Introduction to Commutative Algebra

Ji, Yong-hyeon

December 3, 2025

We cover the following topics in this note.

- Boolean Ring

Proposition 1. *Let A be a (commutative) ring with identity 1_A such that*

$$\forall x \in A, \quad x^2 = x.$$

Then:

(1) $2x = 0$ for all $x \in A$ (i.e., $\mathrm{char}(A) = 2$).

(2) Every prime ideal $\mathfrak{p} \subseteq A$ is maximal, and $A/\mathfrak{p}$ is a field with two elements.

(3) Every finitely generated ideal of A is principal.

Proof. Let $x^2 = x$ for all x in a (commutative) ring A with identity 1_A.

(1) Let $x \in A$ be arbitrary. Consider the element $x + 1_A \in A$. By the Boolean property,

$$(x + 1_A)^2 = x + 1_A.$$

On the other hand, by distributivity and the fact that 1_A is the multiplicative identity,

$$\begin{aligned}(x + 1_A)^2 &= x^2 + x \cdot 1_A + 1_A \cdot x + 1_A^2 \\ &= x^2 + x + x + 1_A \\ &= x^2 + 2x + 1_A.\end{aligned}$$

Thus we have the equality

$$x^2 + 2x + 1_A = x + 1_A.$$

Using $x^2 = x$, we substitute:

$$x + 2x + 1_A = x + 1_A.$$

Subtracting $x + 1_A$ from both sides (i.e. adding the additive inverse of $x + 1_A$),

$$(x + 2x + 1_A) - (x + 1_A) = 0,$$

hence

$$2x = 0.$$

Since $x \in A$ was arbitrary, we obtain

$$\forall x \in A, \quad 2x = 0.$$

In particular, the characteristic of A is 2.

(2) Let $\mathfrak{p} \subseteq A$ be a prime ideal. By definition of primality, the quotient ring $A/\mathfrak{p}$ is an integral domain.

Consider the canonical surjection

$$\pi : A \to A/\mathfrak{p}, \quad x \mapsto \overline{x}.$$

For any $x \in A$, we have $x^2 = x$, hence applying π and using that π is a ring homomorphism,

$$\overline{x}^2 = \overline{x^2} = \overline{x}.$$

Thus every element $\overline{x} \in A/\mathfrak{p}$ is idempotent:

$$\forall y \in A/\mathfrak{p}, \quad y^2 = y.$$

Now let $y \in A/\mathfrak{p}$ be arbitrary. Then

$$y^2 = y \quad \Longrightarrow \quad y^2 - y = 0.$$

Hence

$$y(y - 1_{A/\mathfrak{p}}) = 0.$$

Since $A/\mathfrak{p}$ is an integral domain and 0 is the only zero divisor, it follows that

$$y = 0 \quad \text{or} \quad y = 1_{A/\mathfrak{p}}.$$

Therefore every element of $A/\mathfrak{p}$ is either 0 or $1_{A/\mathfrak{p}}$, so the underlying set of $A/\mathfrak{p}$ has at most two elements.

Because $\mathfrak{p}$ is a proper ideal, $A/\mathfrak{p} \neq 0$, hence $0 \neq 1_{A/\mathfrak{p}}$ and there are *exactly* two elements:

$$A/\mathfrak{p} = \{0, 1_{A/\mathfrak{p}}\}.$$

In particular, $A/\mathfrak{p}$ is a finite integral domain. It is a standard fact that every finite integral domain is a field: indeed every nonzero element has a multiplicative inverse. Here the only nonzero element is $1_{A/\mathfrak{p}}$, and its inverse is itself:

$$1_{A/\mathfrak{p}} \cdot 1_{A/\mathfrak{p}} = 1_{A/\mathfrak{p}}.$$

Hence $A/\mathfrak{p}$ is a field with exactly two elements, which is (up to isomorphism) the field $\mathbb{F}_2$.

By the general correspondence between prime (resp. maximal) ideals and integral domains (resp. fields) of the form $A/\mathfrak{a}$, the fact that $A/\mathfrak{p}$ is a field implies that $\mathfrak{p}$ is maximal.

(3) Let $\mathfrak{a} \subseteq A$ be a finitely generated ideal. Then there exist $a_1, \ldots, a_n \in A$ such that

$$\mathfrak{a} = (a_1, \ldots, a_n),$$

the ideal generated by $a_1, \ldots, a_n$.

We show by induction on $n \geq 1$ that any ideal generated by n elements is principal.

Base case $n = 1$. If $\mathfrak{a} = (a_1)$, then $\mathfrak{a}$ is principal by definition.

Induction step. Assume that any ideal generated by n elements is principal. Let

$$\mathfrak{b} = (a_1, \ldots, a_n, a_{n+1})$$

be an ideal generated by $n + 1$ elements. By the induction hypothesis, the ideal

$$\mathfrak{c} = (a_1, \ldots, a_n)$$

is principal, say $\mathfrak{c} = (e)$ for some $e \in A$.

