Chapter 1: Rings and Ideals

Author: Meng-Gen Tsai
Email: plover@gmail.com

Exercise 1.1. *Let x be a nilpotent element of A. Show that $1 + x$ is a unit of A. Deduce that the sum of a nilpotent element and a unit is a unit.*

Proof.

(1) Suppose $x^m = 0$ for some odd integer $m \geq 0$. Then

$$1 = 1 + x^m = (1 + x)(1 - x + x^2 - \cdots + (-1)^{m-1}x^{m-1}),$$

or $1 + x$ is a unit.

(2) If u is any unit and x is any nilpotent, $u + x = u \cdot (1 + u^{-1}x)$ is a product of two units (using that $u^{-1}x$ is nilpotent and applying (1)) and hence a unit again.

□

Proof (Proposition 1.9).

(1) *The nilradical is a subset of the Jacobson radical.*

  (a) The nilradical $\mathfrak{N}$ of A is the intersection of all the prime ideals of A by Proposition 1.8.

  (b) The Jacobson radical $\mathfrak{J}$ of A is the intersection of all the maximal ideals of A by definition.

(2) By Proposition 1.9, $x \in \mathfrak{J}$ if and only if $1 - xy$ is a unit in A for all $y \in A$. So $1 + x = 1 - (-x) \cdot 1$ is a unit in A since x is a nilpotent and $\mathfrak{J}$ is an ideal.

□

Exercise 1.2. *Let A be a ring and let $A[x]$ be the ring of polynomials in an indeterminate x, with coefficients in A. Let $f = a_0 + a_1x + \cdots + a_nx^n \in A[x]$. Prove that*

(i) *f is a unit in $A[x]$ if and only if a_0 is a unit in A and $a_1, ..., a_n$ are nilpotent. (Hint: If $b_0 + b_1x + \cdots + b_mx^m$ is the inverse of f, prove by induction on r that $a_n^{r+1}b_{m-r} = 0$. Hence show that a_n is nilpotent, and then use Exercise 1.1.)*

(ii) *f is nilpotent if and only if $a_0, a_1, ..., a_n$ are nilpotent.*

(iii) *f is a zero-divisor if and only if there exists $a \neq 0$ such that $af = 0$. (Hint: Choose a polynomial $g = b_0 + b_1 x + \cdots + b_m x^m$ of least degree m such that $fg = 0$. Then $a_n b_m = 0$, hence $a_n g = 0$ (because $a_n g$ annihilates f and has degree $< m$). Now show by induction that $a_{n-r} g = 0$ $(0 \leq r \leq n)$.)*

(iv) *f is said to be primitive if $(a_0, a_1, ..., a_n) = (1)$. Prove that if $f, g \in A[x]$, then fg is primitive if and only if f and g are primitive.*

Proof of (i).

(1) ($\Longleftarrow$) holds by Exercise 1.1.

(2) ($\Longrightarrow$) There exists the inverse g of f, say $g = b_0 + b_1 x + \cdots + b_m x^m$ satisfying $1 = fg$. Clearly, $1 = a_0 b_0$, or a_0 is a unit in A. Also,

$$\begin{aligned}
0 &= a_n b_m, \\
0 &= a_n b_{m-1} + a_{n-1} b_m, \\
0 &= a_n b_{m-2} + a_{n-1} b_{m-1} + a_{n-2} b_m, \\
&\cdots
\end{aligned}$$

A direct computing shows that

$$\begin{aligned}
0 &= a_n^1 b_m, \\
0 &= a_n (a_n b_{m-1} + a_{n-1} b_m) \\
&= a_n^2 b_{m-1} + a_{n-1} a_n b_m \\
&= a_n^2 b_{m-1}, \\
0 &= a_n^2 (a_n b_{m-2} + a_{n-1} b_{m-1} + a_{n-2} b_m) \\
&= a_n^3 b_{m-2} + a_{n-1} a_n^2 b_{m-1} + a_{n-2} a_n^2 b_m \\
&= a_n^3 b_{m-2}, \\
&\cdots
\end{aligned}$$

So we might have $a_n^{r+1} b_{m-r} = 0$ for $r = 0, 1, 2, ..., m$.

(3) *Show that $a_n^{r+1} b_{m-r} = 0$ for $r = 0, 1, 2, ..., m$ by induction on r.*

(a) As $r = 0$, $a_n b_m = 0$ by comparing the coefficient of $fg = 1$ at x^{n+m}.

