Solution to Atiyah and MacDonald
Chapter 1. Rings and Ideals

Jaehyeon Lee

Last update: April 22, 2024

This is a solution to Exercise problems in Chapter 1 of "Introduction to Commutative Algebra" written by M. F. Atiyah and I. G. MacDonald. You can find the updated version and solutions to other chapters on my personal website: [`https://ijhlee0511.github.io`].

WARNNING This solution is written for self-study purposes and to consolidate my understanding. **I do not take responsibility for any disadvantages resulting from the use of this solution. It is at your own risk.** If you find any typos or errors in this solution, please feel free to contact me via email at [`ijhlee0511@gmail.com`] or [`ijhlee0511@kaist.ac.kr`].

Exercises and Solutions

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

Solution. There exists some $n > 0$ such that $x^n = 0$. Then $(1 + x) \sum_{k=0}^{n-1}(-x)^k = 1 + (-x)^n = 1$. Moreover, if u is a unit and x is nilpotent, then $u^{-1}(u + x) = 1 + (u^{-1}x)$ is a sum of 1 and a nilpotent element, so $u + x$ is also unit. □

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 $A[x] \Leftrightarrow a_0$ is a unit in A and $a_1, \ldots, a_n$ are nilpotent.
ii) f is nilpotent $\Leftrightarrow a_0, a_1, \ldots, a_n$ are nilpotent.
iii) f is a zero-divisor $\Leftrightarrow$ there exists $a \neq 0$ in A such that $af = 0$.
iv) f is said to be *primitive* if $(a_0, a_1, \ldots, a_n) = (1)$. Prove that if $f, g \in A[x]$, then fg is primitive $\Leftrightarrow f$ and g are primitive.

Solution. i) Assume $g(x) = b_0 + b_1x + \cdots + b_mx^m$ is the inverse of x. We claim that $a_n^{r+1}b_{m-r} = 0$ for $0 \le r \le m$. Induction on r. When $r = 0$, it is clear that $a_nb_m = 0$. For $r > 0$, consider $f^{r+1}g$. Observe the coefficient of $x^{n(r+1)+m-r}$ is $\sum_{i=0}^{r} a_n^{i+1}a_{n-1}^{r-i}b_{m-i}$, which is $a_n^{r+1}b_{m-r}$ by the induction hypothesis. But $f^{r+1}g = f^r = (a_0 + a_1x + \cdots + a_nx^n)^r$, so $a_n^{r+1}b_{m-r}$ is zero. We get $a_n^m g = 0$ by the claim, so a_n is nilpotent since g is a unit. Then $f - a_nx^n$ is a unit in $A[x]$ by Exercise 1.1. Repeating this process, $a_1, \ldots, a_n$ are all nilpotent, and a_0 is a unit in A. The opposite direction is a direct consequence of Exercise 1.1.

ii) Assume f is nilpotent. In fact, a sum of any tow nilpotent elements is nilpotent; if $a^n = 0$ and $b^m = 0$ for some $n, m > 0$, $(a + b)^{n+m} = 0$. Notice a_0 must be nilpotent, since the constant term of f^j is a_0^j for all $j > 0$. Then $f - a_0$ is also nilpotent. Repeating the same argument repeatedly, a_{n-r} is nilpotent for all $0 \le r \le n$. The opposite direction is clear due to the the fact that a sum of two nilpotent elements is nilpotent. Then $f - a_n x^n$ is a unit in $A[x]$ by Exercise 1.1. Repeating this process, $a_1, \dots, a_n$ are all nilpotent, and a_0 is a unit in A. The opposite direction is a direct consequence of Exercise 1.1.

iii) Choose a nonzero polynomial $g = b_0 + b_1 x + \cdots + b_m x^m$ of least degree m such that $fg = 0$ and $b_m \neq 0$. We claim that $a_{n-r} g = 0$ for $0 \le r \le n$ by induction on r. For $r = 0$, clearly $a_n b_m = 0$; hence, $a_n g = 0$ because $(a_n g) f = 0$ while $\deg a_n g < m$. In particular, $b_m a_n = 0$. Observe $gf = g(f - a_n x^n) = 0$, so by repeating this process we get $b_m a_n = b_m a_{n-1} = \cdots = b_m a_0 = 0$. Therefore, $b_m g = 0$ where b_m is nonzero by the assumption. The converse direction is obvious.

iv) Let $f = a_0 + a_1 x + \cdots + a_n x_n$, $g = b_0 + b_1 x + \cdots + b_m x^m$, and $fg = c_0 + c_1 x + \cdots + c_l x^l$. Since $(c_0, c_1, \dots, c_l) \subseteq (a_0, a_1, \dots, a_n)$ and $(c_0, c_1, \dots, c_l) \subseteq (b_0, b_1, \dots, b_m)$, if fg is primitive, then f and g are primitive. Conversely, suppose f and g are primitive. Since $(c_0, c_1, \dots, c_l) \subseteq (a_0, a_1, \dots, a_n)$ and $(c_0, c_1, \dots, c_l) \subseteq (b_0, b_1, \dots, b_m)$,

$$(a_0, a_1, \dots, a_n)(b_0, b_1, \dots, b_m) \subseteq (c_0, c_1, \dots, c_l).$$

But $(a_0, a_1, \dots, a_n)(b_0, b_1, \dots, b_m) = (1)(1) = (1)$. □

1.3. Generalize the results of Exercise 2 to a polynomial ring $A[x_1, \dots, x_r]$ in several indeterminates.

Solution. We claim following generalized results of Exercise 1.2.

Claim. *Let A be a ring and let $A[x_1, \dots, x_r]$ be the ring of polynomials in an indeterminate $x_1, \dots, x_r$, with coefficients in A. Let*

$$f = \sum_{\underline{i} \in \mathbf{Z}_{\geqslant 0}^r} a_{\underline{i}} \underline{x} \in A[x_1, \dots, x_r].$$

Here, we set $\underline{x}^{\underline{i}} = x_1^{i_1} \cdots x_r^{i_r}$ and $\underline{i} = (i_1, \cdots, i_r)$. Then

i) f is a unit in $A[x_1, \dots, x_r] \Leftrightarrow a_{\underline{0}}$ is a unit in A and $a_{\underline{i}}$ are nilpotent where $\underline{0} = (0, \cdots, 0)$ and $\underline{i} \in \mathbf{Z}_{\geqslant 0}^r \setminus \{\underline{0}\}$.

ii) f is nilpotent $\Leftrightarrow a_{\underline{i}}$ is nilpotent for all $\underline{i} \in \mathbf{Z}_{\geqslant 0}^r$.

iii) f is a zero-divisor $\Leftrightarrow$ there exists $a \neq 0$ in A such that $af = 0$.

iv) f is said to be primitive *if $(a_{\underline{i}} : \underline{i} \in \mathbf{Z}_{\geqslant 0}^r) = (1)$. If $f, g \in A[x_1, \dots, x_r]$, then fg is primitive $\Leftrightarrow f$ and g are primitive.*

Statement (i), (ii), and (iii) of the claim can be shown by tedious repetitions of induction on r, identifying f as a polynomial in $A[x_1, \dots, x_{r-1}][x_r]$; i.e., polynomial ring in an indeterminate x_r, with coefficients in $A[x_1, \dots, x_{r-1}]$. Proof of iv) is just a simple adaptation of the proof of (iv) in Exercise 1.2. □

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

Solution. Let $\mathfrak{N}$ be the nilradical of $A[x]$ and $\mathfrak{R}$ be the Jacobson radical of $A[x]$. Since every maximal ideal is prime, $\mathfrak{N} \subseteq \mathfrak{R}$. Now consider $f \in \mathfrak{R}$. Then by Proposition 1.9, $1 + fx$ is a unit, so $a_0, a_1, \cdots, a_n$ are all nilpotent, implying $f \in \mathfrak{N}$ by Exercise 1.2. □

1.5. Let A be a ring and let $A[[x]]$ be the ring of formal power series $f = \sum_{n=0}^{\infty} a_n x^n$ with coefficients in A. Show that

i) f is a unit in $A[[x]] \Leftrightarrow a_0$ is a unit in A.
ii) If f is nilpotent, then a_n is nilpotent for all $n \geqslant 0$. Is the converse true? (See Chapter 7, Exercise 2.)
iii) f belongs to the Jacobson radical of $A[[x]] \Leftrightarrow a_0$ belongs to the Jacobson radical of A.
iv) The contraction of a maximal ideal $\mathfrak{m}$ of $A[[x]]$ is a maximal ideal of A, and $\mathfrak{m}$ is generated by $\mathfrak{m}^c$ and x.
v) Every prime ideal of A is the contraction of a prime ideal of $A[[x]]$.

Solution. i) Suppose f is a unit, and $g = \sum_{m=0}^{\infty} b_m x^m$ is the multiplicative inverse of f. Then $a_0 b_0 = 1$, so a_0 is a unit in A. Conversely, suppose a_0 is a unit. Let

$$b_n = \begin{cases} a_0^{-1}, & \text{if } n = 0; \\ -a_0^{-1} \sum_{j=1}^{n} a_j b_{n-j}, & \text{if } n > 0. \end{cases}$$

Then $g = \sum_{m=0}^{\infty} b_m x^m$ is the multiplicative inverse of f, so f is a unit in $A[[x]]$.

ii) Induction on n. Assume $f^m = 0$ for some $m > 0$. Then $a_0^m = 0$, so a_0 is nilpotent. For $n > 0$, $f - a_0 - a_1 x - \cdots - a_{n-1}x^{n-1}$ is nilpotent by the induction hypothesis and Exercise 1.2, so a_n is also nilpotent.

