Commutative Algebra

September 6, 2018

Contents

Chapter 1

Introduction

Remark. Throughout this book, R is a CRW1, k is a field.

Remark (Application)**.** (1) In calculus, e.g., $\mathcal{C}(\mathbb{R})$ and $\mathcal{D}(\mathbb{R})$ are both CRW1's.

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

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

(3) In combinatorics, e.g., a simplicial complex Δ on V. Stanley-Reisner ideal $J(\Delta) \leq K[v_1, \cdots, v_d]$. Then

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

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

(4) In number theory, which study the solutions of polynomial equations over $\mathbb{Z}$, e.g., 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.

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

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

Remark. To study geometry, we need continuity. Let $V = V(f_1, \cdots, f_m)$, $W = V(g_1, \cdots, g_n)$ 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 2

Rings and Ideals

Remark (Fact)**.** $R = 0$ iff $1_R = 0_R$.

Remark (Fact)**.** (1) 1_R and 0_R are both unique.

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

(3) If $r \in R^\times$, then r^{-1} is also unique.

Defintion 2.0.1. A *subring* of R is a subset $S \subseteq R$ such that S is a CRW1 under the operations for R and $1_S = 1_R$, i.e., $1_R \in S$.

Remark (Subring test)**.** Need $\emptyset \neq S \subseteq R$, and S is closed under $+, \cdot, -$ and $1_R \in S$.

Example 2.0.2. $R = \mathbb{F}_3 \times \mathbb{F}_3 \supseteq \{(a, a) \mid a \in \mathbb{F}_3\} =: S$. Then S is a subring of R. Although $S_1 = \{(a, 0) \mid a \in \mathbb{F}_3\}$ and $S_2 = \{(0, a) \mid a \in \mathbb{F}_3\}$ are rings but not subrings of R since $1_R = (1, 1) \notin S_1$ and $1_R = (1, 1) \notin S_2$.

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

Defintion 2.0.3. An *ideal* of R is a non-empty set $\mathfrak{a} \subseteq R$ which is a subgroup under addition such that for any $r \in R$ and any $a \in \mathfrak{a}$, we have $ra \in \mathfrak{a}$.

(1) 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 $b \in \mathfrak{a}$.

(2) 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 $\mathfrak{b} = R$.

Remark (ideal test?)**.** A subset $\mathfrak{a} \subseteq R$ is an ideal iff $\mathfrak{a} \neq \emptyset$, $\mathfrak{a}$ is closed under $+$ and $\cdot$, since if $\mathfrak{a} \neq \emptyset$ and $\mathfrak{a}$ is closed under $\cdot$, then for any $a \in \mathfrak{a}$, $-a = (-1_R)a \in \mathfrak{a}$ and since $\mathfrak{a}$ is also closed under $+$, it is automatically closed under $-$.

Example 2.0.4. In $R = \mathbb{Z}$, ideals are $n\mathbb{Z} = \{nm \mid m \in \mathbb{Z}\}$, where $n \in \mathbb{Z}$.

(1) $n\mathbb{Z}$ is prime iff $n = 0$ or $|n|$ is prime.

(2) $n\mathbb{Z}$ is maximal iff $|n|$ is prime.

Example 2.0.5. (1) If $I_\lambda \leq R$ for any $\lambda \in \Lambda$, then $\bigcap_{\lambda\in\Lambda} I_\lambda \leq R$.

(2) If $r_1, \cdots, r_m \in R$, then $\langle r_1, \cdots, r_m\rangle = \langle r_1, \cdots, r_m\rangle R = (r_1, \cdots, r_m) = (r_1, \cdots, r_m)R = \bigcap_{r_1,\cdots,r_m \in I \leq R} I = \{\sum_{i=1}^{m} a_i r_i \mid a_i \in R,\ \forall\ i = 1, \cdots, n\} \leq R$. In particular, for any $r \in R$, $\langle r\rangle = \langle r\rangle R = (r) = (r)R = rR = Rr = \{ar \mid a \in R\} = \bigcap_{r\in I\leq R} I$.

(3) If $A \subseteq R$, then $\langle A\rangle = \bigcap_{A\subseteq I\leq R} I = \{\sum_{a\in A}^{\text{finite}} r_a a \mid r_a \in R\}$.