(b) For any $r > 0$, comparing the coefficient of $fg = 1$ at x^{n+m-r},

$$0 = a_n b_{m-r} + a_{n-1} b_{m-r+1} + \cdots + a_{n-r} b_m.$$

Multiplying by a_n^r on the both sides,

$$\begin{aligned}
0 &= a_n^{r+1} b_{m-r} + a_{n-1} a_n^r b_{m-r+1} + \cdots + a_{n-r} a_n^r b_m \\
&= a_n^{r+1} b_{m-r}.
\end{aligned}$$

by the induction hypothesis.

(4) a_n *is a nilpotent.* Putting $r = m$ in $a_n^{r+1} b_{m-r} = 0$ and get $a_n^{m+1} b_0 = 0$. Notice that b_0 is a unit, $a_n^{m+1} = 0$, or a_n is a nilpotent.

(5) Consider $f - a_n x^n = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1}$, a polynomial $\in A[x]$ of degree $n-1$. Note that f is a unit and $a_n x^n$ is a nilpotent. By Exercise 1.1, $f - a_n x^n$ is a unit too. Applying the (2)(3)(4) again, a_{n-1} is a nilpotent as $n - 1 > 0$, that is, applying descending induction on n then yields the desired property.

□

Proof of (ii).

(1) ($\Longleftarrow$) holds since the nilradical of any ring is an ideal.

(2) ($\Longrightarrow$) $f^N = 0$ for some $N > 0$. So $0 = f^N = a_n^N x^{nN} + \cdots + a_0^N$. Comparing the coefficient in the leading term x^{nN} leads to $a_n^N = 0$, or a_n is a nilpotent.

(3) Consider $f - a_n x^n = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1}$, a polynomial $\in A[x]$ of degree $n - 1$. Note that f and $a_n x^n$ are nilpotent. $f - a_n x^n$ is a nilpotent too. Similar to step (5) in the proof of (i), applying descending induction on n then yields the desired property.

□

Proof of (iii).

(1) ($\Longleftarrow$) holds trivially.

(2) ($\Longrightarrow$) Pick a polynomial $g = b_0 + b_1 x + \cdots + b_m x^m$ of least degree m such that $fg = 0$. Especially, $a_n b_m = 0$.

(3) Consider

$$\begin{aligned} a_n g &= a_n b_0 + \cdots + a_n b_{m-1} x^{m-1} + a_n b_m x^m \\ &= a_n b_0 + \cdots + a_n b_{m-1} x^{m-1} \end{aligned}$$

(since $a_n b_m = 0$). $a_n g$ is a polynomial over A of having degree strictly less than m. Notice that $f \cdot (a_n g) = a_n \cdot (fg) = 0$. By minimality of m, $a_n g = 0$.

(4) Induction on the degree n of f.

(a) As $n = 0$, $f = a_0$. There exists $b_m \neq 0$ such that $b_m f = b_m a_0 = 0$ by (2).

(b) For any zero-divisor f of degree n, there is a polynomial $g = b_0 + b_1 x + \cdots + b_m x^m$ of least degree m such that $fg = 0$. By (2)(3),

$$\begin{aligned} (f - a_n x^n) \cdot g &= fg - a_n x^n g \\ &= 0 - 0 \\ &= 0. \end{aligned}$$

That is, $f - a_n x^n$ is a zero-divisor of degree $n-1$. By the induction hypothesis, there exists $b_m \neq 0$ such that $b_m(f - a_n x^n) = 0$. So $b_m f = b_m(f - a_n x^n) + b_m a_n x^n = 0 + 0 = 0$.

(c) By (a)(b), ($\Longrightarrow$) holds by mathematical induction.

$\square$

Proof of (iv). Note that

(1) $f \notin \mathfrak{m}[x]$ for any maximal ideal $\mathfrak{m}$ of A if and only if f is primitive.

(2) For any maximal ideal $\mathfrak{m}$ of A, $A/\mathfrak{m}$ is a field (or an integral domain).

(3) $A[x]$ is an integral domain if A is an integral domain.

(4) $A[x]/\mathfrak{m}[x] \cong (A/\mathfrak{m})[x]$ as a ring isomorphism.