The converse is not true in general. Let $A = \prod_{i=1}^{\infty} \mathbf{Z}/2^i\mathbf{Z}$ and consider the projection $\pi_i : A \twoheadrightarrow \mathbf{Z}/2^i\mathbf{Z}$. There is an element $a_i \in A$ such that $\pi_i(a_i) = 2 \in \mathbf{Z}/2^i\mathbf{Z}$ for each i, and $p_j(a_i) = 0 \in \mathbf{Z}/2^j\mathbf{Z}$ for every $j \neq i$. Then $a_i^i = 0$ for all $i > 0$, so a_i is nilpotent. However, the formal power series $f = \sum_{i=0}^{\infty} a_i x^i$ is not nilpotent, since there is no finite $m > 0$ such that $f^m = 0$.

iii) If f belongs to the Jacobson radical of $A[[x]]$, then $1 + bf$ is a unit in $A[[x]]$ for any $b \in A$. By (i), it implies $1 + ba_0$ is a unit in A for any $b \in A$, so a_0 is in the Jacobson radical of A. Conversely, suppose a_0 belongs to the Jacobson radical of A. Then for any $g = \sum_{m=0}^{\infty} b_m x^m \in A[[x]]$, $1 + gf$ is a unit in $A[[x]]$; equivalently, $1 + b_0 a_0$ is a unit in A by (i). Because the choice of g is arbitrary, this completes the proof.

iv) For any $f \in A[[x]]$, $1 + xf$ is a unit by (i), so (x) is contained by every maximal ideal of $A[[x]]$. Let $\pi : A[[x]] \twoheadrightarrow A[[x]]/(x)$ be the natural projection. Notice there is a natural isomorphism $A[[x]]/(x) \xrightarrow{\sim} A$ given by $a_0 + (x) \mapsto a_0$ for each $a_0 \in A$, and the composition $A \hookrightarrow A[[x]] \twoheadrightarrow A[[x]]/(x) \xrightarrow{\sim} A$ is actually the identity map on A. Let $\mathfrak{m}$ be a maximal ideal of $A[[x]]$. Since $\mathfrak{m}$. contains (x), the projection $\pi' : A[[x]] \twoheadrightarrow A[[x]]/(x) \xrightarrow{\sim} A$ sends it to a maximal ideal of A. However, it is the image of $\mathfrak{m}^c$ via the identity on A, so $\mathfrak{m}^c$ is a maximal ideal of A. The preimage of $\mathfrak{m}^c \subseteq A$ via π' is $\mathfrak{m}^c + (x)$. However, $\pi'(\mathfrak{m})$ is $\mathfrak{m}^c$, so $\mathfrak{m} \subseteq \mathfrak{m}^c + (x)$. Since $\mathfrak{m}^c \subseteq \mathfrak{m}$ and $(x) \subseteq \mathfrak{m}$, this shows $\mathfrak{m} = \mathfrak{m}^c + (x)$.

v) Under the same setting with the solution of (iv), recall $A \hookrightarrow A[[x]] \twoheadrightarrow A[[x]]/(x) \xrightarrow{\sim} A$ is the identity map on A. Let $\mathfrak{p}$ be a prime ideal of A. Then the preimage of $\mathfrak{p}$ via the projection $\pi' : A[[x]] \twoheadrightarrow A[[x]]/(x) \xrightarrow{\sim} A$ is also prime in $A[[x]]$. Then $\mathfrak{p}$ is the contraction of $(\pi')^{-1}(\mathfrak{p})$. □

1.6. A ring A is such that every ideal not contained in the nilradical contains a nonzero idempotent (that is, an element e such that $e^2 = e \neq 0$). Prove that the nilradical and Jacobson radical of A are equal.

Solution. Since every maximal ideal is prime, the Jacobson radical $\mathfrak{R}$ of A always contains the nilradical $\mathfrak{N}$ of A. If A is a zero ring, then the statement holds vacuously, so assume $1 \neq 0$. If $\mathfrak{R} \not\subseteq \mathfrak{N}$, then there exists a nonzero idempotent element e in $\mathfrak{R}$. Since $e(1-e)$, $1-e$ is a zero divisor; however, $1-e$ must be a unit in A by Proposition 1.9, a contradiction. $\square$

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

Solution. Let $\mathfrak{p}$ be a prime ideal of A. It suffices to show that $(y) + \mathfrak{p} = A$ for any $y \in A \setminus \mathfrak{p}$. For some $m > 1$, we have $y^m = y$, so $y(y^{m-1} - 1) = 0$. Since $\mathfrak{p}$ contains 0, it follows $y^{m-1} - 1 = x$ for some $x \in \mathfrak{p}$. Therefore, $1 = y^{m-1} - x \in (y) + \mathfrak{p}$. This ends the proof. $\square$

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.

Solution. Let $\mathscr{P}$ be a collection of all prime ideals of A, and suppose $\mathscr{C}$ is a totally ordered collection of prime ideals in A with respect to inclusion. Assume $xy \in \bigcap_{\mathfrak{p}\in\mathscr{C}} \mathfrak{p}$ for some $x, y \in A$. We claim that either $x \in \bigcap_{\mathfrak{p}\in\mathscr{C}} \mathfrak{p}$ or $y \in \bigcap_{\mathfrak{p}\in\mathscr{C}} \mathfrak{p}$. If not, then there are some $\mathfrak{p}_1, \mathfrak{p}_2 \in \mathscr{C}$ such that $x \notin \mathfrak{p}_1$ and $y \notin \mathfrak{p}_2$. Since $\mathscr{C}$ is totally ordered with respect to inclusion, we may say $\mathfrak{p}_1 \subseteq \mathfrak{p}_2$. If follows that $y \notin \mathfrak{p}_1$, a contradiction since $xy \in \mathfrak{p}_1$. Therefore, $\bigcap_{\mathfrak{p}\in\mathscr{C}} \mathfrak{p}$ is a prime ideal in A, and it is the lower bound for $\mathscr{C}$ in $\mathscr{P}$. As a result, assuming Zorn's lemma, $\mathscr{P}$ has a minimal element. $\square$

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

Solution. If $\mathfrak{a} = r(\mathfrak{a})$, then $\mathfrak{a}$ is the intersection of prime ideals containing $\mathfrak{a}$ by Proposition 1.14. Conversely, suppose $\mathfrak{a} = \bigcap_{\mathfrak{p}\in\mathcal{C}} \mathfrak{p}$ for some collection $\mathcal{C}$ of prime ideals. Observe $r\left(\bigcap_{\mathfrak{p}\in\mathcal{C}} \mathfrak{p}\right) = \bigcap_{\mathfrak{p}\in\mathcal{C}} \mathfrak{p}$; $x^n \in \mathfrak{p}$ implies $x \in \mathfrak{p}$ for each $\mathfrak{p} \in \mathcal{C}$. This completes the proof. $\square$

1.10. Let A be a ring, $\mathfrak{N}$ its nilradical. Show that the following are equivalent:

i) A has exactly one prime ideal;
ii) every element of A is either a unit or nilpotent;
iii) $A/\mathfrak{N}$ is a field.

Solution. [i) $\Rightarrow$ ii)] Let $\mathfrak{m}$ be the unique prime (hence, maximal) ideal of A. If $x \in A$ is not a unit, then there is some maximal ideal containing x; however, the maximal ideal must be $\mathfrak{m}$. Since $\mathfrak{m} = \mathfrak{N}$ by the assumption, it follows that every element of A is either a unit or nilpotent.

[ii) $\Rightarrow$ iii)] By the assumption, $\mathfrak{N}$ is maximal, because any ideal containing $\mathfrak{N}$ is either $\mathfrak{N}$ or A.

[iii) $\Rightarrow$ i)] Since $\mathfrak{N}$ is the intersection of all prime ideals, $\mathfrak{N}$ becomes the unique prime ideal of A. $\square$

1.11. A ring A is *Boolean* if $x^2 = x$ for all $x \in A$. In a Boolean ring A, show that

i) $2x = 0$ for all $x \in A$;
ii) every prime ideal $\mathfrak{p}$ is maximal, and $A/\mathfrak{p}$ is a field with two elements;
iii) every finitely generated ideal in A is principal.

Solution. i) For any $x \in A$, $2x = (2x)^2 = 2x^2 + 2x = 4x$, so $2x = 0$.

ii) By Exercise 7, every prime ideal is maximal. Suppose $y \in A$ is not in $\mathfrak{p}$. Since $y(y-1) = 0$ and $\mathfrak{p}$ contains 0, $\mathfrak{p}$ contains $y-1$. Therefore, $y = 1 + x$ for some $x \in \mathfrak{p}$, implying that $A/\mathfrak{p}$ consists of $\mathfrak{p}$ and $1 + \mathfrak{p}$.

iii) It suffices to show every ideal generated by two elements is principal. Consider (x, y) for $x, y \in A$. Surprisingly, for any $a, b \in A$, we have $ax + by = (ax + by)(x + y + xy)$, so $(x, y) = (x + y + xy)$. □

1.12. A local ring contains no idempotent $\neq 0, 1$

Solution. Suppose a local ring A with the maximal ideal $\mathfrak{m}$ has an idempotent e, which is neither 0 nor 1 (implying A is nonzero). Notice e is a zero divisor, for $e(1-e) = 0$. Therefore the unique maximal ideal $\mathfrak{m}$ must contains e. By Proposition 1.9, $1 - e$ must be a unit in A, since the Jacobson radical of A is just $\mathfrak{m}$. However, it is a contradiction for a zero divisor to be a unit. □

1.13. Let K be a field and let Σ be the set of all irreducible monic polynomials f in one indeterminate with coefficients in K. Let A be the polynomial ring over K generated by indeterminates x_f, one for each $f \in \Sigma$. Let $\mathfrak{a}$ be the ideal of A generated by the polynomials $f(x_f)$ for all $f \in \Sigma$. Show that $\mathfrak{a} \neq (1)$.