Remark (Fact)**.** 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 $\mathfrak{a} \leq R$, we have $r_1, \cdots, r_m \in \mathfrak{a}$ iff $\langle r_1, \cdots, r_m\rangle \subseteq \mathfrak{a}$. Similarly, $A \subseteq \mathfrak{a}$ iff $\langle A\rangle \subseteq \mathfrak{a}$.

Example 2.0.6. If $A \leq R$, then $A = \langle A\rangle$.

Remark (Construction)**.** Let $\mathfrak{a} \leq R$. For any $r \in R$: $r + \mathfrak{a} = \{r + a \mid a \in \mathfrak{a}\} = \overline{r}$. $R/\mathfrak{a} = \{r + \mathfrak{a} \mid r \in R\}$. Then $R/\mathfrak{a}$ is a CRW1. $\overline{r} \pm \overline{s} = \overline{r \pm s}$, $\overline{r}\,\overline{s} = \overline{rs}$, $0_{R/\mathfrak{a}} = \overline{0_R}$ and $1_{R/\mathfrak{a}} = \overline{1_R}$. Let $\pi : R \to R/\mathfrak{a}$ given by $\pi(r) = \overline{r}$. Then π is a well-defined ring homomorphism. Consider

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

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 $\mathfrak{a} \subseteq \mathrm{Ker}(\phi)$ and if $\mathfrak{a} = \langle A\rangle$, then $\mathfrak{a} \subseteq \mathrm{Ker}(\phi)$ iff $A \subseteq \mathrm{Ker}(\phi)$.

Remark (Fact)**.** Let $\mathfrak{a} \leq R$.

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

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

(3) If $\mathfrak{a}$ is maximal, then $\mathfrak{a}$ is prime.

Theorem 2.0.7 (ideal correspondence for quotients)**.** *Let $\mathfrak{a} \leq R$ and $\pi : R \to R/\mathfrak{a}$ be the canonical epimorphism. Then*

$$\{\text{ideals } I \leq R/\mathfrak{a}\} \rightleftarrows \{\text{ideals } J \leq R \mid \mathfrak{a} \subseteq J\}$$
$$I \mapsto \pi^{-1}(I)$$
$$J/\mathfrak{a} \mapsfrom J$$

$$\{\text{primes ideals of } R/\mathfrak{a}\} \rightleftarrows \{\text{prime ideals } \mathfrak{p} \leq R \mid \mathfrak{a} \subseteq \mathfrak{p}\}$$

$$\{\text{maximal ideals of } R/\mathfrak{a}\} \rightleftarrows \{\text{maximal ideals } \mathfrak{m} \leq R \mid \mathfrak{a} \subseteq \mathfrak{m}\}$$

Note maximal ideals are a subset of prime ideals and prime ideals are a subset of ideals.

Remark. The proof of $\frac{R/\mathfrak{a}}{J/\mathfrak{a}} \cong \frac{R}{J}$.

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

Clearly $J \subseteq \operatorname{Ker}(\tau \circ p)$ and we can use the UMP. Actually, $J = \operatorname{Ker}(\tau \circ p)$. Also, since $\operatorname{Ker}(\overline{\phi}) = 0 + J$, $\overline{\phi}$ 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., $\overline{\phi}(r + J) = (r + \mathfrak{a}) + J/\mathfrak{a}$.

Defintion 2.0.8. Let $\operatorname{Spec}(R) = \{\text{primes ideals of } R\}$, which is called the *prime spectrum of* R. Let $\operatorname{V}(\mathfrak{a}) = \{\mathfrak{p} \in \operatorname{Spec}(R) \mid \mathfrak{p} \supseteq \mathfrak{a}\}$.