Hence,

$$\begin{aligned}
f, g: \text{ primitive} &\Longleftrightarrow f, g \notin \mathfrak{m}[x] \text{ for any maximal ideal } \mathfrak{m} \\
&\Longleftrightarrow f, g \neq 0 \text{ in } (A/\mathfrak{m})[x] \text{ for any maximal ideal } \mathfrak{m} \\
&\Longleftrightarrow fg \neq 0 \text{ in } (A/\mathfrak{m})[x] \text{ for any maximal ideal } \mathfrak{m} \\
&\Longleftrightarrow fg \notin \mathfrak{m}[x] \text{ for any maximal ideal } \mathfrak{m} \\
&\Longleftrightarrow fg: \text{ primitive.}
\end{aligned}$$

$\square$

Exercise 1.4. *In the ring $A[x]$, the Jacobson radical is equal to the nilradical.*

Proof.

(1) The nilradical $\mathfrak{N}$ is a subset of the Jacobson radical $\mathfrak{J}$. It suffices to show that $\mathfrak{J} \subseteq \mathfrak{N}$.

(2) Given any $f \in \mathfrak{J}$. By Proposition 1.9, $f \in \mathfrak{J}$ if and only if $1 - fy$ is a unit in $A[x]$ for all $y \in A[x]$. Especially, pick $y = x \in A[x]$ and then $1 - xf$ is a unit in $A[x]$.

(3) By Exercise 1.2 (i), all coefficients of f are nilpotent. By Exercise 1.2 (ii), f is nilpotent, or $f \in \mathfrak{N}$.

$\square$

Exercise 1.7. *Let A be a ring in which every element satisfies $x^n = x$ for some $n > 1$ (depending on x). Show that every prime ideal in A is maximal.*

Proof. It suffices to show that *for any prime ideal $\mathfrak{p}$ in A, $A/\mathfrak{p}$ is a field.*

(1) Take any $0 \neq \overline{x} \in A/\mathfrak{p}$, which is represented by $x \in A - \mathfrak{p}$. By assumption there exists $n \geq 2$ such that $x^n = x$. So $\overline{x}^n = \overline{x}$ or $\overline{x}(\overline{x}^{n-1} - 1) = 0$.

(2) Since $\mathfrak{p}$ is prime, $A/\mathfrak{p}$ is a integral domain. That is, $\overline{x} = 0$ (impossible) or $\overline{x}^{n-1} - 1 = 0$. Write $\overline{x} \cdot \overline{x}^{n-2} = 1$ in $A/\mathfrak{p}$. So $\overline{x}^{n-2}$ is an inverse of $\overline{x} \neq 0$ in $A/\mathfrak{p}$, which implies that $A/\mathfrak{p}$ is a field (since $\overline{x}$ is arbitrary).

(3) $A/\mathfrak{p}$ is a field if and only if $\mathfrak{p}$ is maximal.

□

Exercise 1.8. *Let A be a ring $\neq 0$. Show that the set of prime ideals of A has minimal elements with respect to inclusion.*

Similar to Theorem 1.3.

Proof (Zorn's Lemma).

(1) Let Σ be the set of all prime ideals of A.

(2) Order Σ by $\supseteq$, that is, $\mathfrak{p} \leq \mathfrak{q}$ if $\mathfrak{p} \supseteq \mathfrak{q}$.

(3) Σ is not empty, since every ring $A \neq 0$ has at least one maximal ideal (or prime ideal) (Theorem 1.3).

(4) To apply Zorn's lemma we must show that every chain in Σ has a lower bound in Σ; let then $(\mathfrak{p}_\alpha)$ be a chain of prime ideals in Σ, so that for each pair of indices α, β we have either $\mathfrak{p}_\alpha \subseteq \mathfrak{p}_\beta$ or $\mathfrak{p}_\beta \subseteq \mathfrak{p}_\alpha$. Let $\mathfrak{p} = \bigcap_\alpha \mathfrak{p}_\alpha$.