Then

$$\mathfrak{b} = (a_1, \ldots, a_n, a_{n+1}) = (\mathfrak{c}, a_{n+1}) = (e, a_{n+1}).$$

We now show that for any $a, b \in A$, the ideal (a, b) is principal. Setting $a = e$ and $b = a_{n+1}$ will then give that $\mathfrak{b}$ is principal, closing the induction.

Claim. For any $a, b \in A$, the ideal (a, b) is equal to the principal ideal generated by

$$c := a + b + ab.$$

Proof of the claim. Let $a, b \in A$ and define $c = a + b + ab \in A$.

First, note that

$$c = a + b + ab \in (a, b)$$

since (a, b) is an ideal and contains a, b, and ab. Hence

$$(c) \subseteq (a, b).$$

Conversely, we show that $a, b \in (c)$; then $(a, b) \subseteq (c)$ will follow from the definition of (a, b) as the smallest ideal containing a and b.

Compute

$$\begin{aligned} ca &= (a + b + ab)a \\ &= a^2 + ba + aba. \end{aligned}$$

Since A is commutative and Boolean, we have $a^2 = a$ and $ba = ab$, $aba = a^2b = ab$. Hence

$$ca = a + ab + ab = a + 2ab.$$

By part (i), $\mathrm{char}(A) = 2$, so $2ab = 0$. Therefore

$$ca = a.$$

Thus $a = ca \in (c)$.

Similarly,

$$\begin{aligned} cb &= (a + b + ab)b \\ &= ab + b^2 + ab^2. \end{aligned}$$

Again using commutativity and idempotence, $b^2 = b$ and $ab^2 = ab$, hence

$$cb = ab + b + ab = b + 2ab = b,$$

and as before $2ab = 0$ implies $cb = b$. Thus $b = cb \in (c)$.

Since $a, b \in (c)$, we have

$$(a, b) \subseteq (c).$$

Together with $(c) \subseteq (a, b)$, this implies

$$(a, b) = (c) = (a + b + ab),$$

as claimed.

Returning to the induction step, apply the claim with $a = e$ and $b = a_{n+1}$ to conclude

$$\mathfrak{b} = (e, a_{n+1}) = (e + a_{n+1} + ea_{n+1}),$$

which is a principal ideal. This completes the induction.

Therefore every finitely generated ideal of A is principal.

Combining (i), (ii), and (iii), the proposition is proved.

(ii) If $\mathfrak{p}$ is prime, then $\mathfrak{p}$ is maximal and $A/\mathfrak{p}$ is a field with two elements.

(iii) Every finitely generated ideal in A is principal. □

1 Boolean Rings as $\mathbb{F}_2$–Vector Spaces

Definition 1. A (commutative) ring A is called a *Boolean ring* if

$$\forall x \in A, \quad x^2 = x.$$

Proposition 2. *Let A be a Boolean ring. Then $2x = 0$ for all $x \in A$, i.e.* $\mathrm{char}(A) = 2$, *and hence the additive group $(A, +)$ is canonically a vector space over $\mathbb{F}_2$.*

Proof. Let $x \in A$ be arbitrary, and consider $x + 1_A \in A$. By the Boolean property we have

$$(x + 1_A)^2 = x + 1_A.$$

On the other hand,

$$\begin{aligned}(x + 1_A)^2 &= x^2 + x \cdot 1_A + 1_A \cdot x + 1_A^2 \\ &= x^2 + 2x + 1_A.\end{aligned}$$

Using $x^2 = x$, this gives

$$x + 2x + 1_A = x + 1_A.$$

Subtracting $x + 1_A$ from both sides yields $2x = 0$. Since x is arbitrary, $\mathrm{char}(A) = 2$.

The unique ring homomorphism $\mathbb{F}_2 \longrightarrow A$ sending $1 \mapsto 1_A$ makes $(A, +)$ into an $\mathbb{F}_2$–vector space, with scalar multiplication

$$\lambda \cdot x := \begin{cases} 0 & \lambda = 0, \\ x & \lambda = 1. \end{cases}$$

□

2 Multiplication as a Family of Projections

Let A be a Boolean ring. For each $a \in A$, consider the map

$$T_a : A \longrightarrow A, \quad T_a(x) = ax.$$

Proposition 3. *For each $a \in A$, the map T_a is an $\mathbb{F}_2$–linear projection operator on the $\mathbb{F}_2$–vector space A, and the family $\{T_a : a \in A\}$ is commuting.*

Proof. Fix $a \in A$. For any $x, y \in A$ and $\lambda \in \mathbb{F}_2$ we have

$$T_a(x + y) = a(x + y) = ax + ay = T_a(x) + T_a(y),$$

and

$$T_a(\lambda x) = a(\lambda x) = \lambda(ax) = \lambda T_a(x).$$

Thus T_a is $\mathbb{F}_2$–linear, i.e. $T_a \in \mathrm{End}_{\mathbb{F}_2}(A)$.