Let $\mathfrak{m}$ be a maximal ideal of A containing $\mathfrak{a}$, and let $K_1 = A/\mathfrak{m}$. Then K_1 is an extension field of K in which each $f \in \Sigma$ has a root. Repeat the construction with K_1 in place of K, obtaining a field K_2 , and so on. Let $L = \bigcup_{n=1}^{\infty} K_n$. Then L is a field in which each $f \in \Sigma$ splits completely into linear factors. Let $\bar{K}$ be the set of all elements of L which are algebraic over K. Then $\bar{K}$ is an algebraic closure of K.

Solution. Suppose $\mathfrak{a} = (1)$. There there exist some $f_1, \ldots, f_n \in \Sigma$ and $g_1, \ldots, g_n \in A$ such that

$$g_1 f_1(x_{f_1}) + \cdots + g_n f_n(x_{f_n}) = 1.$$

Write x_i instead of x_{f_i}. The polynomials g_i's involve only finitely many variables, so we can regard them as polynomials of $x_1, \ldots, x_N$ for some sufficiently large $N \geq n$. Now we have

$$g_1(x_1, \ldots, x_N) f_1(x_1) + \cdots + g_n(x_1, \ldots, x_N) f_n(x_n) = 1$$

By the basic field theory, there is a finite field extension K' so that $\alpha_i \in K'$ is a root for each f_i. Let $x_i = \alpha_i$ for $1 \leq i \leq n$ and $x_{n+1} = \cdots = x_N = 0$. Then we get a contradiction; $0 = 1$. □

1.14. In a ring A, let Σ be the set of all ideals in which every element is a zero-divisor. Show that the set Σ has maximal elements and that every maximal element of Σ is a prime ideal. Hence the set of zero-divisors in A is a union of prime ideals[1].

Solution. For any given $\mathfrak{b} \in \Sigma$, let Π be a totally ordered subset of Σ with respect to inclusion, in which every element contains $\mathfrak{b}$. Then $\bigcup_{\mathfrak{a} \in \Pi} \mathfrak{a}$ is clearly an ideal consisting of zero divisors, which is an upper bound for every element in Π. Assuming Zorn's lemma, Σ has a maximal element containing $\mathfrak{b}$.

[1]In Antiyah-Macdonald, 0 is also a zero divisor.

We claim that maximal elements of Σ are prime. Firstly, observe product of non-zero divisors is also non-zero divisor. Suppose ab is a zero divisor for some non-zero divisors $a, b \in A$. Then there exists some non-zero c so that $abc = 0$. Since a is a non-zero divisor, $bc = 0$, which is a contradiction since b is a non-zero divisor. Now, let $\mathfrak{p}$ be a maximal element of Σ, and suppose there exist $x, y \in A \setminus \mathfrak{p}$ such that xy is in $\mathfrak{p}$. By the maximality of $\mathfrak{p}$, there are some $p, q \in \mathfrak{p}$ and $a, b \in A$ so that both $p + ax$ and $q + by$ are non-zero divisor. However, $(p + ax)(q + by)$ is in $\mathfrak{p}$, which contradicts the previous observation that non-zero divisors are multiplicatively closed. $\square$

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.

These 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 $\operatorname{Spec}(A)$.

Solution. i) Clearly, $V(E) \supseteq V(\mathfrak{a}) \supseteq V(r(\mathfrak{a}))$, because $E \subseteq \mathfrak{a} \subseteq r(\mathfrak{a})$. Suppose $\mathfrak{p} \in V(E)$. Then, $E \subseteq \mathfrak{p}$ implies $\mathfrak{a} \subseteq \mathfrak{p}$, so $\mathfrak{p} \in V(\mathfrak{a})$. Assume $\mathfrak{q} \in V(\mathfrak{a})$. Since $\mathfrak{q} \supseteq \mathfrak{a}$, $\mathfrak{q} = r(\mathfrak{q}) \supseteq r(\mathfrak{a})$. As a result, $V(E) \subseteq V(\mathfrak{a}) \subseteq V(r(\mathfrak{a}))$.

ii) It is trivial.

iii) Suppose $\mathfrak{p} \in V\left(\bigcup_{i \in I} E_i\right)$. Then, $E_i \subseteq \mathfrak{p}$ for each $i \in I$, so $\mathfrak{p} \in \bigcap_{i \in I} V(E_i)$. Conversely, suppose $\mathfrak{q} \in \bigcap_{i \in I} V(E_i)$. Since $\mathfrak{q} \supseteq E_i$ for each $i \in I$, $\mathfrak{q} \supseteq \bigcup_{i \in I} E_i$, so $\mathfrak{q} \in V\left(\bigcup_{i \in I} E_i\right)$.

iv) Since $r(\mathfrak{a}\mathfrak{b}) = r(\mathfrak{a} \cap \mathfrak{b})$, $V(\mathfrak{a}\mathfrak{b}) = V(r(\mathfrak{a}\mathfrak{b})) = V(r(\mathfrak{a} \cap \mathfrak{b})) = V(\mathfrak{a} \cap \mathfrak{b})$ by Exercise 1.13 of the main text. Suppose $\mathfrak{a} \not\subseteq \mathfrak{p}$ and $\mathfrak{b} \not\subseteq \mathfrak{p}$ for some prime ideal $\mathfrak{p}$. By Proposition 1.11, $\mathfrak{a} \cap \mathfrak{b}$ is not contained in $\mathfrak{p}$. Therefore, $V(\mathfrak{a} \cap \mathfrak{b}) = V(\mathfrak{a}\mathfrak{b}) \subseteq V(\mathfrak{a}) \cup V(\mathfrak{b})$. The reverse inclusion is trivial. $\square$

1.16. Draw pictures of $\operatorname{Spec}(\mathbf{Z})$, $\operatorname{Spec}(\mathbf{R})$, $\operatorname{Spec}(\mathbf{C}[x])$, $\operatorname{Spec}(\mathbf{R}[x])$, $\operatorname{Spec}(\mathbf{Z}[x])$.

Solution. Omitted. $\square$

1.17. For each $f \in A$, let X_f denote the complement of $V(f)$ in $X = \operatorname{Spec}(A)$. 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) $X_f = \varnothing \Leftrightarrow f$ is nilpotent;
iii) $X_f = X \Leftrightarrow f$ is a unit;
iv) $X_f = X_g \Leftrightarrow r((f)) = r((g))$;

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

Solution. For any $\mathfrak{p} \in \operatorname{Spec}(A)$, $\mathfrak{p}$ is a proper ideal of A, so there exists some $f \in A$ not in $\mathfrak{p}$, and hence $\mathfrak{p} \in X_f$. Now suppose $\mathfrak{q} \in X_f \cap X_g$ for $f, g \in A$. Since $f \notin \mathfrak{q}$ and $g \notin \mathfrak{q}$, $fg \notin \mathfrak{q}$, so $\mathfrak{q} \in X_{fg}$. Moreover, for any $\mathfrak{p} \in X_{fg}$, $fg \notin \mathfrak{p}$, and therefore $f \notin \mathfrak{p}$ and $g \notin \mathfrak{q}$. As a result, $\mathfrak{q} \in X_{fg} = X_f \cap X_g$, and $\{X_f : f \in A\}$ forms a basis of open sets for the Zariski topology.

i) We have proven it already.

ii) By Proposition 1.8, it is obvious.

iii) $X_f = X$ if and only if every prime ideal does not contain f. By (1.5), every non-unit of A is contained in a maximal ideal, so $X_f = X$ if and only if f is a unit.

iv) $X_f = X_g$ if and only if $V(f) = V(g)$. By Proposition 1.14, the radicals of (f) and (g) are the intersections of the prime ideals which contain f and g, respectively, implying $r((f)) = r((g))$. Conversely, suppose $r(f) = r(g)$. Then,

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

by Exercise 1.15, so $X_f = X_g$.

v) Suppose $X = \bigcup_{i \in I}(X \setminus V(E_i))$ for some family of subsets $\{E_i\}_{i \in I}$ of A. Then,

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

by Exercise 1.15. Therefore, $A \bigcup_{i \in I} E_i = (1)$ (that is, the ideal generated by $\bigcup_{i \in I} E_i$ is A); otherwise, there exists some maximal ideal containing $\bigcup_{i \in I} E_i$ by Proposition 1.4. As a result, we can choose elements $E_1, E_2, \cdots, E_n$ of $\{E_i\}_{i \in I}$ such that

$$x_1 e_1 + x_2 e_2 + \cdots + x_m e_m = 1$$

where $x_1, x_2, \ldots, x_m \in A$ and $e_1, \ldots, e_m \in \bigcup_{j=1}^n E_j$ for $1 \le j \le n$. Now $\{X \setminus V(E_j)\}_{j=1}^n$ is a finite sub-covering of X.

vi) First we claim that $V(E) \subseteq V(F)$ if and only if $r(AE) \supseteq r(AF)$ for subsets E, F of A. Since the radicals of AE and AF are the intersections of the prime ideals which contain E and F respectively, the forward direction is obvious. The opposite direction is also clear, since $V(E) = V(r(AE)) \subseteq V(r(AF)) = V(F)$ by Exercise 1.15.