Remark (Fact)**.** Let $\varphi : R \to S$ be a ring homomorphism. Then $\operatorname{Ker}(\varphi) \leq R$, $\operatorname{Im}(\varphi) \subseteq S$ is a subring and $\operatorname{Im}(\varphi) \cong R/\operatorname{Ker}(\varphi)$.
If S is an integral domain, then so is $\operatorname{Im}(\varphi)$. Hence $\operatorname{Ker}(\varphi)$ is prime. More generally, for any $\mathfrak{q} \leq S$, we have $\varphi^{-1}(\mathfrak{q}) = \{x \in R \mid \varphi(x) \in \mathfrak{q}\} \leq R$.
Let now $\mathfrak{q} \in \operatorname{Spec}(S)$. Then S/q is an integral domain. Since $R/\operatorname{Ker}(\pi \circ \varphi) \cong S/\mathfrak{q}$, $\operatorname{Ker}(\pi \circ \varphi)$ is prime. Note $\varphi^{-1}(\mathfrak{q}) = \operatorname{Ker}(\pi \circ \varphi)$, we have $\varphi^{-1}(\mathfrak{q})$ is prime, i.e., $\varphi^{-1}(\mathfrak{q}) \in \operatorname{Spec}(R)$. Thus, φ induces a well-defined map $\varphi^* : \operatorname{Spec}(S) \to \operatorname{Spec}(R)$.

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

Remark (Fact)**.** (1) 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, $V(\mathfrak{a}) \neq \emptyset$.

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

Defintion 2.0.9. R is *local* if it has a unique maximal ideal $\mathfrak{m}$, which is also known as (A.K.A) *quasi-local*. The *residue field* of R is $R/\mathfrak{m}$.

Remark (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.

Remark (Fact)**.** If $(R, \mathfrak{m})$ is local and $\mathfrak{a} \lneq R$, then $(R/\mathfrak{a}, \mathfrak{m}/\mathfrak{a})$ is also local and $\frac{R/\mathfrak{a}}{\mathfrak{m}/\mathfrak{a}} \cong R/\mathfrak{m}$ canonical isomorphic residue fields. Converse fails in general by h19.

Example 2.0.10. (1) Any field is local with the maximal ideal $\{0\}$.

(2) Let p be prime in $\mathbb{Z}$. Since $\mathbb{Z}$ is a PID, $\mathbb{Z}/\langle p^n \rangle$ 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 maximal, $\langle p \rangle = \langle \mathfrak{m}_1 \rangle$. 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, $\operatorname{Spec}(\mathbb{Z}/\langle p^n \rangle) = \{\langle p \rangle / \langle p^n \rangle\}$.

(3) Let $R = k[X]/\langle X^n \rangle$ is local with the maximal ideal $\langle X \rangle / \langle X^n \rangle$ and $\operatorname{Spec}(R) = \{k[X]/\langle X^n \rangle\}$.

(4) Let $R = \frac{k[X_1, \cdots, X_d]}{\langle X_1^{a_1} \cdots X_d^{a_d} \rangle}$, where $a_i \geq 1$ for any $i = 1, \cdots, d$. Then $\operatorname{Spec}(R) = \left\{ \frac{\langle X_1, \cdots, X_d \rangle}{\langle X_1^{a_1} \cdots X_d^{a_d} \rangle} \right\}$.

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

Proposition 2.0.11. *TFAE.*

(1) R is local.

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

(3) 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)". Claim $\mathfrak{m} = R \setminus R^\times$. It suffices to show $R \setminus \mathfrak{m} = R^\times$. "$\supseteq$". Let $u \in R^\times$. Then $u \notin \mathfrak{m}$ and so $R^\times \subseteq R \setminus \mathfrak{m}$. "$\subseteq$". Let $x \in R \setminus R^\times$. Since $1 \in R^\times$, $\langle x \rangle \lneq R$. Since $\mathfrak{m}$ is the unique maximal ideal in R, $\langle x \rangle \subseteq \mathfrak{m}$, i.e., $x \in \mathfrak{m}$. Thus, $R \setminus R^\times$, 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)". Claim $\mathfrak{a} = R \setminus R^\times$. "$\supseteq$". Let $\mathfrak{a} \lneq R$ such that $R \setminus \mathfrak{a} \subseteq R^\times$. Then $\mathfrak{a} \supseteq R \setminus R^\times$. "$\subseteq$". Let $a \in \mathfrak{a}$. Since $\mathfrak{a} \lneq R$, $a \notin R^\times$. So $a \in R \setminus R^\times$. Then $\mathfrak{a} \subseteq R \setminus R^\times$. 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, $\mathfrak{n} = \mathfrak{a}$. $\square$