(5) *Show that $\mathfrak{p}$ is a prime ideal.* Clearly $\mathfrak{p}$ is an ideal. Given any $xy \in \mathfrak{p}$ and $x \notin \mathfrak{p}$. So xy is in all prime ideals $\mathfrak{p}_\alpha$. By assumption $x \notin \mathfrak{p}$, there is some β such that $x \notin \mathfrak{p}_\beta$, or $x \notin \mathfrak{p}_\alpha$ whenever $\alpha \geq \beta$. So $y \in \mathfrak{p}_\alpha$ whenever $\alpha \geq \beta$. Since $y \in \mathfrak{p}_\beta$, $y \in \mathfrak{p}_\gamma$ whenever $\beta \geq \gamma$. Therefore, $y \in \mathfrak{p}_\alpha$ for all α, or $y \in \mathfrak{p}$, or $\mathfrak{p}$ is prime.

□

Exercise 1.9. *Let $\mathfrak{a}$ be an ideal $\neq (1)$ in a ring A. Show that $\mathfrak{a} = r(\mathfrak{a}) \Longleftrightarrow \mathfrak{a}$ is an intersection of prime ideals.*

Proof.

(1) $(\Longrightarrow)$. By Proposition 1.14, $\mathfrak{a} = r(\mathfrak{a})$ is the intersection of the prime ideals which contain $\mathfrak{a}$.

(2) ($\Longleftarrow$).

$$\begin{aligned}
\mathfrak{a} &= \bigcap\{\mathfrak{p} \in \text{some subset of } \mathrm{Spec}(A)\} \\
&= \bigcap\{\mathfrak{p} \in \text{some subset of } \mathrm{Spec}(A) : \mathfrak{p} \supseteq \mathfrak{a}\} \\
&\supseteq \bigcap\{\mathfrak{p} \in \mathrm{Spec}(A) : \mathfrak{p} \supseteq \mathfrak{a}\} \\
&= r(\mathfrak{a}) \\
&\supseteq \mathfrak{a}.
\end{aligned}$$

$\square$

The prime spectrum of a ring

Exercise 1.15. *Let A be a ring and let X be the set of all prime ideals of A. For each subset E of A, let $V(E)$ denote the set of all prime ideals of A which contain E. Prove that*

(i) *if $\mathfrak{a}$ is the ideal generated by E, then $V(E) = V(\mathfrak{a}) = V(r(\mathfrak{a}))$.*

(ii) $V(0) = X$, $V(1) = \varnothing$.

(iii) *if $(E_i)_{i \in I}$ is any family of subsets of A, then*

$$V\left(\bigcup_{i \in I} E_i\right) = \bigcap_{i \in I} V(E_i).$$

(iv) $V(\mathfrak{a} \cap \mathfrak{b}) = V(\mathfrak{a}\mathfrak{b}) = V(\mathfrak{a}) \cup V(\mathfrak{b})$ *for any ideals $\mathfrak{a}$, $\mathfrak{b}$ of A.*

The results show that the sets $V(E)$ satisfy the axioms for closed sets in a topological space. The resulting topology is called the Zariski topology. The topological space X is called the prime spectrum of A, and is written Spec(A).

Note that if $E_1 \subseteq E_2$, then $V(E_1) \supseteq V(E_2)$.

Proof of (i).

(1) *Show that $V(E) = V(\mathfrak{a})$.*

  (a) *Show that $V(E) \subseteq V(\mathfrak{a})$.* Given any $\mathfrak{p} \in V(E)$, $\mathfrak{p} \supseteq E$. For any $a \in \mathfrak{a}$, since $\mathfrak{a}$ is generated by E, we can write a as a finite sum $a = \sum \alpha\beta$ where $\alpha \in A$ and $\beta \in E$. Since $E \subseteq \mathfrak{p}$, all $\beta \in \mathfrak{p}$. Since $\mathfrak{p}$ is an ideal, $a = \sum \alpha\beta \in \mathfrak{p}$. That is, $\mathfrak{p} \supseteq \mathfrak{a}$, or $\mathfrak{p} \in V(\mathfrak{a})$.

  (b) $V(E) \supseteq V(\mathfrak{a})$ since $\mathfrak{a} \supseteq E$.

(2) *Show that $V(\mathfrak{a}) = V(r(\mathfrak{a}))$.*

(a) *Show that* $V(\mathfrak{a}) \subseteq V(r(\mathfrak{a}))$. Given any $\mathfrak{p} \in V(\mathfrak{a})$,

$$\begin{aligned}
\mathfrak{p} \in V(\mathfrak{a}) &\Longrightarrow \mathfrak{p} \supseteq \mathfrak{a} \\
&\Longrightarrow \mathfrak{p} \supseteq \text{the intersection of the primes ideals } \mathfrak{p} \supseteq \mathfrak{a} \\
&\Longrightarrow \mathfrak{p} \supseteq r(\mathfrak{a}) \text{ (by Proposition 1.14)} \\
&\Longrightarrow \mathfrak{p} \in V(r(\mathfrak{a})).
\end{aligned}$$

(b) $V(\mathfrak{a}) \supseteq V(r(\mathfrak{a}))$ since $r(\mathfrak{a}) \supseteq \mathfrak{a}$.