Assume $X_f \subseteq \bigcup_{i \in I}(X \setminus V(E_i))$ for some family of subsets $\{E_i\}_{i \in I}$ of A. Equivalently,

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

that is,

$$(f) \subseteq r(f) \subseteq r\left(A \bigcup_{i \in I} E_i\right).$$

Then we can choose elements $E_1, E_2, \ldots, E_n$ of $\{E_i\}_{i \in I}$ such that $f^l = x_1 e_1 + x_2 e_2 + \cdots + x_m e_m$ for some $l > 0$, $x_1, x_2, \ldots, x_m \in A$ and $e_1, e_2, \ldots, e_m \in \bigcup_{j=1}^n E_j$, so that $(f) \subseteq r(A \bigcup_j^n E_j)$. Therefore $X_f \subseteq \bigcup_{j=1}^n (X \setminus V(E_j))$.

vii) Since X_f is quasi-compact, if an open subset U of X is a finite union of sets of the form X_f, then clearly U is quasi-compact. Conversely, assume U is quasi-compact. Since X_f forms a basis for the Zariski topology, U can be expressed as the union of some subfamily of $\{X_f\}_{f\in A}$. Consequently, U is a finite union of sets of the form X_f. □

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 $X = \mathrm{Spec}(A)$. 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 $\mathrm{Spec}(A) \Leftrightarrow \mathfrak{p}_x$ is maximal;
ii) $\overline{\{x\}} = V(\mathfrak{p}_x)$;
iii) $y \in \overline{\{x\}} \Leftrightarrow \mathfrak{p}_x \subseteq \mathfrak{p}_y$;
iv) X is a T_0-space (this means that if x, y are distinct points of X, then either there is a neighborhood of x which does not contain y, or else there is a neighborhood of y which does not contain x).

***Solution*.** i) Suppose $\{x\}$ is closed. Then there exists some maximal ideal $\mathfrak{m}$ of A containing $\mathfrak{p}_x$. However, $\{x\}$ is singleton, so $\mathfrak{m} = \mathfrak{p}_x$. Conversely, if $\mathfrak{p}_x$ is maximal, then trivially $\{x\} = V(\mathfrak{p}_x)$.

ii) If $x \in V(E)$ for some $E \subseteq A$, then any prime ideal containing $\mathfrak{p}_x$ also belongs to $V(E)$; therefore $V(\mathfrak{p}_x) \subseteq V(E)$. Since $V(\mathfrak{p}_x)$ is contained by every closed set containing x and it is closed itself, we get $\overline{\{x\}} = V(\mathfrak{p}_x)$.

iii) $y \in \overline{\{x\}} = V(\mathfrak{p}_x)$ if and only if $\mathfrak{p}_y \supseteq \mathfrak{p}_x$ by the definition.

iv) Without loss of generality, assume $\mathfrak{p}_x \subsetneq \mathfrak{p}_y$. Then $\mathfrak{p}_y \notin V(\mathfrak{p}_x)$, so $\mathfrak{p}_y \in X \setminus V(\mathfrak{p}_x)$ and $\mathfrak{p}_x \notin X \setminus V(\mathfrak{p}_x)$. □

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 $\mathrm{Spec}(A)$ is irreducible if and only if the nilradical of A is a prime ideal.

***Solution*.** For any ideal $\mathfrak{a}$ and $\mathfrak{b}$ of A, if $X \setminus V(\mathfrak{a}) \neq \varnothing$ and $X \setminus V(\mathfrak{b}) \neq \varnothing$, then $(X \setminus V(\mathfrak{a})) \cap (X \setminus V(\mathfrak{b})) = \varnothing \Leftrightarrow$ if $V(\mathfrak{a}) \neq \mathrm{Spec}(A)$ and $V(\mathfrak{b}) \neq \mathrm{Spec}(A)$, then $V(\mathfrak{a}) \cup V(\mathfrak{b}) = V(\mathfrak{a}\mathfrak{b}) \neq \mathrm{Spec}(A) \Leftrightarrow$ if $\mathfrak{a} \not\subseteq \mathfrak{N}$ and $\mathfrak{b} \not\subseteq \mathfrak{N}$, then $\mathfrak{a}\mathfrak{b} \not\subseteq \mathfrak{N} \Leftrightarrow \mathfrak{N}$ is prime. □

1.20. Let X be a topological space.

i) If Y is an irreducible (Exercise 19) subspace of X, then the closure $\overline{Y}$ of Y in X is irreducible.
ii) Every irreducible subspace of X is contained in a maximal irreducible subspace.
iii) The maximal irreducible subspaces of X are closed and cover X. They are called the *irreducible components* of X. What are the irreducible components of a Hausdorff space?
iv) If A is a ring and $X = \mathrm{Spec}(A)$, then the irreducible components of X are the closed sets $V(\mathfrak{p})$, where $\mathfrak{p}$ is a minimal prime ideal of A (Exercise 8).

***Solution*.** i) Let U_1, U_2 be open set of X. If $Y \cap U_1 = \varnothing$, then U_1 contains no limit point of Y; hence, $\overline{Y} \cap U_1 = \varnothing$. Therefore, if $\overline{Y} \cap U_1 \neq \varnothing$ and $\overline{Y} \cap U_2 \neq \varnothing$, then $Y \cap U_1 \neq \varnothing$ and $Y \cap U_2 \neq \varnothing$. Since Y is irreducible, we get $Y \cap (U_1 \cap U_2) \neq \varnothing$, so $\overline{Y} \cap (U_1 \cap U_2) \neq \varnothing$. This shows $\overline{Y}$ is also irreducible.

ii) Let $\mathcal{I}$ be a collection of all irreducible subspaces of X containing an irreducible subspace $I \subseteq X$, and $\mathcal{C}$ be a totally ordered collection of irreducible subspaces in $\mathcal{I}$ with respect to inclusion. Suppose there are two disjoint nonempty open sets U_1 and U_2 of $\bigcup_{Y \in \mathcal{C}} Y$. Since U_1 is nonempty, there is some $Y_1 \in \mathcal{C}$ so that $U_1 \cap Y_1 \neq \varnothing$. Similarly, there exists $Y_2 \in \mathcal{C}$ such that $U_2 \cap Y_2 \neq \varnothing$. Because $\mathcal{C}$ is totally ordered, we may say $Y_1 \subseteq Y_2$. Then $Y_2 \cap U_1$ and $Y_2 \cap U_2$ are two disjoint nonempty open sets of Y_2, a contradiction for Y_2 to be irreducible. Therefore, $\bigcup_{Y \in \mathcal{C}} Y$ is also irreducible, and hence it is an upper bound for $\mathcal{C}$. Assuming Zorn's lemma, this shows I is contained in a maximal irreducible subspace.

iii) By (i), maximal irreducible subspaces of X are closed. Since one-point sets are clearly irreducible, every single point of X is contained in some maximal irreducible subspace by (ii); hence, it covers X. Now suppose X is Hausdorff. For any given subset $Y \subseteq X$, if Y has at least two points x_1 and x_2, then there are two disjoint open sets U_1 and U_2 of X so that $x_1 \in U_1 \cap Y$ and $x_2 \in U_2 \cap Y$. Therefore, the irreducible components of a Hausdorff space are singletons.

iv) We claim that closed irreducible subspaces of X are exactly the closed sets $V(\mathfrak{q})$, where $\mathfrak{q}$ is a prime ideal of A. Since $\{\mathfrak{q}\}$ is a singleton subset of $\operatorname{Spec}(A)$, it is irreducible; hence, its closure $\overline{\{\mathfrak{q}\}} = V(\mathfrak{q})$ is also irreducible by (i) and Exercise 1.18. Conversely, suppose $V(\mathfrak{a})$ is irreducible for given ideal $\mathfrak{a}$ of A. We may say $\mathfrak{a} = r(\mathfrak{a})$. If $\mathfrak{a}$ is not prime, then there are $b, c \in A \setminus \mathfrak{a}$ such that $bc \in \mathfrak{a}$. Then, $V(\mathfrak{a}) \supsetneq V(\mathfrak{a} + (b))$ and $V(\mathfrak{a}) \supsetneq V(\mathfrak{a} + (c))$, since $r(\mathfrak{a}) \neq r(\mathfrak{a} + (b))$ and $r(\mathfrak{a}) \neq r(\mathfrak{a} + (c))$. However, $V(\mathfrak{a}) \subseteq V(\mathfrak{a} + (b)) \cup V(\mathfrak{a} + (c))$, and hence $V(\mathfrak{a}) \setminus V(\mathfrak{a} + (b))$ and $V(\mathfrak{a}) \setminus V(\mathfrak{a} + (c))$ are two nonempty disjoin open sets of $V(\mathfrak{a})$, a contradiction. As a result, the claim implies the irreducible components of X are exactly $V(\mathfrak{p})$, where $\mathfrak{p}$ is a minimal prime ideal of A. □

1.21. Let $\phi : A \to B$ be a ring homomorphism. Let $X = \operatorname{Spec}(A)$ and $Y = \operatorname{Spec}(B)$. If $\mathfrak{q} \in Y$, then $\phi^{-1}(\mathfrak{q})$ is a prime ideal of A, i.e., a point of X. Hence ϕ induces a mapping $\phi^* : Y \to X$. Show that

i) If $f \in A$ then $\phi^{*-1}(X_f) = Y_{\phi(f)}$, and hence that ϕ^* is continuous.
ii) If $\mathfrak{a}$ is an ideal of A, then $\phi^{*-1}(V(\mathfrak{a})) = V(\mathfrak{a}^e)$
iii) If $\mathfrak{b}$ is an ideal of B, then $\overline{\phi^*(V(\mathfrak{b}))} = V(\mathfrak{b}^c)$.
iv) If ϕ is surjective, then ϕ^* is a homeomorphism of Y onto the closed subset $V(\operatorname{Ker}(\phi))$ of X. (In particular, $\operatorname{Spec}(A)$ and $\operatorname{Spec}(A/\mathfrak{N})$ (where $\mathfrak{N}$ is the nilradical of A) are naturally homeomorphic.)
v) If ϕ is injective, then $\phi^*(Y)$ is dense in X. More precisely, $\phi^*(Y)$ is dense in $X \Leftrightarrow \operatorname{Ker}(\phi) \subseteq \mathfrak{N}$.
vi) Let $\psi : B \to C$ be another ring homomorphism. Then $(\psi \circ \phi)^* = \phi^* \circ \psi^*$.
vii) Let A be an integral domain with just one non-zero prime ideal $\mathfrak{p}$, and let K be the field of fractions of A. Let $B = (A/\mathfrak{p}) \times K$. Define $\phi : A \to B$ by $\phi(x) = (\bar{x}, x)$, where $\bar{x}$ is the image of x in $A/\mathfrak{p}$. Show that ϕ^* is bijective but not a homeomorphism.