Proposition 2.0.12. *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 $\langle x, \mathfrak{m} \rangle = \langle \{x\} \cup \mathfrak{m} \rangle = \{ax + m \mid a \in R, m \in \mathfrak{m}\}$. Then $\mathfrak{m} \subsetneq \langle x, \mathfrak{m} \rangle \leq R$. Since $\mathfrak{m}$ is maximal, $\langle x, \mathfrak{m} \rangle = R$. So $1 = ax + m$ for some $a \in R$ and $m \in \mathfrak{m}$, i.e., $ax = 1 - m \in 1 + \mathfrak{m} \subseteq R^\times$. Thus, $a, x \in R^\times$. $\square$

Defintion 2.0.13. $x \in R$ is *nilpotent* if there exists $n \in \mathbb{N}$ such that $x^n = 0$. Then *nilradical* of R is $\operatorname{Nil}(R) = \operatorname{N}(R) = \{\text{nilpotent elements of } R\}$.

Example 2.0.14. In $\mathbb{Z}/\langle p^n \rangle$, $\overline{p}$ is nilpotent. Similarly, in $k[x]/\langle x^n \rangle$ and $k[x_1, \cdots, x_n]/\langle x_1^{a_1}, \cdots, x_d^{a_d} \rangle$.

Proposition 2.0.15. *(1)* $\operatorname{Nil}(R) \leq R$*.*

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

(3) $\operatorname{Nil}(R) = R$ *iff* $R = 0$*.*

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

Proof. (1) Let $r \in R$ and $a, b \in \operatorname{Nil}(R)$. 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 $ra \in \operatorname{Nil}(R)$. Since $(a+b)^{m+n} = \sum_{i=0}^{m+n} \binom{m+n}{i} a^i b^{m+n-i} = 0$, we have $a + b \in \operatorname{Nil}(R)$.

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

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

(4) "$\subseteq$". Let $x \in \mathrm{Nil}(R)$. Then $x^n = 0 \in \mathfrak{p}$ 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 $x \in R \setminus \mathrm{Nil}(R)$. It suffices to show $x \notin \bigcap_{\mathfrak{p}\in\mathrm{Spec}(R)}$. It is enough 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 $x \neq 0$, $(0) \in \Sigma$ and then $\Sigma \neq \emptyset$. Let $\mathscr{C} \subseteq \Sigma$ be chain. Then $\mathfrak{q} := \bigcup_{\mathfrak{a}\in\mathscr{C}} \mathfrak{a} \leq R$. Suppose $x^n \in \mathfrak{q}$ for some $n \in \mathbb{N}$. Then $x^n \in \mathfrak{a}$ for some $\mathfrak{a} \in \mathscr{C} \subseteq \Sigma$, a contradiction. So $x^n \notin \mathfrak{q}$ for any $n \in \mathbb{N}$ and hence $\mathfrak{q} \in \Sigma$. Then $\mathfrak{q}$ is an upper bound for $\mathscr{C}$ in Σ. So by Zorn's lemma, Σ has a maximal element I. Claim I is prime. Suppose $I = R$. Then $x^n \in R = I$, a contradiction. So $I \lneq R$. Let $r, s \in R \setminus I$. Then $I \lneq \langle r, I\rangle \leq R$ and $I \lneq \langle s, I\rangle \leq R$. 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 $x^{m+n} = x^m x^n = (ar+i)(bs+j) = abrs + (arj + bsi + ij) \in \langle rs, I\rangle$. Hence $\langle rs, I\rangle \notin \Sigma$ and so $rs \notin I$. Thus, $I \in \mathrm{Spec}(R)$ such that $x \notin I$.

$\square$

Example 2.0.16. Let $R = \frac{k[X_1,\cdots,X_d]}{(X_1^{a_1},\cdots,X_d^{a_d})} \neq 0$. Then $\mathrm{Nil}(R) = \frac{\langle X_1,\cdots,X_d\rangle}{\langle X_1^{a_1},\cdots,X_d^{a_d}\rangle}$.