□

Proof of (ii).

(1) $V(1) = \varnothing$ since no prime ideal contains 1 by definition.

(2) $V(0) = X$ since 0 is in every ideal (especially in every prime ideal).

□

Proof of (iii).

$$\begin{aligned}
\mathfrak{p} \in V\left(\bigcup_{i \in I} E_i\right) &\Longleftrightarrow \mathfrak{p} \supseteq \bigcup_{i \in I} E_i \\
&\Longleftrightarrow \mathfrak{p} \supseteq E_i \text{ for all } i \in I \\
&\Longleftrightarrow \mathfrak{p} \in V(E_i) \text{ for all } i \in I \\
&\Longleftrightarrow \mathfrak{p} \in \bigcap_{i \in I} V(E_i).
\end{aligned}$$

□

Lemma. *For any* $\mathfrak{p} \supseteq \mathfrak{a}\mathfrak{b}$, $\mathfrak{p} \supseteq \mathfrak{a}$ *or* $\mathfrak{p} \supseteq \mathfrak{b}$.

Proof of Lemma.

(1) If $\mathfrak{p} \supseteq \mathfrak{a}$. We are done.

(2) If $\mathfrak{p} \not\supseteq \mathfrak{a}$, there exists $a \in \mathfrak{a} - \mathfrak{p}$. So for any $b \in \mathfrak{b}$, $b \in \mathfrak{p}$ since $ab \in \mathfrak{a}\mathfrak{b} \subseteq \mathfrak{p}$ and $\mathfrak{p}$ is a prime ideal, that is, $\mathfrak{p} \supseteq \mathfrak{b}$.

By (1)(2), $\mathfrak{p} \supseteq \mathfrak{a}$ or $\mathfrak{p} \supseteq \mathfrak{b}$. □

Proof of (iv).

(1) *Show that* $V(\mathfrak{a} \cap \mathfrak{b}) = V(\mathfrak{a}\mathfrak{b})$.

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

(b) *Show that* $V(\mathfrak{a}\cap\mathfrak{b}) \supseteq V(\mathfrak{a}\mathfrak{b})$. Given any $\mathfrak{p} \in V(\mathfrak{a}\mathfrak{b})$, $\mathfrak{p} \supseteq \mathfrak{a}\mathfrak{b}$. By Lemma, $\mathfrak{p} \supseteq \mathfrak{a}$ or $\mathfrak{p} \supseteq \mathfrak{b}$. Notice that $\mathfrak{a} \supseteq \mathfrak{a}\cap\mathfrak{b}$ and $\mathfrak{b} \supseteq \mathfrak{a}\cap\mathfrak{b}$. In any case, $\mathfrak{p} \supseteq \mathfrak{a}\cap\mathfrak{b}$, $\mathfrak{p} \in V(\mathfrak{a}\cap\mathfrak{b})$.

(2) *Show that* $V(\mathfrak{a}\mathfrak{b}) = V(\mathfrak{a}) \cup V(\mathfrak{b})$.

(a) *Show that* $V(\mathfrak{a}\mathfrak{b}) \subseteq V(\mathfrak{a}) \cup V(\mathfrak{b})$. Given any $\mathfrak{p} \in V(\mathfrak{a}\mathfrak{b})$, $\mathfrak{p} \supseteq \mathfrak{a}\mathfrak{b}$. By Lemma, $\mathfrak{p} \supseteq \mathfrak{a}$ or $\mathfrak{p} \supseteq \mathfrak{b}$, $\mathfrak{p} \in V(\mathfrak{a})$ or $\mathfrak{p} \in V(\mathfrak{b})$, $\mathfrak{p} \in V(\mathfrak{a}) \cup V(\mathfrak{b})$.