Solution. i) Notice $\mathfrak{q} \in \phi^{*-1}(X_f) \Leftrightarrow \phi^*(\mathfrak{q}) \in X_f \Leftrightarrow \phi^{-1}(\mathfrak{q}) \in X_f \Leftrightarrow f \notin \phi^{-1}(\mathfrak{q}) \Leftrightarrow \phi(f) \notin \mathfrak{q} \Leftrightarrow \mathfrak{q} \in Y_{\phi(f)}$, so $\phi^{*-1}(X_f) = Y_{\phi(f)}$. Because X_f forms a basis for the Zariski topology, ϕ^* is continuous.

ii) Observe $\mathfrak{p} \in \phi^{*-1}(V(\mathfrak{a})) \Leftrightarrow \phi^*(\mathfrak{p}) \in V(\mathfrak{a}) \Leftrightarrow \mathfrak{a} \subseteq \phi^*(\mathfrak{p}) \Leftrightarrow \mathfrak{a} \subseteq \phi^{-1}(\mathfrak{p}) \Leftrightarrow \mathfrak{a}^e \subseteq \mathfrak{p} \Leftrightarrow \mathfrak{p} \in V(\mathfrak{a}^e)$.

iii) Notice $\phi^*(V(\mathfrak{b}))$ consists of $\mathfrak{q}^c$ where $\mathfrak{q} \subseteq B$ is a prime ideal containing $\mathfrak{b}$. Since $\mathfrak{b} \subseteq \mathfrak{q}$ implies $\mathfrak{b}^c \subseteq \mathfrak{q}^c$, we get $\phi^*(V(\mathfrak{b})) \subseteq V(\mathfrak{b}^c)$. To show $V(\mathfrak{b}^c)$ is actually the smallest closed set containing $\phi^*(V(\mathfrak{b}))$, suppose $\phi^*(V(\mathfrak{b})) \subseteq V(\mathfrak{a})$ for some ideal $\mathfrak{a}$ of A. Then $V(\mathfrak{b}) \subseteq \phi^{*-1}(V(\mathfrak{a})) = V(\mathfrak{a}^e)$, so $r(\mathfrak{b}) \supseteq r(\mathfrak{a}^e)$. However, $r(\mathfrak{b}^c) = r(\mathfrak{b})^c \supseteq r(\mathfrak{a}^e)^c = r(\mathfrak{a}^{ec}) \supseteq r(\mathfrak{a})$, and hence $V(\mathfrak{b}^c) \subseteq V(\mathfrak{a})$.

iv) For $\mathfrak{p}, \mathfrak{q} \in Y$, suppose $\phi^*(\mathfrak{p}) = \phi^*(\mathfrak{q})$. Then $\phi^{-1}(\mathfrak{p}) = \phi^{-1}(\mathfrak{q})$, and hence $\mathfrak{p} = \mathfrak{q}$ by the surjectivity of ϕ. Therefore, ϕ^* is injective. Now prove the following claim.

Claim. *Let $\phi : A \to B$ be a surjective ring homomorphism. If $\mathfrak{a}$ is an ideal of A, then $\phi(\mathfrak{a})$ is also an ideal of B. Moreover, if $\mathfrak{a}$ is a prime containing* $\mathrm{Ker}(\phi)$*, then $\phi(\mathfrak{a})$ is also prime.*

Proof. For any $y \in B$, $\phi(x) = y$ for some $x \in A$. Then $y\phi(\mathfrak{a}) = \phi(x)\phi(\mathfrak{a}) = \phi(x\mathfrak{a}) \subseteq \phi(\mathfrak{a})$. Now assume $\mathfrak{a}$ is a prime ideal of A. Then $\overline{\phi} : A/\mathfrak{a} \to B/\phi(\mathfrak{a})$ defined by $x+\mathfrak{a} \mapsto \phi(x)+\phi(\mathfrak{a})$ is a ring isomorphism, for it is clearly surjective, and $\phi(x) \in \phi(\mathfrak{p})$ implies $x \in \mathfrak{a}+\mathrm{Ker}(\phi) = \mathfrak{a}$. Therefore, $B/\phi(\mathfrak{p})$ is an integral domain, so $\phi(\mathfrak{a})$ is prime in B. □

Assume $\mathfrak{p}$ is a prime ideal of A containing $\mathrm{Ker}(\phi)$; that is, $\mathfrak{p} \in V(\mathrm{Ker}(\phi))$. Then $\phi(\mathfrak{p})$ is prime in B by the claim, so $\mathfrak{p}$ is a preimage of some prime in Y, implying $V(\mathrm{Ker}(\phi)) \subseteq \phi^*(Y)$. Since every prime ideal contains 0, the opposite inclusion is trivial.

Finally, let's show $\phi^* : Y \to V(\mathrm{Ker}(\phi))$ is a closed map. For any ideal $\mathfrak{b}$ of Y, we claim that $\phi^*(V(\mathfrak{b})) = V(\mathrm{Ker}(\phi)) \cap V(\mathfrak{b}^c)$. If a prime ideal $\mathfrak{q}$ in B contains $\mathfrak{b}$, then clearly $\mathfrak{q}^c$ contains $\mathfrak{b}^c$ and $\mathrm{Ker}(\phi)$, so $\phi^*(V(\mathfrak{b})) \subseteq V(\mathrm{Ker}(\phi)) \cap V(\mathfrak{b}^c)$. For the opposite inclusion, notice $V(\mathrm{Ker}(\phi)) \cap V(\mathfrak{b}^c) = V(\mathrm{Ker}(\phi) + \mathfrak{b}^c) = V(\mathfrak{b}^c)$. By the claim, if a prime ideal $\mathfrak{p}$ of A contains $\mathfrak{b}^c$, then $\phi(\mathfrak{p})$ is a prime containing $\mathfrak{b}$. This shows $\phi^* : Y \to V(\mathrm{Ker}(\phi))$ is a closed map, so is a homeomorphism of Y onto V $(\mathrm{Ker}(\phi))$. Since $\mathfrak{p} \supseteq \mathrm{Ker}(\phi)$, $\phi^{-1}(\phi(\mathfrak{p})) = \mathfrak{p} + \mathrm{Ker}(\phi) = \mathfrak{p}$; hence, $\mathfrak{p} \in \phi^*(V(\mathfrak{b}))$ and $\phi^*(V(\mathfrak{b})) = V(\phi^{-1}(\mathfrak{b}))$. This shows that ϕ^* is a homeomorphism from Y to $V(\mathrm{Ker}(\phi))$.

In particular, natural surjective homomorphism $\pi : A \to A/\mathfrak{N}$ induces homeomorphism π^* from $\mathrm{Spec}(A)$ to $\mathrm{Spec}(A/\mathfrak{N})$ for the Zariski topology, observing $V(\mathfrak{N}) = \mathrm{Spec}(A)$.

v) By (iii), $X = \overline{\phi^*(Y)} = \overline{\phi^*(V(0))} = V(\mathrm{Ker}(\phi))$ if and only if $\mathrm{Ker}(\phi) \subseteq \mathfrak{N}$. In particular, if ϕ is injective, then $\phi^*(Y)$ is dense in X.

vi) Let $\mathfrak{q}$ be a prime ideal of C. Then $(\psi \circ \phi)^*(\mathfrak{q}) = (\psi \circ \phi)^{-1}(\mathfrak{q}) = \phi^{-1}(\psi^{-1}(\mathfrak{q})) = (\phi^* \circ \psi^*)(\mathfrak{q})$.

vii) $\mathrm{Spec}(A)$ is the Sierpiński space on $\{0, \mathfrak{p}\}$. It is easy to show that for any nonzero commutative rings A, B, prime ideals of the direct product $A \times B$ are of the form $\mathfrak{p} \times B$ or $A \times \mathfrak{q}$ where $\mathfrak{p}$ and $\mathfrak{q}$ are prime ideals of A and B respectively. Therefore, $\mathrm{Spec}(B)$ is the discrete topology on $\{\bar{0} \times K, A/\mathfrak{p} \times 0\}$. Since $\phi^*(\bar{0} \times K) = \mathfrak{p}$ and $\phi^*(A/\mathfrak{p} \times 0) = 0$, ϕ^* is a bijective continuous function, but clearly not a homeomorphism. □

1.22. Let $A = \prod_{i=1}^n A_i$ be the direct product of rings A_i. Show that $\mathrm{Spec}(A)$ is the disjoint union of open (and closed) subspaces X_i, where X_i is canonically homeomorphic with $\mathrm{Spec}(A_i)$.

