mathfrak{a}_2)S) = (f(\mathfrak{a}_1)f(\mathfrak{a}_2))S = \langle f(a_1)f(a_2) \mid a_1 \in \mathfrak{a}_1, a_2 \in \mathfrak{a}_2\rangle S = \langle f(a_1 a_2) \mid a_1 \in \mathfrak{a}_1, a_2 \in \mathfrak{a}_2\rangle S \subseteq \langle f(\mathfrak{a}_1\mathfrak{a}_2)\rangle S = (\mathfrak{a}_1\mathfrak{a}_2)S$.

(f)
- The set of generators of $(\mathfrak{a}_1 : \mathfrak{a}_2)S$ over S is $\{f(r) \mid r \in (\mathfrak{a}_1 : \mathfrak{a}_2)\} = \{f(r) \mid r\mathfrak{a}_2 \subseteq \mathfrak{a}_1\} \subseteq \{f(r) \mid rf(\mathfrak{a}_2) \subseteq f(\mathfrak{a}_1)\} \subseteq \{s \in S \mid sf(\mathfrak{a}_2) \subseteq f(\mathfrak{a}_1)\} = \{s \in S \mid sf(\mathfrak{a}_2)S \subseteq f(\mathfrak{a}_1)S\} = \{s \in S \mid s\mathfrak{a}_2 S \subseteq \mathfrak{a}_1 S\} = (\mathfrak{a}_1 S : \mathfrak{a}_2 S)$.
- $f^{-1}(\mathfrak{b}_1 : \mathfrak{b}_2) = \{f^{-1}(s) \mid s \in (\mathfrak{b}_1 : \mathfrak{b}_2)\} = \{f^{-1}(s) \mid s\mathfrak{b}_2 \subseteq \mathfrak{b}_1\} \subseteq \{f^{-1}(s) \mid sf^{-1}(\mathfrak{b}_2) \subseteq f^{-1}(\mathfrak{b}_1)\} \subseteq \{r \in R \mid rf^{-1}(\mathfrak{b}_2) \subseteq f^{-1}(\mathfrak{b}_1)\} = (f^{-1}(\mathfrak{b}_1) : f^{-1}(\mathfrak{b}_2))$.

(g)
- Let $s \in \mathrm{rad}(\mathfrak{a})S$. Then there exists $m \in \mathbb{N}$ and $a_i \in \mathrm{rad}(\mathfrak{a})$ and $s_i \in S$ for any $i = 1, \cdots, m$ such that $s = \sum_{i=1}^m f(a_i)s_i$. Since $a_i \in \mathrm{rad}(\mathfrak{a})$, there exists $n_i \in \mathbb{N}$ such that $a_i^{n_i} \in \mathfrak{a}$ for each $i = 1, \cdots, m$. Let $n = n_1 + \cdots + n_m$. Then by PHP,

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

So $s \in \mathrm{rad}(\mathfrak{a}S)$.

- Note $x \in f^{-1}(\mathrm{rad}(\mathfrak{b}))$ iff $f(x) \in \mathrm{rad}(\mathfrak{b})$ iff $f(x)^n \in \mathfrak{b}$ for some $n \in \mathbb{N}$ iff $f(x^n) \in \mathfrak{b}$ for some $n \in \mathbb{N}$ iff $x^n \in f^{-1}(\mathfrak{b})$ for some $n \in \mathbb{N}$ iff $x \in \mathrm{rad}(\mathfrak{b})$.

$\square$

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

Proof. Let $x \in \mathrm{Nil}(R)$. Then there is a $n \in \mathbb{N}$ such that $x^n = 0$. Let $\eta = 1 - x + x^2 - \cdots + (-1)^{n-1}x^{n-1}$. Then $\eta(1+x) = 1 - x^n = 1$. So $1 + x \in R^\times$. Let $u \in R^\times$. Then $u^{-1}x \in \mathrm{Nil}(R)$. So $1 + u^{-1}x \in R^\times$. Hence $u + x = u(1 + (u^{-1}x)) \in R^\times$. $\square$

1.7 Power Series Rings

Let A be a CRW1.

Definition 1.65. $A[\![X]\!] = \{f = \sum_{i=0}^{\infty} a_i X^i \mid a_i \in A,\ \forall\ i\} \cong \prod_{i=0}^{\infty} A$ with addition and multiplication given 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 each $i \in \mathbb{Z}^+$.
$0_{A[\![X]\!]} = 0_A = \sum_{i=0}^{\infty} 0_A X^i$ and $1_{A[\![X]\!]} = 1_A = 1_A + \sum_{i=0}^{\infty} 0_A X^i$. More generally, for any $\mathfrak{a} \leq A$, $\mathfrak{a}[\![X]\!] = \{\sum_{i=0}^{\infty} a_i X^i \mid a_i \in \mathfrak{a},\ \forall\ i\} \leq A[\![X]\!]$.