Proof. M1: This is the intersection of the unique prime ideal of R.
M2: Since $\overline{X}_i \in \mathrm{Nil}(R)$ for each $i = 1, \cdots, d$, we have $\overline{\langle X_1, \cdots, X_d\rangle} = \langle \overline{X}_1, \cdots, \overline{X}_d\rangle \subseteq \mathrm{Nil}(R) \subsetneq R$. Since $\overline{\langle X_1, \cdots, X_d\rangle}$ is maximal, we have $\mathrm{Nil}(R) = \overline{\langle X_1, \cdots, X_d\rangle}$. $\square$

Remark (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 $\langle \overline{r}_1, \cdots, \overline{r}_n\rangle = \frac{\langle r_1,\cdots,r_n\rangle}{\mathfrak{a}}$.

Defintion 2.0.17. The Jacobson radical of R is $\mathrm{Jac}(J) = \mathcal{R}(R) = \mathcal{J}(R) = \bigcap_{\mathfrak{m}\leq R \text{ max'l}} \mathfrak{m}$.

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

Proposition 2.0.18. $\mathcal{J}(R) = \{x \in R \mid 1 - xy \in R^\times,\ \forall\ y \in Y\}$.

Proof. "$\subseteq$". Let $x \in \mathcal{J}(R)$. 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 $x \in \mathcal{J}(R) \subseteq \mathfrak{m}$, $xy \in \mathfrak{m}$. 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 $x \notin \mathcal{J}(R)$. Then there exists $\mathfrak{m} \leq R$ maximal such that $x \notin \mathfrak{m}$. So $\mathfrak{m} \lneq \langle \mathfrak{m}, x\rangle \leq R$. Hence $\langle x, \mathfrak{m}\rangle = R$. Then there exists $y \in R$ and $m \in \mathfrak{m}$ such that $1 = xy + m$. Then $1 - xy = m \in \mathfrak{m}$. So $1 - xy \notin R^\times$, a contradiction. $\square$

2.1 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 Λ is an index set.

Defintion 2.1.1. $\mathfrak{a} + \mathfrak{b} = \langle \mathfrak{a} \cup \mathfrak{b}\rangle = \bigcap_{\mathfrak{a}\cup\mathfrak{b}\subseteq I\leq R}$.

Remark (Fact)**.** (1) $\mathfrak{a} + \mathfrak{b} \subseteq \mathfrak{c}$ iff $\mathfrak{a} \cup \mathfrak{b} \subseteq \mathfrak{c}$.

(2) $\mathfrak{a} + \mathfrak{b}$ is the (unique) smallest ideal of R that contains $\mathfrak{a} \cup \mathfrak{b}$.

Proposition 2.1.2. *(1)* $\mathfrak{a} + \mathfrak{b} = \{a + b \mid a \in \mathfrak{a}, b \in \mathfrak{b}\}$.

(2) If $\mathfrak{a} = \langle S\rangle$ *and* $\mathfrak{b} = \langle T\rangle$*, then* $\mathfrak{a}+\mathfrak{b} = \langle S\cup T\rangle$.

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

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

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

Proof. (1) Set $I = \{a+b \mid a\in\mathfrak{a}, b\in\mathfrak{b}\} \le R$. 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 (1), $\mathfrak{a}+\mathfrak{b}\subseteq I$. On the other hand (OTOH), for any $a+b\in I$, $a,b\in\mathfrak{a}\cup\mathfrak{b}\subseteq\mathfrak{a}+\mathfrak{b}\le R$. So $a+b\in\mathfrak{a}+\mathfrak{b}$.

(2) Let $I\le R$. $I\supseteq\mathfrak{a}\cup\mathfrak{b}$ 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 $\mathfrak{a}+\mathfrak{b} = \bigcap_{\mathfrak{a}\cup\mathfrak{b}\subseteq I\le R} I = \bigcap_{S\cup T\subseteq I\le R} I = \langle S\cup T\rangle$.

(3) By (2).

(4) By (1).

(5) 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 2.1.3. $m\mathbb{Z}+n\mathbb{Z} = \langle m,n\rangle\mathbb{Z} = \gcd(m,n)\mathbb{Z}$, where $m\neq 0$ or $n\neq 0$.

Remark (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 2.1.4. *(1)* $\mathrm{V}(S) = \mathrm{V}(\langle S\rangle)$ *for any* $S\subseteq R$.