Conversely, let A be any ring. Show that the following statements are equivalent:

i) $X = \mathrm{Spec}(A)$ is disconnected.
ii) $A \cong A_1 \times A_2$ where neither of the rings A_1, A_2 is the zero ring.
iii) A contains an idempotent $\neq 0, 1$.

In particular, the spectrum of a local ring is always connected (Exercise 12)

Solution. It is easy to show that every ideals of A is of the form $\mathfrak{a}_1 \times \cdots \times \mathfrak{a}_n$ where each $\mathfrak{a}_i$ is an ideal of A_i, and every prime ideal of A is of the form $A_1 \times \cdots \times A_{i-1} \times \mathfrak{p} \times A_{i+1} \times \cdots \times A_n$ where $\mathfrak{p}$ is a prime ideal of A_i. Let

$$X_i := V(A_1 \times \cdots \times A_{i-1} \times 0 \times A_{i+1} \times \cdots \times A_n)$$

for each $1 \leq i \leq n$. Clearly, $A = \coprod_{i=1}^n X_i$ as a set. Since

$$X_i = A \setminus (X_1 \cup \cdots \cup X_{i-1} \cup X_{i+1} \cup \cdots \cup X_n),$$

each X_i is both open and closed. Let S be subset of A. Then,

$$S \cap X_i = V(A_1 \times \cdots \times A_{i-1} \times \mathfrak{a}_i \times A_{i+1} \times \cdots \times A_n)$$

for an ideal $a_i \subseteq A_i$ for each $1 \leq i \leq n$ if and only if $S = V(\mathfrak{a}_1 \times \cdots \times \mathfrak{a}_n)$. Therefore, $A = \coprod_{i=1}^n X_i$ as a topology. Consider the canonical projection $\pi_i : A \to A_i$. Since $\mathrm{Ker}(\pi) = A_1 \times \cdots \times A_{i-1} \times 0 \times A_{i+1} \times \cdots \times A_n$, the induced continuous map $\pi^* : \mathrm{Spec}(A_i) \to \mathrm{Spec}(A)$ is a homeomorphism of $\mathrm{Spec}(A_i)$ into X_i by Exercise 1.22.

By the previous discussion, (ii) clearly implies (i). Since $(1, 0) \in A_1 \times A_2$ is an idempotent, (ii) also implies (iii). Conversely, if A contains an idempotent $e \neq 0, 1$, then by the Chines Remainder Theorem (Proposition 1.10), we get

$$A \cong A/(e(e-1)) = A/(e)(e-1) \cong A/(e) \times A/(e-1),$$

since $(e) + (e-1) = (1)$. This shows that (ii) and (iii) are equivalent. The remaining part, which is actually the hardest one, is to show (i) $\Rightarrow$ (ii) or (iii). Firstly, we shall prove a lemma.

Lemma. *Let A be a ring. For $a, b \in A$, if $(a) + (b) = (1)$, then $(a^k) + (b) = (1)$ for any integer $k \geq 1$.*

Proof. Induction on k. The case for $k = 1$ is trivial; there are $c_1, d_1 \in A$ satisfying $c_1 a + d_1 b = 1$. For $k > 1$, by the induction hypothesis, there exist $c_{k-1}, d_{k-1} \in A$ so that $c_{k-1}a^{k-1} + d_{k-1}b = 1$. Then,

$$1 = (c_1 a + d_1 b)(c_{k-1}a^{k-1} + d_{k-1}b) = c_1 c_{k-1} a^k + (c_1 d_{k-1} + d_1 c_{k-1} a^{k-1} + d_1 d_{k-1} b)b.$$

□

Now, suppose $\mathrm{Spec}(A)$ is disconnected. There exist two ideals $\mathfrak{a}_1, \mathfrak{a}_2$ of A so that $\mathrm{Spec}(A) = V(\mathfrak{a}_1) \cup V(\mathfrak{a}_2)$ and $V(\mathfrak{a}_1) \cap V(\mathfrak{a}_2) = \varnothing$. There is no harm assuming $r(\mathfrak{a}_1) = \mathfrak{a}_1$ and $r(\mathfrak{a}_2) = \mathfrak{a}_2$ (Exercise 1.15). Let $\mathfrak{N}$ be the nilradical of A. Since $V(\mathfrak{a}_1) \cup V(\mathfrak{a}_2) = V(\mathfrak{a}_1 \cap \mathfrak{a}_2)$, we get $\mathfrak{a}_1 \cap \mathfrak{a}_2 \subseteq \mathfrak{N}$. However, $r(\mathfrak{a}_1 \cap \mathfrak{a}_2) = r(\mathfrak{a}_1) \cap r(\mathfrak{a}_2) = \mathfrak{a}_1 \cap \mathfrak{a}_2$, so $\mathfrak{a}_1 \cap \mathfrak{a}_2 = \mathfrak{N}$, for $\mathfrak{a}_1 \cap \mathfrak{a}_2$ is itself the intersection of all prime ideals in A. Moreover, because $V(\mathfrak{a}_1) \cap V(\mathfrak{a}_2) = V(\mathfrak{a}_1 + \mathfrak{a}_2) = \varnothing$, we have $\mathfrak{a}_1 + \mathfrak{a}_2 = (1)$. Therefore, due to the Chinese Remainder Theorem,

$$A/\mathfrak{N} = A/\mathfrak{a}_1\mathfrak{a}_2 \cong A/\mathfrak{a}_1 \times A/\mathfrak{a}_2.$$

Hence, $A/\mathfrak{N}$ has an idempotent $(\bar{1}, \bar{0})$, so there exists $e \in A$ so that $e^2 - e = n$ for some $n \in \mathfrak{N}$. Since n is nilpotent, there is some positive integer k so that $n^k = 0$, implying $e^k(e-1)^k = 0$. However, by the lemma, $(e)^k + (1-e)^k = (1)$, so by the Chinese Remainder Theorem again,

$$A \cong A/(e)^k(1-e)^k \cong A/(e)^k \times A/(1-e)^k.$$

In particular, a local ring contains no idempotent (Exercise 1.12), so the spectrum of a local ring must be connected. □

1.23. Let A be a Boolean ring (Exercise 11), and let $X = \mathrm{Spec}(A)$.

i) For each $f \in A$, the set X_f (Exercise 17) is both open and closed in X.
ii) Let $f_1, \dots, f_n \in A$. Show that $X_{f_1} \cup \dots \cup X_{f_n} = X_f$ for some $f \in A$.
iii) The sets X_f are the only subsets of X which are both open and closed.
iv) X is a compact Hausdorff space.

Solution. i) We only need to show X_f is closed. Since $f(f-1) = 0$ and $(f)+(f-1) = (1)$, every prime ideal of A contains only one of f and $f-1$. Therefore, $X_f = V(f-1)$.

ii) By Exercise 1.11, every finitely generated ideal in A is principal. Therefore, there exists some f such that $(f_1, \dots, f_n) = (f)$, so $X_{f_1} \cup \dots \cup X_{f_n} = X_f$.

iii) Suppose $V(\mathfrak{a})$ is a set which are both open and closed. Since X_f forms a basis for $\mathrm{Spec}(A)$, there are family of sets $\{X_f\}_{f \in S}$ for some subset S of A such that $V(\mathfrak{a}) = \bigcup_{f \in S} X_f$. However, closed subspace of quasi-compact space is also quasi-compact, so there are finitely many $f_1, \dots, f_n$ so that $V(\mathfrak{a}) = X_{f_1} \cup \dots \cup X_{f_n}$. By (ii), we get $V(\mathfrak{a}) = X_g$ for some $g \in A$.

iv) We already know X is quasi-compact (Exercise 1.17). To show X is Hausdorff, consider two distinct primes $\mathfrak{p}$ and $\mathfrak{q}$ of A. Choose some $f \in \mathfrak{p} \setminus \mathfrak{q}$. Then $\mathfrak{q}$ must contain $f-1$, since $0 = f(f-1)$. Because every prime ideal must contain one of f and $f-1$, open sets X_f and X_{f-1} are disjoint, while satisfying $\mathfrak{q} \in X_f$ and $\mathfrak{q} \in X_{f-1}$. □

1.24. Let L be a lattice, in which the sup and inf of two elements a, b are denoted by $a \vee b$ and $a \wedge b$ respectively. L is a *Boolean lattice* (or *Boolean algebra*) if

i) L has a least element and a greatest element (denoted by 0, 1 respectively).
ii) Each of $\vee, \wedge$ is distributive over the other.
iii) Each $a \in L$ has a unique "complement" $a' \in L$ such that $a \vee a' = 1$ and $a \wedge a' = 0$.

(For example, the set of all subsets of a set, ordered by inclusion, is a Boolean lattice.)

Let L be a Boolean lattice. Define addition and multiplication in L by the rules

$$a + b = (a \wedge b') \vee (a' \wedge b), \quad ab = a \wedge b.$$

Verify that in this way L becomes a Boolean ring, say $A(L)$.

Conversely, starting from a Boolean ring A, define an ordering on A as follows: $a \leqslant b$ means that $a = ab$. Show that, with respect to this ordering, A is a Boolean lattice.

Solution. Let a, b, c be arbitrary elements of L. Clearly, $a \wedge b = b \wedge a$ and $a \vee b = b \vee a$, so the addition and multiplication of $A(L)$ are commutative. Notice $0' = 1$ and $1' = 0$. Using the definition of supremum and infimum, it is easy to show that the associativity laws for $\wedge$ and $\vee$ hold; $a \vee (b \vee c) = (a \vee b) \vee c$ and $a \wedge (b \wedge c) = (a \wedge b) \wedge c$. Now, we shall prove two lemmas.