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 CRW1 and A is a subring of $A[X]$ and $A[X]$ is a subring of $A[\![X]\!]$.*

Proposition 1.68. Let $f = \sum_{i=0}^{\infty} a_i X^i$.

(a) f is a unit in $A[\![X]\!]$ iff $a_0 \in A^\times$.

(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 $\frac{A[\![X]\!]}{\mathfrak{a}[\![X]\!]} \cong \frac{A}{\mathfrak{a}}[X]$. In addition, $\mathfrak{a} \cdot A[\![X]\!] = \mathfrak{a}[\![X]\!]$ if $\mathfrak{a} \leq A$ is finitely generated.

(d) Let $\mathfrak{a} \leq A$. Then $\langle X, \mathfrak{a}\rangle A[\![X]\!] = X \cdot A[\![X]\!] + \mathfrak{a} \cdot A[\![X]\!] = XA[\![X]\!] + \mathfrak{a}[\![X]\!] = \{\sum_{i=0}^{\infty} b_i X^i \mid b_0 \in \mathfrak{a},\ b_i \in A,\ \forall\ i \in \mathbb{N}\} \leq A[\![X]\!]$ and $\frac{A[\![X]\!]}{\langle X, \mathfrak{a}\rangle A[\![X]\!]} \cong \frac{A}{\mathfrak{a}}$. In particular, if $\mathfrak{a} = 0$, then $\langle X\rangle A[\![X]\!] = \{\sum_{i=1}^{\infty} b_i x_i \mid b_i \in A,\ \forall\ i \in \mathbb{N}\} \leq A[\![X]\!]$ and $\frac{A[\![X]\!]}{\langle X\rangle A[\![X]\!]} \cong A$.

(e) If $f \in \mathrm{Nil}(A[\![X]\!])$, then $a_i \in \mathrm{Nil}(A)$ for any $i \in \mathbb{Z}^+$. Converse holds if $= \langle a_0, a_1, a_2, \cdots\rangle$ is finitely generated. Also, $\mathrm{Nil}(A) \cdot A[\![X]\!] \subseteq \mathrm{Nil}(A[\![X]\!]) \subseteq \mathrm{Nil}(A)[\![X]\!]$.

Proof. (a) "$\Rightarrow$". Let the multiplicative inverse of f be $f^{-1}(X) = \sum_{i=0}^{\infty} b_i X^i \in A[\![X]\!]$. Then $1_A = f \cdot f^{-1} = (\sum_{i=0}^{\infty} a_i X^i)(\sum_{j=0}^{\infty} b_j X^j) = a_0 b_0 + (a_0 b_1 + a_1 b_0)X + \cdots$. So $a_0 b_0 = 1_A$ and hence $a_0 \in A^\times$. "$\Leftarrow$". We try find $g = \sum_{j=0}^{\infty} b_i X^i \in A[\![X]\!]$ such that $fg = 1$, i.e., $1 = \sum_{i=0}^{\infty} c_i X^i$, where $c_i = \sum_{j=0}^{i} a_j b_{i-j}$. If $a_0 = 1$, then $b_0 = a_0 b_0 = 1$ and $\sum_{j=0}^{i} a_j b_{i-j} = c_i = 0$ for any $i \in \mathbb{N}$.

So $b_1 = -a_1$, $b_2 = -a_2 + a_1^2$ and we can solve b_n's inductively. If $a_0 \neq 1$, then $a_0 \in A\times$ and so $f = \sum_{i=0}^{\infty} a_i X^i = \sum_{i=0}^{\infty} a_0(a_0^{-1}a_i)X^i = a_0 \underbrace{\left(1 + \sum_{i=1}^{\infty}(a_0^{-1}a_i)X^i\right)}_{\in A[\![X]\!]^\times} \in A[\![X]\!]^\times$.