(b) *Show that* $V(\mathfrak{a}\mathfrak{b}) \supseteq V(\mathfrak{a})\cup V(\mathfrak{b})$. Given any $\mathfrak{p} \in V(\mathfrak{a})\cup V(\mathfrak{b})$, $\mathfrak{p} \in V(\mathfrak{a})$ or $\mathfrak{p} \in V(\mathfrak{b})$, $\mathfrak{p} \supseteq \mathfrak{a}$ or $\mathfrak{p} \supseteq \mathfrak{b}$. Notice that $\mathfrak{a} \supseteq \mathfrak{a}\mathfrak{b}$ and $\mathfrak{b} \supseteq \mathfrak{a}\mathfrak{b}$. In any cases, $\mathfrak{p} \supseteq \mathfrak{a}\mathfrak{b}$, or $\mathfrak{p} \in V(\mathfrak{a}\mathfrak{b})$.

$\square$

Exercise 1.17. *For each $f \in A$, let X_f denote the complement of $V(f)$ in $X = Spec(A)$. The sets X_f are open. Show that they form a basis of open sets for the Zariski topology, and that*

(i) $X_f \cap X_g = X_{fg}$.

(ii) $X_f = \varnothing \Longleftrightarrow f$ *is nilpotent.*

(iii) $X_f = X \Longleftrightarrow f$ *is a unit.*

(iv) $X_f = X_g \Longleftrightarrow r((f)) = r((g))$.

(v) *X is quasi-compact (compact), that is, every open covering of X has a finite subcovering.*

(vi) *More generally, each X_f is quasi-compact.*

(vii) *An open subset of X is quasi-compact if and only if it is a finite union of sets X_f.*

The sets X_f are called basic open sets of $X = Spec(A)$.

(Hint: To prove (v), remark that it is enough to consider a covering of X by basic open sets $X_{f_i} (i \in I)$. Show that the f_i generate the unit ideal and hence that there is an equation of the form

$$1 = \sum_{i\in J} g_i f_i \quad (g_i \in A)$$

where J is some finite subset of I. Then the $X_{f_i} (i \in J)$ cover X.)

Proof of basis. It is equivalent to Exercise 1.15 (iii). Given any open set O in X. Write $O = X - V(\mathfrak{a})$ for some ideal $\mathfrak{a}$ of A. Since

$$V(\mathfrak{a}) = V\left(\bigcup_{f\in\mathfrak{a}}(f)\right) = \bigcap_{f\in\mathfrak{a}} V(f),$$

we have

$$O = X - V(\mathfrak{a}) = X - \bigcap_{f\in\mathfrak{a}} V(f) = \bigcup_{f\in\mathfrak{a}} (X - V(f)) = \bigcup_{f\in\mathfrak{a}} X_f,$$

or any open set is a union of basic open sets. □

Proof of (i). $X_f \cap X_g = X_{fg} \iff V(f) \cup V(g) = V(fg)$ holds by Exercise 1.15 (iv). □

Proof of (ii).

$$\begin{aligned} X_f = \varnothing &\iff V(f) = X \\ &\iff f \in \mathfrak{p} \text{ for all prime ideal } \mathfrak{p} \text{ of } A \\ &\iff f \in \mathfrak{N}, \text{the nilradical of } A \text{ (Proposition 1.8)} \\ &\iff f \text{ is nilpotent (Proposition 1.7)} \end{aligned}$$

□

Proof of (ii)(Using (iv)).

$$\begin{aligned} X_f = \varnothing &\iff X_f = X_0 && \text{(Exercise 15(ii))} \\ &\iff r(f) = r(0) && \text{((iv))} \\ &\iff f \in r(f) = r(0) \\ &\iff f^m = 0 \text{ for some } m > 0 \\ &\iff f \text{ is nilpotent} \end{aligned}$$

□

Proof of (iii).

$$\begin{aligned} X_f = X &\iff V(f) = \varnothing \\ &\iff f \notin \mathfrak{p} \text{ for all prime ideal } \mathfrak{p} \text{ of } A \\ &\iff f \text{ is unit (Corollary 1.5)} \end{aligned}$$

□

Proof of (iii)(Using (iv)).

$$\begin{aligned} X_f = X &\iff X_f = X_1 && \text{(Exercise 15(ii))} \\ &\iff r(f) = r(1) && \text{((iv))} \\ &\iff f \in r(f) = r(1) \\ &\iff f^m = 1 \text{ for some } m > 0 \\ &\iff f \text{ is unit} \end{aligned}$$

□

Proof of (iv).