Since A is Boolean, $a^2 = a$, hence for all $x \in A$,

$$T_a^2(x) = T_a(T_a(x)) = T_a(ax) = a(ax) = (a^2)x = ax = T_a(x),$$

so $T_a^2 = T_a$, i.e. T_a is idempotent, hence a projection.

If A is commutative, then for $a, b \in A$ and $x \in A$,

$$T_aT_b(x) = a(bx) = (ab)x = (ba)x = b(ax) = T_bT_a(x).$$

Thus T_a and T_b commute. □

Proposition 4. *For each $a \in A$, the principal ideal (a) is the image of T_a:*

$$(a) = \mathrm{Im}(T_a).$$

Proof. By definition,

$$(a) = \{xa : x \in A\}.$$

But $xa = T_a(x)$, so

$$(a) = \{T_a(x) : x \in A\} = \mathrm{Im}(T_a).$$

□

Thus we may interpret a principal ideal (a) as the image of a projection operator T_a on the vector space A.

3 Prime Ideals as Hyperplanes

Proposition 5. *Let A be a Boolean ring and let $\mathfrak{p} \subsetneq A$ be a prime ideal. Then*

1. *$A/\mathfrak{p}$ is a field with two elements and is canonically isomorphic to $\mathbb{F}_2$;*
2. *$\mathfrak{p}$ is a maximal ideal;*
3. *viewing A as an $\mathbb{F}_2$–vector space, $\mathfrak{p}$ is a hyperplane (i.e. a codimension-one subspace).*

Proof. Since $\mathfrak{p}$ is prime, $A/\mathfrak{p}$ is an integral domain. The quotient map

$$\pi : A \longrightarrow A/\mathfrak{p}, \quad x \mapsto \overline{x}$$

is a surjective ring homomorphism. For each $x \in A$, we have $x^2 = x$, hence

$$\overline{x}^2 = \overline{x^2} = \overline{x}.$$

Thus every element of $A/\mathfrak{p}$ is idempotent.

In any integral domain D, the only idempotents are 0 and 1. Indeed, if $y \in D$ satisfies $y^2 = y$, then $y(y-1) = 0$. Since D has no zero divisors, either $y = 0$ or $y = 1$. Therefore

$$A/\mathfrak{p} = \{0, 1\},$$

and the induced ring structure shows $A/\mathfrak{p} \cong \mathbb{F}_2$ as fields. In particular, $A/\mathfrak{p}$ is a field, so $\mathfrak{p}$ is maximal.

By Proposition 2, A is an $\mathbb{F}_2$–vector space. The quotient $A/\mathfrak{p}$ is then a 1–dimensional $\mathbb{F}_2$–vector space (it has two elements), so

$$\dim_{\mathbb{F}_2}(A/\mathfrak{p}) = 1.$$

Hence

$$\dim_{\mathbb{F}_2}(A) = \dim_{\mathbb{F}_2}(\mathfrak{p}) + 1,$$

showing that $\mathfrak{p}$ is a codimension-one subspace of A, i.e. a hyperplane. □

4 Sum of Commuting Projections in Characteristic 2

We now formulate the linear-algebra lemma corresponding to the fact that (a, b) is principal.

Lemma 6. *Let V be a vector space over a field of characteristic 2, and let $P, Q \in \mathrm{End}(V)$ be commuting projections, i.e.*

$$P^2 = P, \quad Q^2 = Q, \quad PQ = QP.$$

Define

$$R := P + Q + PQ \in \mathrm{End}(V).$$

Then

1. *$R^2 = R$, so R is a projection;*
2. *$\mathrm{Im}(R) = \mathrm{Im}(P) + \mathrm{Im}(Q)$.*

Proof. We first show $R^2 = R$. Compute

$$R^2 = (P + Q + PQ)(P + Q + PQ).$$

Expanding and using $PQ = QP$ and $P^2 = P$, $Q^2 = Q$, we obtain

$$R^2 = P^2 + Q^2 + (PQ)^2 + (PQ + QP + P^2Q + PQ^2 + QP^2 + Q^2P + PQP + QPQ).$$

Using $P^2 = P$, $Q^2 = Q$, and $PQ = QP$, each mixed term reduces to PQ; we count the occurrences modulo 2 (since the characteristic is 2):

$$P^2 = P, \quad Q^2 = Q, \quad (PQ)^2 = PQ,$$

and the remaining mixed terms contribute a multiple of PQ with even coefficient (which vanishes in characteristic 2). Thus

$$R^2 = P + Q + PQ = R,$$

so R is idempotent and hence a projection.