Lemma 1 (De Morgan's Law)**.** *Let L be a Boolean lattice. Then $(a \vee b)' = a' \wedge b'$ and $(a \wedge b)' = a' \vee b'$ for any $a, b \in L$.*

Proof. $(a \vee b) \vee (a' \wedge b') = [(a \vee a') \vee b] \wedge [a \vee (b \vee b')] = (1 \vee b) \wedge (a \vee 1) = 1 \wedge 1 = 1$, and $(a \vee b) \wedge (a' \wedge b') = [(a \wedge a') \vee (b \wedge a')] \wedge [(a \wedge b') \vee (b \wedge b')] = [0 \vee (b \wedge a')] \wedge [(a \wedge b') \vee 0] = (b \wedge a') \wedge (a \wedge b') = (a \wedge a') \wedge (b \wedge b') = 0 \wedge 0 = 0$. Therefore, by the uniqueness of complement, we have $(a \vee b)' = a' \wedge b'$. By switching the position of a' with a', and b' with b in $(a \vee b)' = a' \wedge b'$, we get $(a \wedge b)' = a' \vee b'$. □

Lemma 2. *Let L be a Boolean lattice. Then $(a \wedge b') \vee (a' \wedge b) = (a \vee b) \wedge (a \wedge b)'$.*

Proof. Using Lemma 1, $(a\wedge b')\vee(a'\wedge b) = (a\vee(a'\wedge b))\wedge(b'\vee(a'\wedge b)) = (a\vee b)\wedge(b'\vee a') = (a \vee b) \wedge (a \wedge b)'$. □

We claim the addition '$+$' is associative. Using the lemmas, we have

$$\begin{aligned}(a+b)+c &= ((a+b)\wedge c') \vee ((a+b)' \wedge c)\\ &= (((a\wedge b')\vee(a'\wedge b))\wedge c')\vee(((a\vee b)'\vee(a\wedge b))\wedge c)\\ &= (a\wedge b'\wedge c')\vee(a'\wedge b\wedge c')\vee(a'\wedge b'\wedge c)\vee(a\vee b\vee c).\end{aligned}$$

Observe the last expression is independent of the order of a, b, c, so the addition is associative. The additive identity is the least element 0, since

$$a+0 = (a\wedge 1)\vee(a'\wedge 0) = a\vee 0 = a.$$

Similarly, the multiplicative identity is the greatest element 1; $a1 = a \wedge 1 = a$. Lastly, the distributive law holds, because

$$\begin{aligned}ab+ac &= (a\wedge b\wedge(a\wedge c)')\vee((a\wedge b)'\wedge a\wedge c)\\ &= (a\wedge b\wedge(a'\vee c'))\vee((a'\vee b')\wedge a\wedge c)\\ &= (b\wedge(a\wedge c'))\vee((b'\wedge a)\wedge c)\\ &= a\wedge((b\wedge c')\vee(b'\wedge c))\\ &= a(b+c).\end{aligned}$$

Since $a^2 = a \wedge a = a$, this shows that $A(L)$ is a Boolean ring.

Conversely, assume A is a Boolean ring. Then 1 is the greatest element since $a = a1$ for any $a \in A$. Because $0 = 0a$ for all $a \in A$, 0 is the least element. Notice $a(a+b+ab) = a$ and $b(a+b+ab) = b$ (Exercise 1.11). Moreover, if $c \in A$ satisfies $a = ac$ and $b = bc$, then $(a+b+ab)c = a+b+ab$. Similarly, it is easy to see that $(ab)a = (ab)b = ab$, and if $d \in A$ satisfies $d = da = db$, then $d = (ab)d$. Therefore, $a \vee b = a+b+ab$ and $a \wedge b = ab$. Using this fact,

$$\begin{aligned}a\wedge(b\vee c) &= a(b+c+bc)\\ &= ab+ac+abc\\ &= ab+ac+a^2bc\\ &= ab+ac+(ab)(ac)\\ &= (a\wedge b)\vee(a\wedge c),\end{aligned}$$

and

$$\begin{aligned}(a\vee b)\wedge(a\vee c) &= (a+b+ab)(a+c+ac)\\ &= a+bc+abc\\ &= a\vee(b\wedge c).\end{aligned}$$

The complement of a is $a' := 1-a$, since $a\vee a' = a+(1-a)+a(1-a) = 1$ and $a(1-a) = 0$. This shows that A is a Boolean lattice. □

1.25. From the last two exercises deduce Stone's theorem, that every Boolean lattice is isomorphic to the lattice of open-and-closed subsets of some compact Hausdorff topological space.

Solution. Let L be a Boolean lattice. Then by Exercise 24, we can view L as a Boolean ring $A(L)$ where the order is given by $a \leqslant b \Leftrightarrow a = ab$. Recall $\operatorname{Spec}(A(L))$ is a compact Hausdorff topological space, and $X_a := \operatorname{Spec}(A(L)) \setminus V(a)$ is an open-and-closed subset for each $a \in A$. Let $\mathcal{B} := \{X_a \subseteq \operatorname{Spec}(A(L)) : a \in A\}$, and endow order on $\mathcal{B}$ with respect to inclusion. Then $\mathcal{B}$ becomes a Boolean lattice, since

- $X_1 = \operatorname{Spec}(A(L))$ is the greatest, $X_0 = \emptyset$ is the least element,
- $X_a \vee X_b = X_a \cup X_b = X_{a+b+ab}$ ($\because$ Exercise 1.11),
- $X_a \wedge X_b = X_a \cap X_b = X_{ab}$,
- Each $\wedge, \vee$ is distributive, for each $\cap, \cup$ is,
- $X_a' = X_{(1-a)}$.

We claim that $X_a \subseteq X_b$ if and only if $a \leq b$. In particular, $X_a = X_b$ if and only if $a = b$. Only the forward direction is non-trivial. If $X_a \subseteq X_b$, then $r(a) \subseteq r(b)$. But $A(L)$ is boolean, so $(a) \subseteq (b)$. Therefore, there is some $x \in A(L)$ so that $a = xb$. Because $a = a^2 = xab$ and $ab = (xab)b = xab$, we finally get $a = ab$. Therefore, a map $\psi : L \to \mathcal{B}$ defined by $a \mapsto X_a$ is a well-defined bijection, since it is clearly surjective. Actually, it is a lattice isomorphism; observe

$$\begin{aligned} \psi(a \wedge b) &= \psi(ab) = X_{ab} = X_a \wedge X_b, \text{ and} \\ \psi(a \vee b) &= \psi(a + b + ab) = X_{a+b+ab} = X_a \vee X_b. \end{aligned}$$

This ends the proof. $\square$

1.26. Let A be a ring. The subspace of $\operatorname{Spec}(A)$ consisting of the maximal ideals of A, with the induced topology, is called the *maximal spectrum* of A and is denoted by $\operatorname{Max}(A)$. For arbitrary commutative rings it does not have the nice functorial properties of $\operatorname{Spec}(A)$ (see Exercise 21), because the inverse image of a maximal ideal under a ring homomorphism need not be maximal.

Let X be a compact Hausdorff space and let $C(X)$ denote the ring of all real-valued continuous functions on X (add and multiply functions by adding and multiplying their values). For each $x \in X$, let $\mathfrak{m}_x$ be the set of all $f \in C(X)$ such that $f(x) = 0$. The ideal $\mathfrak{m}_x$ is maximal, because it is the kernel of the (surjective) homomorphism $C(X) \to \mathbf{R}$ which takes f to $f(x)$. If $\widetilde{X}$ denotes $\operatorname{Max}(C(X))$, we have therefore defined a mapping $\mu : X \to \widetilde{X}$, namely $x \mapsto \mathfrak{m}_x$.

We shall show that μ is a homeomorphism of X onto $\widetilde{X}$.

i) Let $\mathfrak{m}$ be any maximal ideal of $C(X)$, and let $V = V(\mathfrak{m})$ be the set of common zeros of the functions in $\mathfrak{m}$: that is,

$$V = \{x \in X : f(x) = 0 \text{ for all } f \in \mathfrak{m}\}.$$

Suppose that V is empty. Then for each $x \in X$ there exists $f_x \in \mathfrak{m}$ such that $f_x(x) \neq 0$. Since f_x is continuous, there is an open neighborhood U_x of x in X on which f_x does not vanish. By compactness a finite number of the neighborhoods, say $U_{x_i}, \dots, U_{x_n}$ cover X. Let

$$f = f_{x_1}^2 + \cdots + f_{x_n}^2.$$

Then f does not vanish at any point of X, hence is a unit in $C(X)$. But this contradicts $f \in \mathfrak{m}$, hence V is not empty.

Let x be a point of V. Then $\mathfrak{m} \subseteq \mathfrak{m}_x$, hence $\mathfrak{m} = \mathfrak{m}_x$ because $\mathfrak{m}$ is maximal. Hence μ is surjective.

ii) By Urysohn's lemma (this is the only non-trivial fact required in the argument) the continuous functions separate the points of X. Hence $x \neq y \Rightarrow \mathfrak{m}_x \neq \mathfrak{m}_y$, and therefore μ is injective.

iii) Let $f \in C(X)$; let

$$U_f = \{x \in X : f(x) \neq 0\}$$

and let

$$\widetilde{U}_f = \{\mathfrak{m} \in \tilde{X} : f \notin \mathfrak{m}\}$$

Show that $\mu(U_f) = \widetilde{U}_f$. The open sets U_f (resp. $\widetilde{U}_f$) form a basis of the topology of X (resp. $\widetilde{X}$) and therefore μ is a homeomorphism.