(1) *Show that* $X_f \subseteq X_g \Longleftrightarrow r((f)) \subseteq r((g))$. Actually,

$$\begin{aligned}
X_f \subseteq X_g &\Longrightarrow V(f) \supseteq V(g) \\
&\Longrightarrow \{\mathfrak{p} \in \operatorname{Spec}(A) : \mathfrak{p} \supseteq (f)\} \supseteq \{\mathfrak{p} \in \operatorname{Spec}(A) : \mathfrak{p} \supseteq (g)\} \\
&\Longrightarrow \bigcap_{(f)\subseteq\mathfrak{p}\in\operatorname{Spec}(A)} \mathfrak{p} \subseteq \bigcap_{(g)\subseteq\mathfrak{p}\in\operatorname{Spec}(A)} \mathfrak{p} \\
&\overset{1.14}{\Longrightarrow} r(f) \subseteq r(g) \\
&\Longrightarrow V(r(f)) \supseteq V(r(g)) \\
&\Longrightarrow V(f) \supseteq V(g) \\
&\Longrightarrow X_f \subseteq X_g.
\end{aligned}$$

(2) By (1),

$$\begin{aligned}
X_f \subseteq X_g &\Longleftrightarrow r((f)) \subseteq r((g)), \\
X_f \supseteq X_g &\Longleftrightarrow r((f)) \supseteq r((g)).
\end{aligned}$$

Hence,

$$X_f = X_g \Longleftrightarrow r((f)) = r((g)).$$

□

Proof of (v). Notice that it is enough to consider a covering of X by basic open sets $X_{f_i} (i \in I)$.

(1) Since X is covered by $X_{f_i} (i \in I)$,

$$\begin{aligned}
X = \bigcup_{i\in I} X_{f_i} &\Longrightarrow X - V(1) = \bigcup_{i\in I} (X - V(f_i)) \\
&\Longrightarrow V(1) = \bigcap_{i\in I} V(f_i) \\
&\Longrightarrow V(1) = V\left(\sum_{i\in I} f_i\right) \\
&\Longrightarrow r(1) = r\left(\sum_{i\in I} f_i\right).
\end{aligned}$$

Hence, $1 \in r(1) = r\left(\sum_{i\in I} f_i\right)$ can be expressed as

$$1 = 1^m = \sum_{j\in J} g_j f_j$$

where J is a finite subset of I and $g_j \in A$. That is, $(1) = \sum_{j\in J} f_j$.

(2) Hence, $V(1) = V\left(\sum_{j\in J} f_j\right)$. Therefore, X is covered by finite subcovering $\{X_{f_j}\}(j \in J)$.

$\square$

Proof of (v)(Using (vi)). Since $X = X_1$, X is quasi-compact by (vi). $\square$

Proof of (vi). Notice that it is enough to consider a covering of X_f by basic open sets $X_{f_i}(i \in I)$.

(1) Since X_f is covered by $X_{f_i}(i \in I)$,

$$\begin{aligned} X_f = \bigcup_{i\in I} X_{f_i} &\Longrightarrow X - V(f) = \bigcup_{i\in I}(X - V(f_i)) \\ &\Longrightarrow V(f) = \bigcap_{i\in I} V(f_i) \\ &\Longrightarrow V(f) = V\left(\sum_{i\in I} f_i\right) \\ &\Longrightarrow r(f) = r\left(\sum_{i\in I} f_i\right). \end{aligned}$$

Hence, $f \in r(f) = r\left(\sum_{i\in I} f_i\right)$ can be expressed as

$$f^m = \sum_{j\in J} g_j f_j$$

where J is a finite subset of I and $g_j \in A$. That is, $f^m \in \sum_{j\in J} f_j$.

(2) *Show that* $V\left(\sum_{j\in J} f_j\right) = V(f)$.

(a) ($\subseteq$) For any prime ideal $\mathfrak{p} \supseteq \sum_{j\in J} f_j$, $f^m \in \mathfrak{p}$ or $f \in \mathfrak{p}$ (since $\mathfrak{p}$ is prime). So $\mathfrak{p} \supseteq (f)$, or $V\left(\sum_{j\in J} f_j\right) \subseteq V(f)$.