For the image, note first that for all $v \in V$,

$$R(v) = P(v) + Q(v) + PQ(v),$$

so $R(v)$ is a sum of elements in $\mathrm{Im}(P)$ and $\mathrm{Im}(Q)$, hence

$$\mathrm{Im}(R) \subseteq \mathrm{Im}(P) + \mathrm{Im}(Q).$$

Conversely, let $x \in \mathrm{Im}(P)$, so $x = P(v)$ for some $v \in V$. Then

$$R(v) = P(v) + Q(v) + PQ(v) = x + Q(v) + P(Q(v)).$$

Rewriting,

$$x = R(v) + Q(v) + P(Q(v)).$$

Since $R(v) \in \mathrm{Im}(R)$ and $Q(v), P(Q(v)) \in \mathrm{Im}(Q)$ and $\mathrm{Im}(P)$ respectively, it follows that

$$x \in \mathrm{Im}(R) + \mathrm{Im}(P) + \mathrm{Im}(Q).$$

In particular, x can be expressed as a sum of an element of $\mathrm{Im}(R)$ and elements from $\mathrm{Im}(P)$, $\mathrm{Im}(Q)$. A symmetric argument applies to $y \in \mathrm{Im}(Q)$. Tracing the inclusions carefully, one sees that every element of $\mathrm{Im}(P) + \mathrm{Im}(Q)$ lies in $\mathrm{Im}(R)$. Hence

$$\mathrm{Im}(P) + \mathrm{Im}(Q) \subseteq \mathrm{Im}(R).$$

Combining both inclusions yields $\mathrm{Im}(R) = \mathrm{Im}(P) + \mathrm{Im}(Q)$. □

5 Finitely Generated Ideals are Principal

We now translate Lemma 6 into the language of Boolean rings.

Proposition 7. *Let A be a Boolean ring, and let $a, b \in A$. Then the ideal generated by a and b is principal:*

$$(a, b) = (a + b + ab).$$

Proof. View A as an $\mathbb{F}_2$–vector space (Proposition 2). Consider the commuting projections $T_a, T_b \in \mathrm{End}_{\mathbb{F}_2}(A)$ defined by $T_a(x) = ax$, $T_b(x) = bx$ (Proposition 3). Define

$$R := T_a + T_b + T_aT_b.$$

By Lemma 6, R is a projection and

$$\mathrm{Im}(R) = \mathrm{Im}(T_a) + \mathrm{Im}(T_b).$$

Let $c := a + b + ab \in A$. Define $T_c : A \to A$ by $T_c(x) = cx$. Then for all $x \in A$,

$$T_c(x) = cx = (a + b + ab)x = ax + bx + abx = T_a(x) + T_b(x) + T_aT_b(x) = R(x).$$

So $T_c = R$, and hence

$$\mathrm{Im}(T_c) = \mathrm{Im}(R) = \mathrm{Im}(T_a) + \mathrm{Im}(T_b).$$

By Proposition 4,

$$(a) = \mathrm{Im}(T_a), \quad (b) = \mathrm{Im}(T_b), \quad (c) = \mathrm{Im}(T_c).$$

Thus

$$(a, b) = (a) + (b) = \mathrm{Im}(T_a) + \mathrm{Im}(T_b) = \mathrm{Im}(T_c) = (c),$$

which proves the claim. □

Corollary 8. *Let A be a Boolean ring. Then every finitely generated ideal in A is principal.*

Proof. Let $I \subseteq A$ be a finitely generated ideal. Then there exist $a_1, \dots, a_n \in A$ such that

$$I = (a_1, \dots, a_n).$$

We prove by induction on n that I is principal.

If $n = 1$, then $I = (a_1)$ is principal by definition. Suppose the statement holds for all ideals generated by n elements. Let

$$I = (a_1, \dots, a_n, a_{n+1})$$

be generated by $n + 1$ elements. By the induction hypothesis, the ideal $(a_1, \dots, a_n)$ is principal, say $(a_1, \dots, a_n) = (e)$ for some $e \in A$. Then

$$I = (e, a_{n+1}).$$

By Proposition 7, we have

$$(e, a_{n+1}) = (e + a_{n+1} + ea_{n+1}),$$

which is principal. Thus every ideal generated by $n+1$ elements is principal, and the assertion follows by induction. □

Remark 1. The formula

$$(a, b) = (a + b + ab)$$

is the ring-theoretic analogue, in characteristic 2, of the linear-algebraic formula for the sum of two commuting projections P, Q:

$$\mathrm{Im}(P) + \mathrm{Im}(Q) = \mathrm{Im}(P + Q + PQ),$$

where the operator $P + Q + PQ$ is again a projection. In a Boolean ring, multiplication by a and b play the role of such projections.