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

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

(4) If $\mathfrak{a}\subseteq\mathfrak{b}$*, then* $\mathrm{V}(\mathfrak{a})\supseteq\mathrm{V}(\mathfrak{b})$.

(5) If $S\subseteq T\subseteq R$*, then* $\mathrm{V}(S)\supseteq\mathrm{V}(T)$.

Proof. (a) "$\supseteq$". Since $S\subseteq\langle S\rangle$, $\mathrm{V}(S)\supseteq\mathrm{V}(\langle S\rangle)$ by definition.
"$\subseteq$". 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 $\mathfrak{m}\le R$ maximal such that $\mathfrak{m}\supseteq\mathfrak{a}$. Since $\mathfrak{m}\in\mathrm{Spec}(R)$, $\mathfrak{m}\in\mathrm{V}(\mathfrak{a})$, a contradiction.

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

(d) Similar to (1).

(e) By (1) and (4).

□

Proposition 2.1.5. *(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 $\mathfrak{a}+\mathfrak{b} = \langle \mathfrak{a} \cup \mathfrak{b} \rangle$, $\mathrm{V}(\mathfrak{a}+\mathfrak{b}) = \mathrm{V}(\mathfrak{a}\cup\mathfrak{b})$. 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.

Remark (Fact)**.** (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) $\sum_{\lambda\in\Lambda} \mathfrak{a}_\lambda = \left\{ \sum_{\lambda\in\Lambda}^{\text{finite}} a_\lambda \,\middle|\, a_\lambda \in \mathfrak{a}_\lambda,\ \forall\ \lambda \in \Lambda \right\}$

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

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

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

Defintion 2.1.6. $\mathfrak{a}\mathfrak{b} = \langle N \rangle = \bigcap_{N \subseteq I \leq R} R$, where $N = \{ab \mid a \in \mathfrak{a}, b \in \mathfrak{b}\}$.

Remark (Fact)**.** Let $\mathfrak{a}\mathfrak{b} = \langle N \rangle$.

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

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

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

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

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

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

Proof. (c) Let $I = \{\sum_i^{\text{finite}} a_i b_i \mid a_i \in \mathfrak{a}, b_i \in \mathfrak{b}\} \leq R$. Then, by definition, $\mathfrak{a}\mathfrak{b} = \langle N \rangle = I$.

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

□

Proposition 2.1.7. *(a)* $\mathrm{V}(\mathfrak{a}\mathfrak{b}) = \mathrm{V}(\mathfrak{a}\cap\mathfrak{b}) = \mathrm{V}(\mathfrak{a}) \cup \mathrm{V}(\mathfrak{b})$.

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

Proof. (a) Let $\mathfrak{p} \in \mathrm{Spec}(R)$. Then $\mathfrak{p} \supseteq \mathfrak{a}\mathfrak{b}$ iff $\mathfrak{p} \supseteq \mathfrak{a}$ or $\mathfrak{p} \supseteq \mathfrak{b}$. So $\mathrm{V}(\mathfrak{a}\mathfrak{b}) = \mathrm{V}(\mathfrak{a}) \cup \mathrm{V}(\mathfrak{b})$. Since $\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{a}\cap\mathfrak{b}$, $\mathrm{V}(\mathfrak{a}\mathfrak{b}) \supseteq \mathrm{V}(\mathfrak{a}\cap\mathfrak{b})$. Let $\mathfrak{p} \in \mathrm{V}(\mathfrak{a}\mathfrak{b})$. Let $x \in \mathfrak{a}\cap\mathfrak{b}$. Then $x^2 = x \cdot x \in \mathfrak{a}\mathfrak{b} \subseteq \mathfrak{p}$. Since $\mathfrak{p}$ is prime, $x \in \mathfrak{p}$. So $\mathfrak{p} \subseteq \mathfrak{a}\cap\mathfrak{b}$ and then $\mathfrak{p} \in \mathrm{V}(\mathfrak{a}\cap\mathfrak{b})$. Hence $\mathrm{V}(\mathfrak{a}\mathfrak{b}) \subseteq \mathrm{V}(\mathfrak{a}\cap\mathfrak{b})$.