(b) ($\supseteq$)

$$\sum_{j\in J} f_j \subseteq \sum_{i\in I} f_i \Longrightarrow V\left(\sum_{j\in J} f_j\right) \supseteq V\left(\sum_{i\in I} f_i\right) = V(f).$$

(3) Therefore, X_f is covered by finite subcovering $\{X_{f_j}\}(j \in J)$.

$\square$

Proof of (vi)(Using (v)). Exercise 3.21 (i) shows that X_f is the spectrum of A_f. By (v), X_f is quasi-compact. $\square$

Proof of (vii).

(1) ($\Longrightarrow$) Given an open subset O. Since X_f form a basis of open sets,

$$O = \bigcup_{f \in \mathfrak{a}} X_f \text{ for some ideal } \mathfrak{a} \text{ of } A$$

Especially, $\{X_f\}_{f \in \mathfrak{a}}$ is an open covering of O. Since O is quasi-compact, there exists a finite subcovering $\{X_f\}_{f \in J}$ of O, where J is a finite subset of $\mathfrak{a}$ (as a set). That is, $O = \bigcup_{f \in J} X_f$ is a finite union of sets X_f.

(2) ($\Longleftarrow$) Since X_f is quasi-compact, any finite union of quasi-compact sets is quasi-compact again.

□

Exercise 1.18. *For psychological reasons it is sometimes convenient to denote a prime ideal of A by a letter such as x or y when thinking of it as a point of $X = Spec(A)$. When thinking of x as a prime ideal of A, we denote it by $\mathfrak{p}_x$ (logically, of course, it is the same thing). Show that*

(i) *The set $\{x\}$ is closed (we say that x is a "closed point") in $Spec(A)$ $\Longleftrightarrow$ $\mathfrak{p}_x$ is maximal;*

Exercise 1.19. *A topological space X is said to be irreducible if $X \neq \varnothing$ and if every pair of non-empty open sets in X intersect, or equivalently if every non-empty open set is dense in X. Show that $Spec(A)$ is irreducible if and only if the nilradical of A is a prime ideal.*

Exercise 1.20. *Let X be a topological space.*

(i) *If Y is an irreducible subspace of X, then the closure $\overline{Y}$ of Y in X is irreducible.*

Proof of (i).

(1) *Y is irreducible if and only if Y cannot be represented as the union of two proper closed subspaces.*

$$\begin{aligned}
&\forall \text{ nonempty open sets } U_1 \text{ and } U_2, U_1 \cap U_2 \neq \varnothing \\
\Longleftrightarrow &\forall \text{ nonempty open sets } U_1 \text{ and } U_2, X - (U_1 \cap U_2) \neq X \\
\Longleftrightarrow &\forall \text{ nonempty open sets } U_1 \text{ and } U_2, (X - U_1) \cup (X - U_2) \neq X \\
\Longleftrightarrow &\forall \text{ proper closed sets } Y_1 \text{ and } Y_2, Y_1 \cup Y_2 \neq X \\
\Longleftrightarrow &\nexists \text{ proper closed sets } Y_1 \text{ and } Y_2, Y_1 \cup Y_2 = X.
\end{aligned}$$

(2) If $\overline{Y}$ were reducible, there are two closed set Y_1 and Y_2 such that

$$\overline{Y} \subseteq Y_1 \cup Y_2, \overline{Y} \not\subseteq Y_i (i = 1, 2).$$

(a) $Y \subseteq \overline{Y} \subseteq Y_1 \cup Y_2$.

(b) $Y \not\subseteq Y_i (i = 1, 2)$. If not, $Y \subseteq Y_i$ for some i. Take closure to get $\overline{Y} \subseteq \overline{Y_i} = Y_i$ (since Y_i is closed), contrary to the assumption.

By (a)(b), Y is reducible, which is absurd.

□

Supplement. *(Exercise I.1.6 in Robin Hartshorne, Algebraic Geometry.) Any nonempty open subset of an irreducible topological space is dense and irreducible. If Y is a subset of a topological space X, which is irreducible in its induced topology, then the closure $\overline{Y}$ is also irreducible.*

Here we use the definition of irreducibility given by Hartshorne.

Definition. A nonempty subset Y of a topological space X is irreducible if it cannot be expressed as the union $Y = Y_1 \cup Y_2$ of two proper subsets, each one of which is closed in Y. The empty set is not considered to be irreducible.

The proof is the same as Exercise 1.20(i).