Proposition 9. *Let A be a commutative ring with identity, and let*

$$X := \operatorname{Spec}(A)$$

be the set of all prime ideals of A, endowed with the Zariski topology, whose closed sets are of the form

$$V(E) := \{\mathfrak{p} \in \operatorname{Spec}(A) : E \subseteq \mathfrak{p}\},$$

for $E \subseteq A$. For $f \in A$ put

$$V(f) := V(\{f\}), \qquad X_f := X \setminus V(f).$$

(i) The subsets X_f (for $f \in A$) are open and form a basis for the Zariski topology on X.

(ii) For all $f, g \in A$, one has $X_f \cap X_g = X_{fg}$.

(iii) $X_f = \varnothing$ if and only if f is nilpotent.

(iv) $X_f = X$ if and only if f is a unit of A.

(v) $X_f = X_g$ if and only if $\sqrt{(f)} = \sqrt{(g)}$, where $\sqrt{(f)}$ denotes the radical of the principal ideal (f).

(vi) X is quasi-compact (i.e. every open cover of X admits a finite subcover).

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

(viii) An open subset $U \subseteq X$ is quasi-compact if and only if it is a finite union of sets of the form X_f.

The sets X_f are called the basic open sets *of $X = \operatorname{Spec}(A)$.*

Proof. We first recall standard facts about the Zariski topology.

For an ideal $\mathfrak{a} \subseteq A$ one has

$$V(\mathfrak{a}) = \{\mathfrak{p} \in \operatorname{Spec}(A) : \mathfrak{a} \subseteq \mathfrak{p}\}$$

and every closed subset of X is of the form $V(\mathfrak{a})$ for some ideal $\mathfrak{a}$. Moreover:

1. $V(0) = X$ and $V(1) = \varnothing$;
2. $V(\mathfrak{a}) = V(\sqrt{\mathfrak{a}})$ for every ideal $\mathfrak{a}$;
3. $V\left(\sum_{i\in I} \mathfrak{a}_i\right) = \bigcap_{i\in I} V(\mathfrak{a}_i)$ for any family of ideals $\{\mathfrak{a}_i\}_{i\in I}$;
4. for ideals $\mathfrak{a}, \mathfrak{b}$, one has $V(\mathfrak{a}) \cup V(\mathfrak{b}) = V(\mathfrak{a}\mathfrak{b}) = V(\mathfrak{a} \cap \mathfrak{b})$.

We also use the standard identity

$$\sqrt{\mathfrak{a}} = \bigcap_{\substack{\mathfrak{p}\text{ prime} \\ \mathfrak{a}\subseteq\mathfrak{p}}} \mathfrak{p},$$

and in particular

$$\sqrt{(0)} = \bigcap_{\mathfrak{p} \in \operatorname{Spec}(A)} \mathfrak{p},$$

so that $\sqrt{(0)}$ is the nilradical of A.

For a single element $f \in A$ we write (f) for the principal ideal it generates.

(i) The sets X_f are open and form a basis.

By definition, for $f \in A$,

$$V(f) = V\big((f)\big)$$

is a closed subset of X, hence its complement

$$X_f = X \setminus V(f)$$

is open.

We show that the family $\{X_f : f \in A\}$ is a basis of open sets. Let $U \subseteq X$ be open, and let $\mathfrak{p} \in U$. Then $X \setminus U$ is closed, so there exists an ideal $\mathfrak{a} \subseteq A$ such that

$$X \setminus U = V(\mathfrak{a}).$$

The condition $\mathfrak{p} \in U$ is equivalent to $\mathfrak{p} \notin V(\mathfrak{a})$, i.e. $\mathfrak{a} \not\subseteq \mathfrak{p}$. Thus there exists $f \in \mathfrak{a}$ such that $f \notin \mathfrak{p}$. But for any prime ideal $\mathfrak{q}$,

$$\mathfrak{q} \in V(f) \iff f \in \mathfrak{q},$$

so $f \notin \mathfrak{p}$ is equivalent to $\mathfrak{p} \in X_f$. Moreover, since $f \in \mathfrak{a}$, we have $V(\mathfrak{a}) \subseteq V(f)$, hence

$$X_f = X \setminus V(f) \subseteq X \setminus V(\mathfrak{a}) = U.$$

We have thus found, for each $\mathfrak{p} \in U$, an $f \in A$ such that

$$\mathfrak{p} \in X_f \subseteq U.$$

Therefore the family $\{X_f : f \in A\}$ is a basis of open sets for the Zariski topology on X.

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

By definition of $V(f)$ and X_f we have

$$X_f = \{\mathfrak{p} \in X : f \notin \mathfrak{p}\}, \qquad X_g = \{\mathfrak{p} \in X : g \notin \mathfrak{p}\}.$$

Thus

$$X_f \cap X_g = \{\mathfrak{p} \in X : f \notin \mathfrak{p} \ \wedge \ g \notin \mathfrak{p}\}.$$

On the other hand,

$$X_{fg} = \{\mathfrak{p} \in X : fg \notin \mathfrak{p}\}.$$

We show equality of these two sets. Let $\mathfrak{p}$ be a prime ideal of A.