(b) $\mathrm{V}(\mathfrak{a}) \cap \mathrm{V}(\mathfrak{b}) = \mathrm{Spec}(R)$ iff $\mathrm{V}(\mathfrak{a}\mathfrak{b}) = \mathrm{Spec}(R)$ iff $\mathfrak{a}\mathfrak{b} \subseteq \mathrm{Nil}(R)$ and similarly for $\mathfrak{a}\cap\mathfrak{b}$.

□

Defintion 2.1.8. If $\mathfrak{a}+\mathfrak{b}=R$, then $\mathfrak{a}$ and $\mathfrak{b}$ are called "coprime" or "comaximal".

Proposition 2.1.9. *(a)* $\mathfrak{a}\mathfrak{b}=\mathfrak{b}\mathfrak{a}$ *and* $(\mathfrak{a}\mathfrak{b})\mathfrak{c}=\mathfrak{a}(\mathfrak{b}\mathfrak{c})$.

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

(c) If $\mathfrak{a}+\mathfrak{b}=R$*, then* $\mathfrak{a}\mathfrak{b}=\mathfrak{a}\cap\mathfrak{b}$.

(d) If R *is PID and* $\mathfrak{a}\mathfrak{b}=\mathfrak{a}\cap\mathfrak{b}$ *with* $\mathfrak{a}\neq 0\neq\mathfrak{b}$*, then* $\mathfrak{a}+\mathfrak{b}=R$.

Proof. (c) We always have $\mathfrak{a}\cap\mathfrak{b}\supseteq\mathfrak{a}\mathfrak{b}$.
M1: Assume $\mathfrak{a}+\mathfrak{b}=R$. Then $1=a+b$ for some $a\in\mathfrak{a}$ and $b\in\mathfrak{b}$. Let $x\in\mathfrak{a}\cap\mathfrak{b}$. Then $x=1\cdot x=(a+b)x=ax+bx\in\mathfrak{a}\mathfrak{b}$.
M2: $\mathfrak{a}\cap\mathfrak{b}=R(\mathfrak{a}\cap\mathfrak{b})=(\mathfrak{a}+\mathfrak{b})(\mathfrak{a}\cap\mathfrak{b})=\mathfrak{a}(\mathfrak{a}\cap\mathfrak{b})+\mathfrak{b}(\mathfrak{a}\cap\mathfrak{b})\subseteq\mathfrak{a}\mathfrak{b}$.

(d) Let R be 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 $\in\operatorname{Spec}(R)$ non-associates. Assume $\mathfrak{a}\cap\mathfrak{b}=\mathfrak{a}\mathfrak{b}$. Since R is a PID, $\mathfrak{a}\cap\mathfrak{b}=\operatorname{lcm}(p_1^{e_1}\cdots p_n^{e_n},p_1^{f_1}\cdots p_n^{f_n})R=\mathfrak{p}_1^{\max\{e_1,f_1\}}\cdots\mathfrak{p}_n^{\max\{e_n,f_n\}}$ and $\mathfrak{a}\mathfrak{b}=\mathfrak{p}_1^{e_1+f_1}\cdots\mathfrak{p}_n^{e_n+f_n}$. So $e_i=0$ or $f_i=0$ for any $i=1,\cdots,n$. In other words, for any $\mathfrak{p}\in\operatorname{Spec}(R)$, 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 $\mathfrak{p}\in\operatorname{Spec}(R)$. Thus, $\mathfrak{a}+\mathfrak{b}=R$.

□

Remark. You can do this for $\mathfrak{a}_1,\cdots,\mathfrak{a}_n$.
If R is not a UFD, (4) may fail. For example, $R=k[x,y]$. Let $\mathfrak{a}=\langle x\rangle$ and $\mathfrak{b}=\langle y\rangle$. Then $\mathfrak{a}\cap\mathfrak{b}=\langle xy\rangle=\mathfrak{a}\mathfrak{b}$. But $\mathfrak{a}+\mathfrak{b}=\langle x,y\rangle\subsetneq R$.

Defintion 2.1.10. Let $\mathfrak{a}\leq R$ and $n\in\mathbb{N}$. Let $\mathfrak{a}^n=\underbrace{\mathfrak{a}\cdots\mathfrak{a}}_{n\text{ times}}$ and $\mathfrak{a}^0=R$.