(b) $\varphi[\![X]\!]$ is a well-defined ring homomorphism, done. Note

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

(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 $A[\![X]\!] \geq \operatorname{Ker}(\tau[\![X]\!]) = \operatorname{Ker}(\tau)[\![X]\!] = \mathfrak{a}[\![X]\!]$. Since τ is onto, by the 1IT, $\frac{A[\![X]\!]}{\mathfrak{a}[\![X]\!]} \cong \frac{A}{\mathfrak{a}}[\![X]\!]$. Since $\mathfrak{a} = \operatorname{Ker}(\tau) \subseteq \operatorname{Ker}(\tau[\![X]\!])$, we have $\langle\mathfrak{a}\rangle A[\![X]\!] \subseteq \operatorname{Ker}(\tau[\![X]\!]) = \mathfrak{a}[\![X]\!]$. Assume $\mathfrak{a} = (\alpha_1, \cdots, \alpha_n)A$. Let $f = \sum_{i=1}^{\infty} a_i X^i \in \mathfrak{a}[\![X]\!]$, where $a_i \in \mathfrak{a} = (\alpha_1, \cdots, \alpha_n)A$ for each $i \in \mathbb{Z}^+$. Then for each $i \in \mathbb{Z}^+$, $a_i = \sum_{j=1}^{n} b_{ij}\alpha_j$ for some $b_{i1}, \cdots, b_{in} \in A$. So $f = \sum_{i=0}^{\infty} a_i X^i = \sum_{i=0}^{\infty}\left(\sum_{j=1}^{n} b_{ij}\alpha_j\right)X^i = \sum_{j=1}^{n}\alpha_j\left(\sum_{i=0}^{\infty} b_{ij}X^i\right) \in \langle\mathfrak{a}\rangle A[\![X]\!]$.

(d) Note

$$\begin{array}{ccc} A[\![X]\!] & \xrightarrow{\ \pi\ } & A \\ \big\downarrow & & \big\downarrow{\scriptstyle \tau} \\ \frac{A}{\mathfrak{a}}[\![X]\!] & \xrightarrow{\ \pi'\ } & \frac{A}{\mathfrak{a}} \end{array}$$

Let π and π' be defined by $\pi(\sum_{i=0}^{\infty} b_i X^i) = b_0$ and $\pi'(\sum_{i=0}^{\infty} \bar{b}_i X^i) = \bar{b}_0$, respectively.
Check π and π^{-1} are well-defined ring epimorphisms and the diagram commutes.
Note $\operatorname{Ker}(\pi) = \{\sum_{i=1}^{\infty} b_i X^i \mid b_i \in A,\ \forall\ i \in \mathbb{N}\} = X\{\sum_{i=0}^{\infty} b_{i+1}X^i \mid b_i \in A,\ \forall\ i \in \mathbb{N}\} = X \cdot A[\![X]\!]$.
In general, $A[\![X]\!] \geq \operatorname{Ker}(\tau \circ \pi) = \{\sum_{i=0}^{\infty} b_i X^i \mid b_0 \in \mathfrak{a},\ b_i \in A,\ \forall\ i \in \mathbb{N}\} =: I$.
Let $\sum_{i=0}^{\infty} b_i X^i \in I$, i.e., $b_0 + X\sum_{i=0}^{\infty} b_{i+1}X^i \in \mathfrak{a} + XA[\![X]\!] \subseteq \langle X, \mathfrak{a}\rangle A[\![X]\!]$. So $I \subseteq \langle X, \mathfrak{a}\rangle A[\![X]\!]$. Since $X = 0 + X$, $X \in I$. Also, since if $\sum_{i=0}^{\infty} b_i X^i \in \mathfrak{a}[\![X]\!] \leq A[\![X]\!]$, we have $b_0 \in \mathfrak{a}$ and then $\mathfrak{a}[\![X]\!] \subseteq I$. Hence $\langle X\rangle A[\![X]\!] + \mathfrak{a}[\![X]\!] \subseteq I$.
Thus, by (c),

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

So $\langle X, \mathfrak{a}\rangle A[\![X]\!] = \langle X\rangle A[\![X]\!] + \langle\mathfrak{a}\rangle A[\![X]\!] = \langle X\rangle A[\![X]\!] + \mathfrak{a}[\![X]\!] = I = \operatorname{Ker}(\tau \circ \pi)$. By the 1IT, $\frac{A[\![X]\!]}{\langle X, \mathfrak{a}\rangle A[\![X]\!]} \cong \frac{A}{\mathfrak{a}}$.

(e) Since $f \in \operatorname{Nil}(A[\![X]\!])$, $0 = f^n = a_0^n + \cdots$ for some $n \in \mathbb{N}$. So a_0 is nilpotent. Since $f, a_0 \in \operatorname{Nil}(A[\![X]\!])$, $\sum_{i=1}^{\infty} a_i X^i = f - a_0 \in \operatorname{Nil}(A[\![X]\!])$. Similarly, we have a_1 is nilpotent. By induction, $a_i \in \operatorname{Nil}(A)$ for each $i \in \mathbb{Z}^+$. So $\operatorname{Nil}(A[\![X]\!]) \subseteq \operatorname{Nil}(A)[\![X]\!]$. Also, since $\operatorname{Nil}(A) \subseteq$

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

$\square$