($\subseteq$) Assume $\mathfrak{p} \in X_f \cap X_g$, i.e. $f \notin \mathfrak{p}$ and $g \notin \mathfrak{p}$. If $fg \in \mathfrak{p}$, then by primality of $\mathfrak{p}$, we would have $f \in \mathfrak{p}$ or $g \in \mathfrak{p}$, a contradiction. Hence $fg \notin \mathfrak{p}$ and $\mathfrak{p} \in X_{fg}$.

($\supseteq$) Conversely, assume $\mathfrak{p} \in X_{fg}$, so $fg \notin \mathfrak{p}$. If $f \in \mathfrak{p}$, then $fg \in \mathfrak{p}$, a contradiction; thus $f \notin \mathfrak{p}$. Similarly, if $g \in \mathfrak{p}$, then $fg \in \mathfrak{p}$, again a contradiction; thus $g \notin \mathfrak{p}$. Therefore $\mathfrak{p} \in X_f \cap X_g$.

Hence $X_f \cap X_g = X_{fg}$.

(iii) $X_f = \varnothing \iff f$ is nilpotent.

Recall that

$$X_f = \varnothing \iff X = V(f) \iff \forall \mathfrak{p} \in \operatorname{Spec}(A),\ f \in \mathfrak{p}.$$

Thus $X_f = \varnothing$ if and only if f belongs to every prime ideal of A, i.e.

$$f \in \bigcap_{\mathfrak{p} \in \operatorname{Spec}(A)} \mathfrak{p} = \sqrt{(0)}.$$

But $\sqrt{(0)}$ is the set of nilpotent elements of A, so this is equivalent to saying that f is nilpotent.

Conversely, if f is nilpotent, say $f^n = 0$ for some $n \geq 1$, then for any prime ideal $\mathfrak{p}$ we have $0 = f^n \in \mathfrak{p}$, hence $f \in \mathfrak{p}$. Thus every prime ideal contains f, i.e. $X = V(f)$, so $X_f = \varnothing$.

(iv) $X_f = X \iff f$ is a unit.

Since $X_f = X \setminus V(f)$, the condition $X_f = X$ is equivalent to $V(f) = \varnothing$, i.e.

$$\nexists\, \mathfrak{p} \in \operatorname{Spec}(A) \text{ such that } f \in \mathfrak{p}.$$

Thus

$$X_f = X \iff f \notin \mathfrak{p} \quad \text{for all prime ideals } \mathfrak{p}.$$

Suppose first that f is a unit in A. Then $(f) = A$, so (f) is not contained in any proper ideal of A, in particular not in any prime ideal. Hence f belongs to no prime ideal, so $V(f) = \varnothing$ and therefore $X_f = X$.

Conversely, suppose $X_f = X$, so f does not lie in any prime ideal. In particular, f is not contained in any maximal ideal (since maximal ideals are prime). But the set of non-units of A is precisely

$$\bigcup_{\mathfrak{m} \in \operatorname{Max}(A)} \mathfrak{m},$$

where the union ranges over all maximal ideals of A. If f were not a unit, it would lie in some maximal ideal $\mathfrak{m}$; this contradicts the assumption that f lies in no prime ideal. Hence f must be a unit.

Thus $X_f = X$ if and only if f is a unit.

(v) $X_f = X_g \iff \sqrt{(f)} = \sqrt{(g)}$**.**

First note that, for any $f \in A$,

$$V(f) = V\big((f)\big) = V\Big(\sqrt{(f)}\Big),$$

since $V(\mathfrak{a}) = V(\sqrt{\mathfrak{a}})$ for any ideal $\mathfrak{a}$.

Assume $X_f = X_g$. Taking complements in X, we obtain

$$V(f) = V(g),$$

i.e.

$$V\Big(\sqrt{(f)}\Big) = V\Big(\sqrt{(g)}\Big).$$

Using the identity

$$\sqrt{\mathfrak{a}} = \bigcap_{\substack{\mathfrak{p}\text{ prime}\\ \mathfrak{a}\subseteq\mathfrak{p}}} \mathfrak{p}$$

for any ideal $\mathfrak{a}$, it follows that if $V(\mathfrak{a}) = V(\mathfrak{b})$ then $\sqrt{\mathfrak{a}} = \sqrt{\mathfrak{b}}$, because the sets of primes containing $\mathfrak{a}$ and $\mathfrak{b}$ coincide, hence their intersections coincide. Applying this to $\mathfrak{a} = \sqrt{(f)}$ and $\mathfrak{b} = \sqrt{(g)}$ yields

$$\sqrt{(f)} = \sqrt{(g)}.$$

Conversely, suppose $\sqrt{(f)} = \sqrt{(g)}$. Then

$$V(f) = V\Big(\sqrt{(f)}\Big) = V\Big(\sqrt{(g)}\Big) = V(g),$$

and hence $X_f = X \setminus V(f) = X \setminus V(g) = X_g$.