Remark (Warning)**.** $\mathfrak{a}^n$ 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 $\mathfrak{a}^2=\langle x^2,xy,y^2\rangle\neq\langle f^2\mid f\in\mathfrak{a}\rangle\not\ni xy$.

Proposition 2.1.11. *(a) Let* $\mathfrak{a}^n=\langle N\rangle$*. Then for any* $\mathfrak{b}\leq R$, $\mathfrak{a}^n\subseteq\mathfrak{b}$ *iff* $N\subseteq\mathfrak{b}$.

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

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

(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* $\mathfrak{a}^n=\langle x_{i_1}\cdots x_{i_n}\mid i_j=1,\cdots,m,\ \forall\ j=1,\cdots,n\rangle$.

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

Proposition 2.1.12. *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* $1\leq i\neq j\leq R$*, then* $\bigcap_{i=1}^n\mathfrak{a}_i=\mathfrak{a}_1\cdots\mathfrak{a}_n$ *and* $\mathfrak{a}_i+(\bigcap_{j\neq i}\mathfrak{a}_j)R=R$.

(c) ϕ *is surjective iff* $\mathfrak{a}_i+\mathfrak{b}_j=R$ *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* $1 \le i \ne j \le R$ *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. (2) To show $\mathfrak{a}_i + (\bigcap_{j\ne i})R = R$. It suffices to show $V() \ne \emptyset$.

(3) "$\Rightarrow$". Assume ϕ 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 $2 \le i \le n$. Hence $1 - x \in \mathfrak{a}_1$ and $x \in \mathfrak{a}_i$ for any $2 \le i \le n$. Also, since $1 = (1-x) + x$, we have $\mathfrak{a}_1 + \mathfrak{a}_i = R$ for any $2 \le i \le n$. Consider $(\overline{0}, \cdots, \overline{0}, \overline{1}, \overline{0}, \cdots, \overline{0})$ arrow $\mathfrak{a}_i + \mathfrak{a}_j = R$ for any $1 \le i \ne j \le n$.
"$\Leftarrow$". Assume $\mathfrak{a}_i + \mathfrak{b}_j = R$ for any $1 \le i \ne j \le n$. By (2), $\mathfrak{a}_1 + (\bigcap_{i=2}^n \mathfrak{a}_i)R = R$. So $1 = a_1 + y$ with $a_1 \in \mathfrak{a}_1$ and $y \in \bigcap_{i=2}^n \mathfrak{a}_i$. Then $\phi(y) = (\overline{y}, \overline{y}, \cdots, \overline{y}) = (y + \mathfrak{a}_1, y + \mathfrak{b}_2, \cdots, y + \mathfrak{a}_n) = (1 + \mathfrak{a}_1, 0 + \mathfrak{a}_2, \cdots, 0 + \mathfrak{a}_n) = (\overline{1}, \overline{0}, \cdots, \overline{0})$. Similarly, for any $i = 1, \cdots, n$, there exists y_i such that $\phi(y_i) = (\overline{0}, \cdots, \overline{0}, \overline{1}, \overline{0}, \cdots, \overline{0})$. Then for any $(\overline{r}_1, \cdots, \overline{r}_n) \in \frac{R}{\mathfrak{a}_1} \times \cdots \times \frac{R}{\mathfrak{a}_n}$, $(\overline{r}_1, \cdots, \overline{r}_n) = \sum_{i=1}^n r_i((\overline{0}, \cdots, \overline{0}, \overline{1}, \overline{0}, \cdots, \overline{0})) = \sum_{i=1}^n r_i \phi(y_i) = \phi(\sum_{i=1}^n r_i y_i)$.

□

Proposition 2.1.13. *Let* $\mathfrak{a}_1, \cdots, \mathfrak{a}_n \le R$ *and* $\mathfrak{p} \in \mathrm{Spec}(R)$.

(a) If $\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_n$*, 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. (2) Assume $\mathfrak{p}_1 \cap \cdots \mathfrak{p}_n \supseteq \mathfrak{a}_1 \cdots \mathfrak{a}_n$. Since $\mathfrak{p} \in \mathrm{Spec}(R)$, there exists $i \in \{1, \cdots, n\}$ such that $\mathfrak{p} \supseteq \mathfrak{a}_i$.

□

Fact 1.