# Commutative Algebra

September 10, 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 $\Delta$ 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 $\phi$ to be continuous if $K = \mathbb{F}_3$? Need a notion of open sets in $V$ and $W$.

# Chapter 1

# Rings and Ideals

Let $R$ be a 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.

**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 $\langle A \rangle = \{\sum_{a \in A}^{\text{finite}} r_a a \mid r_a \in R,\ \forall\, a\}$.

**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 $r \in R$, $r + \mathfrak{a} = \{r + a \mid a \in \mathfrak{a}\} = \overline{r}$. Let $R/\mathfrak{a} := \{r + \mathfrak{a} \mid r \in R\}$. Then $R/\mathfrak{a}$ is a CRW1 with $\overline{r} \pm \overline{s} = \overline{r \pm s}$, $\overline{r}\,\overline{s} = \overline{rs}$, $0_{R/\mathfrak{a}} = \overline{0_R}$ and $1_{R/\mathfrak{a}} = \overline{1_R}$.
Let $\pi : R \to R/\mathfrak{a}$ be given by $\pi(r) = \overline{r}$. Then $\pi$ 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 $\overline{\phi}(\overline{r}) = \overline{\phi}(\pi(r)) = \phi(r)$.
Note $\phi(\mathfrak{a}) = 0$ iff $\mathfrak{a} \subseteq \operatorname{Ker}(\phi)$. In particular, if $\mathfrak{a} = \langle A \rangle$, then $\mathfrak{a} \subseteq \operatorname{Ker}(\phi)$ iff $A \subseteq \operatorname{Ker}(\phi)$.

**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.

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

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

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

**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, 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 $\mathfrak{q} \in \operatorname{Spec}(S)$. Then $S/\mathfrak{q}$ is an integral domain. Also, since $R/\operatorname{Ker}(\pi \circ \phi) \cong S/\mathfrak{q}$, we have $R/\operatorname{Ker}(\pi \circ \phi)$ 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, $\phi$ induces a well-defined map $\phi^* : \operatorname{Spec}(S) \to \operatorname{Spec}(R)$.

**Example.** Let $\phi : \mathbb{Z} \to \mathbb{Q}$ be an inclusion map. Note $\mathfrak{q} := (0)\mathbb{Q} \leq \mathbb{Q}$ is maximal, but $\phi^{-1}(\mathfrak{q}) = \phi^{-1}(0) = \operatorname{Ker}(\phi) = 0\mathbb{Z}$, 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, $\mathrm{V}(\mathfrak{a}) = \{\mathfrak{p} \in \operatorname{Spec}(R) \mid \mathfrak{p} \supseteq \mathfrak{a}\} \neq \emptyset$.

(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 $\operatorname{Spec}(\mathbb{Z}/\langle p^n \rangle) = \{\langle p \rangle/\langle p^n \rangle\}$.

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

(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, $\operatorname{Spec}(R) = \left\{ \frac{\langle X_1, \cdots, X_d \rangle}{\langle X_1^{a_1}, \cdots, X_d^{a_d} \rangle} \right\}$.

**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.

**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)$\Rightarrow$(ii)". Assume $(R, \mathfrak{m})$ is local. Claim $\mathfrak{m} = R \setminus R^\times$. It suffices to show $R \setminus \mathfrak{m} = R^\times$.
"$\supseteq$". Let $u \in R^\times$. Then $\langle u \rangle = R$ and so $u \notin \mathfrak{m} \lneq R$, i.e., $u \in R \setminus \mathfrak{m}$. Hence $R^\times \subseteq R \setminus \mathfrak{m}$.
"$\subseteq$". Let $x \in R \setminus R^\times$. Then $\langle x \rangle \lneq R$. 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)$\Rightarrow$(iii)". Assume $R \setminus R^\times \lneq R$. Set $\mathfrak{a} = R \setminus R^\times$. Then $R \setminus \mathfrak{a} = R^\times$.
"(iii)$\Rightarrow$(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. $\square$

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

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

**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 $\mathbb{Z}/\langle p^n \rangle$, $\overline{p}$ 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 $\overline{x} \in \mathrm{Nil}(R/\mathrm{Nil}(R))$. Then there exists $n \in \mathbb{N}$ such that $\overline{x^n} = \overline{x}^n = 0$, i.e., $x^n \in \mathrm{Nil}(R)$. So there exists $m \in \mathbb{N}$ such that $(x^n)^m = 0$, i.e., $x^{mn} = 0$. Thus, $x \in \mathrm{Nil}(R)$, i.e., $\overline{x} = 0$.