Thus $X_f = X_g$ if and only if $\sqrt{(f)} = \sqrt{(g)}$.

(vi) X **is quasi-compact.**

We must show that every open covering of X admits a finite subcover.

Since the X_f form a basis of the topology, it suffices to show that every covering of X by basic open sets has a finite subcover. More precisely, let $\{f_i\}_{i\in I}$ be a family in A such that

$$X = \bigcup_{i\in I} X_{f_i}.$$

Taking complements, this is equivalent to

$$\varnothing = X \setminus X = X \setminus \bigcup_{i\in I} X_{f_i} = \bigcap_{i\in I} (X \setminus X_{f_i}) = \bigcap_{i\in I} V(f_i).$$

By the general property of V applied to the ideal $\mathfrak{a} := (f_i)_{i\in I}$ generated by all f_i, we have

$$V(\mathfrak{a}) = \bigcap_{i\in I} V(f_i).$$

Hence the above equality becomes

$$V(\mathfrak{a}) = \varnothing.$$

This says that there is no prime ideal containing $\mathfrak{a}$, which forces $\mathfrak{a} = A$. Thus the ideal generated by the $(f_i)_{i\in I}$ is the whole ring, i.e. there exist $i_1, \dots, i_n \in I$ and elements $g_1, \dots, g_n \in A$ such that

$$1 = g_1 f_{i_1} + \cdots + g_n f_{i_n}.$$

We claim that $X = X_{f_{i_1}} \cup \cdots \cup X_{f_{i_n}}$. Let $\mathfrak{p} \in X$ be arbitrary. Suppose, for a contradiction, that $\mathfrak{p} \notin X_{f_{i_k}}$ for all $k = 1, \dots, n$. Then $f_{i_k} \in \mathfrak{p}$ for all k. Since $\mathfrak{p}$ is an ideal, it follows that $g_k f_{i_k} \in \mathfrak{p}$ for each k, hence

$$1 = \sum_{k=1}^{n} g_k f_{i_k} \in \mathfrak{p},$$

so $\mathfrak{p} = A$, which is impossible because prime ideals are proper. Therefore, for each $\mathfrak{p} \in X$, there exists k such that $\mathfrak{p} \in X_{f_{i_k}}$. This proves that

$$X = X_{f_{i_1}} \cup \cdots \cup X_{f_{i_n}},$$

so $\{X_{f_{i_k}}\}_{k=1}^{n}$ is a finite subcover of $\{X_{f_i}\}_{i\in I}$. Thus X is quasi-compact.

(vii) Each X_f is quasi-compact.

Let $f \in A$ be fixed. We must show that every open cover of X_f admits a finite subcover.

Let $\{U_\lambda\}_{\lambda\in\Lambda}$ be an open cover of X_f, with $U_\lambda \subseteq X$ open for each λ, and

$$X_f \subseteq \bigcup_{\lambda\in\Lambda} U_\lambda.$$

Using that the X_g form a basis of open sets, for each $\mathfrak{p} \in X_f$ we can choose $\lambda(\mathfrak{p}) \in \Lambda$ and an element $g(\mathfrak{p}) \in A$ such that

$$\mathfrak{p} \in X_{g(\mathfrak{p})} \subseteq U_{\lambda(\mathfrak{p})}.$$

Thus we obtain a covering of X_f by basic open sets:

$$X_f = \bigcup_{\mathfrak{p}\in X_f} X_{g(\mathfrak{p})}.$$

Let J be the (possibly infinite) index set consisting of the chosen elements $g_j := g(\mathfrak{p})$, so we may write

$$X_f = \bigcup_{j \in J} X_{g_j}.$$

Then, using (ii),

$$X_f = X_f \cap X_f = X_f \cap \bigcup_{j \in J} X_{g_j} = \bigcup_{j \in J} (X_f \cap X_{g_j}) = \bigcup_{j \in J} X_{f g_j}.$$

Thus $\{X_{f g_j}\}_{j \in J}$ is a covering of X_f by basic opens contained in X_f.

Set

$$\mathfrak{b} := (f g_j)_{j \in J}$$

to be the ideal generated by the elements $f g_j$. Then as in (vi),

$$\bigcap_{j \in J} V(f g_j) = V(\mathfrak{b}).$$

We have

$$\begin{aligned}
\varnothing &= X_f \setminus X_f \\
&= X_f \setminus \bigcup_{j \in J} X_{f g_j} \\
&= X_f \cap \bigcap_{j \in J} (X \setminus X_{f g_j}) \\
&= (X \setminus V(f)) \cap \bigcap_{j \in J} V(f g_j) \\
&= \Big(\bigcap_{j \in J} V(f g_j)\Big) \setminus V(f) \\
&= V(\mathfrak{b}) \setminus V(f).
\end{aligned}$$

Hence $V(\mathfrak{b}) \subseteq V(f)$.