Thus X can be reconstructed from the ring of functions $C(X)$.

Solution. Suppose $\mathfrak{m}$ is in $\mu(U_f)$. Then $\mathfrak{m} = \mathfrak{m}_x$ for some $x \in X$ such that $f(x) \neq 0$. Hence, $f \notin \mathfrak{m}_x$, so $\mu(U_f) \subseteq \widetilde{U}_f$. Conversely, suppose $\mathfrak{n} \in \widetilde{U}_f$. Since μ is surjective, there is some $y \in X$ so that $\mathfrak{n} = \mathfrak{m}_y$. Then $f(y) \neq 0$, so y is in U_f. This shows $\mu(U_f) = \widetilde{U}_f$.

Let $Y := \operatorname{Spec}(C(X))$. For each $f \in C(X)$, notice $\widetilde{U}_f = \widetilde{X} \cap Y_f$. Since the open sets Y_f of Y form a basis for the topology of Y by Exercise 1.17, the open sets $\widetilde{U}_f$ form a basis for the subspace $\widetilde{X}$ of Y. For each $x \in X$, $x \in U_g$ for any constant function g, so open sets U_f cover X. Also, for any $f, g \in C(X)$, observe $U_{fg} = U_f \cap U_g$. Therefore, open sets U_f form a basis for X. □

1.27. Let k be an algebraically closed field and let

$$f_\alpha(t_1, \ldots, t_n) = 0$$

be a set of polynomial equations in n variables with coefficients in k. The set X of all points $x = (x_1, \ldots, x_n) \in k^n$ which satisfy these equations is an *affine algebraic variety*.

Consider the set of all polynomials $g \in k[t_1, \ldots, t_n]$ with the property that $g(x) = 0$ for all $x \in X$. This set is an ideal $I(X)$ in the polynomial ring, and is called the *ideal of the variety* X. The quotient ring

$$P(X) = k[t_1, \ldots, t_n]/I(X)$$

is the ring of polynomial functions on X, because two polynomials g, h define the same polynomial function on X if and only if $g - h$ vanishes at every point of X, that is, if and only if $g - h \in I(X)$.

Let ξ_i be the image of t_i in $P(X)$. The ξ_i $(1 \leqslant i \leqslant n)$ are the *coordinate functions* on X: if $x \in X$, then $\xi_i(x)$ is the ith coordinate of x. $P(X)$ is generated as a k-algebra by the coordinate functions, and is called the *coordinate ring* (or affine algebra) of X.

As in Exercise 26, for each $x \in X$ let $\mathfrak{m}_x$ be the ideal of all $f \in P(X)$ such that $f(x) = 0$; it is a maximal ideal of $P(X)$. Hence, if $\widetilde{X} = \operatorname{Max}(P(X))$, we have defined a mapping $\mu : X \to \widetilde{X}$, namely $x \mapsto \mathfrak{m}_x$.

It is easy to show that μ is injective: if $x \neq y$, we must have $x_i \neq y_i$ for for some i $(1 \leqslant i \leqslant n)$, and hence $\xi_i - x_i$ is in $\mathfrak{m}_x$, but not in $\mathfrak{m}_y$, so that $\mathfrak{m}_x \neq \mathfrak{m}_y$. What is less obvious (but still true) is that μ is *surjective*. This is one form of Hilbert's Nullstellensatz (see Chapter 7).

Solution. (It is too hard to solve this problem without assuming any result in Chapter 7) Assume Corollary 7.10. Then for any $\mathfrak{m} \in \widetilde{X}$, we have $P(X)/\mathfrak{m} \cong k$ since $P(X)$ is a finitely generated k-algebra generated by $\xi_1, \dots \xi_n$. Let a_i be the image of ξ_i in k by the homomorphism $P(X) \twoheadrightarrow P(X)/\mathfrak{m} \cong k$, and $a := (a_1, \dots, a_n) \in k^n$. It is easy to see that $(\xi_1 - a_1, \dots, \xi_n - a_n)$ is a maximal ideal of $P(X)$. Since $\mathfrak{m}_a$ contains $(\xi_1 - a_1, \dots, \xi_n - a_n)$, we get $\mathfrak{m}_a = (\xi_1 - a_1, \dots, \xi_n - a_n)$. Then $\mathfrak{m}$ is a maximal ideal which contains $\mathfrak{m}_a = (\xi_1 - a_1, \dots, \xi_n - a_n)$. Therefore, $\mathfrak{m} = \mu(a)$. □

1.28. Let $f_1, \dots, f_m$ be elements of $k[t_1, \dots, t_n]$. They determine a *polynomial mapping* $\phi : k^n \to k^m$: if $x \in k^n$, the coordinates of $\phi(x)$ are $f_1(x), \dots, f_m(x)$.

Let X, Y be affine algebraic varieties in k^n, k^m respectively. A mapping $\phi : X \to Y$ is said to be *regular* if ϕ is the restriction to X of a polynomial mapping from k^n to k^m.

If η is a polynomial function on Y, then $\eta \circ \phi$ is a polynomial function on X. Hence ϕ induces a k-algebra homomorphism $P(Y) \to P(X)$, namely $\eta \mapsto \eta \circ \phi$. Show that in this way we obtain a one-to-one correspondence between the regular mappings $X \to Y$ and the k-algebra homomorphisms $P(Y) \to P(X)$.

Solution. For a given regular map $\phi : X \to Y$, let $\phi_\star : P(Y) \to P(X)$ be the induced k-algebra homomorphism given by $\eta \mapsto \eta \circ \phi$. Then $\phi \mapsto \phi_\star$ is a map from the set of regular maps $X \to Y$ to the set of k-algebra homomorphisms $P(Y) \to P(X)$. Now, we construct an inverse of $\phi \mapsto \phi_\star$. Suppose $\varphi : P(Y) \to P(X)$ is a k-algebra homomorphism. Then we can find a k-algebra homomorphism $\tilde{\varphi} : k[t'_1, \dots, t'_m] \to k[t_1 \dots, t_n]$ so that the following diagram commutes[2]

$$\begin{tikzcd} k[t'_1, \dots, t'_m] \arrow[r, "\tilde{\varphi}"] \arrow[d, two heads] & k[t_1, \dots, t_n] \arrow[d, two heads] \\ P(Y) \arrow[r, "\varphi"] & P(X). \end{tikzcd}$$

Define a polynomial map $\varphi^* : k^n \to k^m$ by

$$\varphi^*(x) := (\tilde{\varphi}(t'_1)(x), \dots, \tilde{\varphi}(t'_m)(x)).$$

For any $f \in k[t'_1, \dots, t'_m]$, notice $\tilde{\varphi}(f) = f(\tilde{\varphi}(t'_1), \dots, \tilde{\varphi}(t'_m))$. Since the previous diagram commutes, if $f \in I(Y)$ then $f(\tilde{\varphi}(t'_1), \dots, \tilde{\varphi}(t'_m))$ is in $I(X)$. Therefore, for $x \in X$, we have $f(\varphi^*(x)) = 0$ for any $f \in I(Y)$, so $\varphi^*(X) \subseteq Y$. This shows $\varphi^* : X \to Y$ is regular, and we get a map $\varphi \mapsto \varphi^*$ from the set of k-algebra homomorphisms $P(Y) \to P(X)$ to the set of regular maps $X \to Y$.

We claim that $\varphi \mapsto \varphi^*$ is the two-sided inverse of $\phi \mapsto \phi_\star$. For any k-algebra homomorphism $\varphi : P(Y) \to P(X)$, $g \in P(Y)$, and $x \in X$,

$$\begin{aligned} (\varphi^*)_\star(g)(x) &= (g \circ \varphi^*)(x) \\ &= g(\tilde{\varphi}(t'_1)(x), \dots, \tilde{\varphi}(t'_m)(x)) \\ &= \varphi(g)(x), \end{aligned}$$

observing $\tilde{\varphi}(\tilde{g}) = \tilde{g}(\tilde{\varphi}(t'_1), \dots, \tilde{\varphi}(t'_m))$ where $\tilde{g} \in k[t'_1, \dots, t'_n]$ is a preimage of g. Therefore, $(\varphi^*)_\star = \varphi$. Conversely, suppose $\phi : X \to Y$ is a regular map. Then $\phi(x) =$

[2]One may construct $\tilde{\varphi}$ as follows. Let ξ_i be the image of t'_i in $P(Y)$ and ζ_j be the image of t_j in $P(X)$. Then $\varphi(\xi_i) = p_i(\zeta_1, \dots, \zeta_n)$ for some polynomial $p_i \in k[t_1, \dots, t_n]$. By letting $t'_i \mapsto p_i(t_1, \dots, t_n)$, we get a desired k-algebra homomorphism.

$(f_1(x), \ldots, f_m(x))$ where $f_i \in k[t_1, \ldots, t_m]$. For $x \in X$, we have

$$\begin{aligned}(\phi_\star)^*(x) &= (\tilde{\phi}_\star(t'_1)(x), \ldots, \tilde{\phi}_\star(t'_m)(x)) \\ &= (f_1(x), \ldots, f_m(x)) \\ &= \phi(x),\end{aligned}$$

observing $\phi_\star(g) = g \circ \phi = g(f_1, \ldots, f_m)$ for any $g \in P(Y)$ and hence $\tilde{\phi}_\star(t'_i) = f_i$. Therefore, $(\phi_\star)^* = \phi$ This shows that $\phi \mapsto \phi_\star$ and $\varphi \mapsto \varphi^*$ are bijections. $\square$