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

(d) "$\subseteq$". Let $x \in \mathrm{Nil}(R)$. Then there exists $n \in \mathbb{N}$ such that $x^n = 0 \in \mathfrak{p}$ for any $\mathfrak{p} \in \mathrm{Spec}(R)$. So $x \in \mathfrak{p}$ for any $p \in \mathrm{Spec}(R)$. Thus, $x \in \bigcap_{\mathfrak{p} \in \mathrm{Spec}(R)} \mathfrak{p}$.
"$\supseteq$". Let $x \in R \setminus \mathrm{Nil}(R)$. Need to show $x \notin \bigcap_{\mathfrak{p} \in \mathrm{Spec}(R)}$. It is equivalent to show there exists $\mathfrak{p} \in \mathrm{Spec}(R)$ such that $x \notin \mathfrak{p}$. Let $\Sigma = \{\mathfrak{a} \leq R \mid x, x^2, x^3 \cdots \notin \mathfrak{a}\}$. Since $x \notin \mathrm{Nil}(R)$, $x^k \neq 0$ 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 $\Sigma$. Since the chain

$\mathscr{C} \subseteq \Sigma$ is arbitrary, by Zorn's lemma, $\Sigma$ 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 $\Sigma$, 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 $x \notin I$.

□

**Example.** Let $k$ be a field and $R = \frac{k[X_1, \cdots, X_d]}{\langle X_1^{a_1}, \cdots, X_d^{a_d} \rangle} \neq 0$, 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 $\operatorname{Nil}(R) = \overline{\langle X_1, \cdots, X_d \rangle}$. □

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

**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. □

## 1.1 Operations on Ideals

Let $\mathfrak{a}, \mathfrak{b}, \mathfrak{c} \leq R$, $\mathfrak{a}_1, \cdots, \mathfrak{a}_n \leq R$ and $\mathfrak{a}_\lambda \leq R$ for any $\lambda \in \Lambda$, where $\Lambda$ 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 $\mathfrak{a}+\mathfrak{b} = R$.

$\square$

**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 $b \in \mathfrak{b}$.

$\square$

**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 $\mathfrak{p}_i$'s $\in \mathrm{Spec}(R)$ 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 $\phi(x) = (\overline{x}, \cdots, \overline{x}) = (x + \mathfrak{a}_1, \cdots, x + \mathfrak{a}_n)$ 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) $\phi$ 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 $\mathrm{V}(\mathfrak{a}_i) \cap \left(\bigcup_{j\neq i} \mathrm{V}(\mathfrak{a}_j)\right) = \mathrm{V}(\mathfrak{a}_i) \cap \mathrm{V}\left(\bigcap_{j\neq i} \mathfrak{a}_j\right) = \mathrm{V}(\mathfrak{a}_i + \bigcap_{j\neq i} \mathfrak{a}_j) = \emptyset$. Suppose $\mathrm{V}(\mathfrak{a}_i) \cap \left(\bigcup_{j\neq i} \mathrm{V}(\mathfrak{a}_j)\right) \neq \emptyset$. 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 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) "$\Rightarrow$". Assume $\phi$ is surjective. In particular, there exists $x \in R$ such that $(\overline{1}, \overline{0}, \cdots, \overline{0}) = \phi(x) = (\overline{x}, \overline{x}, \cdots, \overline{x})$. 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 $(\overline{0}, \cdots, \overline{0}, \underset{\uparrow j\text{th}}{\overline{1}}, \overline{0}, \cdots, \overline{0}) \rightsquigarrow \mathfrak{a}_i + \mathfrak{a}_j = R$ for any $1 \leq i \neq j \leq n$.

"$\Leftarrow$". 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 $\phi(y) = (\overline{y}, \overline{y}, \cdots, \overline{y}) = (y + \mathfrak{a}_1, y + \mathfrak{a}_2, \cdots, y + \mathfrak{a}_n) = (1 + \mathfrak{a}_1, 0 + \mathfrak{a}_2, \cdots, 0 + \mathfrak{a}_n) = (\overline{1}, \overline{0}, \cdots, \overline{0})$. Similarly, for any $j = 1, \cdots, n$, there exists $y_j$ such that $\phi(y_j) = (\overline{0}, \cdots, \overline{0}, \underset{\uparrow j\text{th}}{\overline{1}}, \overline{0}, \cdots, \overline{0})$. Then for any $(\overline{r}_1, \cdots, \overline{r}_n) \in \frac{R}{\mathfrak{a}_1} \times \cdots \times \frac{R}{\mathfrak{a}_n}$, $(\overline{r}_1, \cdots, \overline{r}_n) = \sum_{j=1}^n r_j(\overline{0}, \cdots, \overline{0}, \underset{\uparrow j\text{th}}{\overline{1}}, \overline{0}, \cdots, \overline{0}) = \sum_{j=1}^n r_j \phi(y_j) = \phi(\sum_{j=1}^n r_j y_j)$. So $\phi$ is surjective.

□

**Proposition 1.47.** Let $\mathfrak{a}_1, \cdots, \mathfrak{a}_n \leq R$ 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 $i \in \{1, \cdots, n\}$.

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

□

**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 $\mathfrak{a}_1 \cap \mathfrak{a}_2 = \langle xy \rangle \neq \langle x \rangle = \mathfrak{p} = \langle x \rangle \neq \langle xy \rangle = \mathfrak{a}_1\mathfrak{a}_2$.

**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 $\mathfrak{a} \not\subseteq \bigcup_{i=1}^n \mathfrak{p}_i$.*

**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 $\mathfrak{a} \subseteq \bigcup_{i=1}^n \mathfrak{b}_i$, $\mathfrak{a} \subseteq \mathfrak{b}_i$ for some $i \in \{1, \cdots, n\}$.*

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