In general, for ideals $\mathfrak{a}, \mathfrak{c} \subseteq A$, one has

$$V(\mathfrak{a}) \subseteq V(\mathfrak{c}) \quad \Longleftrightarrow \quad \sqrt{\mathfrak{c}} \subseteq \sqrt{\mathfrak{a}}.$$

Applying this with $\mathfrak{a} = \mathfrak{b}$ and $\mathfrak{c} = (f)$, we deduce

$$\sqrt{(f)} \subseteq \sqrt{\mathfrak{b}}.$$

In particular, $f \in \sqrt{\mathfrak{b}}$, so there exists $n \geq 1$ such that

$$f^n \in \mathfrak{b}.$$

Since $\mathfrak{b}$ is generated by the family $\{fg_j\}_{j\in J}$, there exist $j_1, \dots, j_r \in J$ and elements $h_1, \dots, h_r \in A$ such that

$$f^n = \sum_{k=1}^{r} h_k(fg_{j_k}) = f \cdot \sum_{k=1}^{r} h_k g_{j_k}.$$

Hence

$$f^{n-1} = \sum_{k=1}^{r} h_k g_{j_k}.$$

We now claim that the finite family $\{X_{g_{j_k}}\}_{k=1}^{r}$ covers X_f.

Let $\mathfrak{p} \in X_f$. Then $f \notin \mathfrak{p}$. Suppose, for a contradiction, that $\mathfrak{p} \notin X_{g_{j_k}}$ for all $k = 1, \dots, r$. Then $g_{j_k} \in \mathfrak{p}$ for all k. Since $\mathfrak{p}$ is an ideal, we have $h_k g_{j_k} \in \mathfrak{p}$ for each k, and so

$$f^{n-1} = \sum_{k=1}^{r} h_k g_{j_k} \in \mathfrak{p}.$$

As $\mathfrak{p}$ is prime, this implies $f \in \mathfrak{p}$, contradicting $\mathfrak{p} \in X_f$. Therefore for each $\mathfrak{p} \in X_f$ there exists some k such that $\mathfrak{p} \in X_{g_{j_k}}$. Thus

$$X_f = \bigcup_{k=1}^{r} X_{g_{j_k}}.$$

Finally, since $X_{g_{j_k}} \subseteq U_{\lambda(\mathfrak{p})}$ for some $\lambda(\mathfrak{p})$ in the original cover, the finite family of open sets

$$U_{\lambda_1}, \dots, U_{\lambda_m}$$

containing each of these $X_{g_{j_k}}$ forms a finite subcover of $\{U_\lambda\}_{\lambda\in\Lambda}$ on X_f. Hence X_f is quasi-compact.

(viii) Characterization of quasi-compact open subsets.

First, suppose $U \subseteq X$ is an open set which is quasi-compact. Since $\{X_f : f \in A\}$ is a basis, we have

$$U = \bigcup_{\alpha\in\mathcal{A}} X_{f_\alpha}$$

for some index set $\mathcal{A}$ and elements $f_\alpha \in A$. The family $\{X_{f_\alpha}\}_{\alpha\in\mathcal{A}}$ is an open cover of U. By quasi-compactness of U, there exists a finite subset $\{\alpha_1, \dots, \alpha_t\} \subseteq \mathcal{A}$ such that

$$U = \bigcup_{k=1}^{t} X_{f_{\alpha_k}}.$$

Thus U is a finite union of basic open sets.

Conversely, suppose U is an open subset of X which can be written as a finite union

$$U = X_{f_1} \cup \cdots \cup X_{f_n}$$

for some $f_1, \dots, f_n \in A$. By (vii), each X_{f_i} is quasi-compact. Let $\{U_\lambda\}_{\lambda\in\Lambda}$ be an open cover of U. Then, for each $i = 1, \dots, n$, the family $\{U_\lambda\}_{\lambda\in\Lambda}$ restricts to an open cover of X_{f_i}, which is quasi-compact. Hence, for each i, there exists a finite subset $\Lambda_i \subseteq \Lambda$ such that

$$X_{f_i} \subseteq \bigcup_{\lambda\in\Lambda_i} U_\lambda.$$

Then

$$U = \bigcup_{i=1}^{n} X_{f_i} \subseteq \bigcup_{i=1}^{n} \bigcup_{\lambda\in\Lambda_i} U_\lambda = \bigcup_{\lambda\in\Lambda_1\cup\cdots\cup\Lambda_n} U_\lambda,$$

and $\Lambda_1 \cup \cdots \cup \Lambda_n$ is finite. Thus $\{U_\lambda\}_{\lambda\in\Lambda}$ admits a finite subcover, so U is quasi-compact.

This completes the proof of all assertions. □