

Rings and Ideals

Xie, Kaitao

Exercise 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: From the formula $1 - x^n = (1 - x)(1 + x^2 + \cdots + x^{n-1})$ we get $1 - (-x)^n = (1 + x)(1 + x^2 + \cdots + (-x)^{n-1})$. Since x is nilpotent, the formula immediately show that $1 + x$ is a unit. If u is a unit and x as above, then $u^{-1}(u + x) = 1 + u^{-1}x$ and since $u^{-1}x$ is nilpotent, $1 + u^{-1}x$ is a unit, which implies that $u + x = u(1 + u^{-1}x)$ is also a unit.

Exercise 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, \cdots, a_n are nilpotent.

ii) f is nilpotent $\Leftrightarrow a_0, \cdots, a_n$ 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 $(a_0, \cdots, a_n) = (1)$. Prove that if $f, g \in A[x]$, then fg is primitive $\Leftrightarrow f$ and g are primitive.

Solution: i) If f is a unit, then a_0 must be a unit. If $g = b_0 + b_1x + \cdots + b_mx^m$ satisfies $fg = 1$, then we show by induction that $a_n^{r+1}b_{m-r} = 0$ for $0 \leq r \leq m$. Since $fg = 1$, we have $a_nb_m = 0$, and $\sum_{i+j=t} a_ib_j = 0$ for $0 \leq t \leq m+n-1$. Suppose that $a_n^k b_{m-k} = 0$ holds for $0 \leq k \leq r-1$, then from $a_n^r \sum_{i+j=m+n-r} a_ib_j = 0$ we have $a_n^{r+1}b_{m-r} = 0$ ($0 \leq i \leq n$ hence $m-r \leq j \leq m$). a_n is nilpotent since $a_n^{m+1}b_0 = 0$ and b_0 is a unit. Hence $f - a_nx^n$ is also a unit from Exercise 1. Apply induction we see that a_i is nilpotent for $1 \leq i \leq n$.

If a_1, \cdots, a_n are nilpotent and a_0 is a unit, suppose $a_i^{m_i} = 0$ and let $m = \sum_{i=1}^n m_i$, then $f^m = a_0^m$ which is a unit, so f is a unit.

ii) Suppose f is nilpotent, and $f^m = 0$, which implies that $a_n^m = 0$, and $f - a_nx^n$ is also nilpotent. Apply induction we see that a_0, \cdots, a_n are nilpotent.

Suppose a_0, \cdots, a_n are nilpotent and $a_i^{m_i} = 0$, and let $m = \sum_{i=0}^n m_i$, then $f^m = 0$.

iii) \Leftarrow is trivial.

Suppose $g = b_0 + b_1x + \cdots + b_mx^m$ is a polynomial of **lowest degree** such that $fg = 0$, then $a_nb_m = 0$ and $a_ng = 0$ by the selection of g . Suppose $a_{n-k}g = 0$ for $0 \leq k \leq r-1$, then $(f - \sum_{k=0}^{r-1} a_{n-k}x^{n-k})g = 0$ and $a_{n-r}b_m = 0$ so $a_{n-r}g = 0$. This implies that $a_ib_0 = 0$ for $0 \leq i \leq n$ and $b_0f = 0$.

iv) If f or g is not primitive, then fg is not primitive from the formula of the coefficients of fg .

If both f and g primitive but fg is not primitive, let M be a maximal ideal that contains all of the coefficients of fg . Send an element of $A[x]$ to $(A/M)[x]$ by sending the coefficients to the equivalent class, then $f \neq 0$ and $g \neq 0$ since they are primitive, but $fg = 0$. This contradicts to the fact that A/M is a field and $(A/M)[x]$ is an integral domain.

Exercise 3

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

Solution: DO NOT WANT TO.

Exercise 4

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

Solution: Since all the maximal ideal is prime, the nilradical is in the Jacobson radical. If f is in the Jacobson radical, then $1 - fg$ is a unit for all $g \in A[x]$. Let $g = -x$ then $1 + xf$ is a unit implies that all the coefficients of f is nilpotent by Exercise 2 i), and this gives that f is nilpotent by Exercise 2 ii).

Exercise 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 $n \geq 0$. Is the converse true?

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 M of $A[[x]]$ is a maximal ideal of A , and M is generated by M^c and x .

v) Every prime ideal of A is the contraction of a prime ideal of $A[[x]]$.

Solution: i) If f is a unit then a_0 is a unit by the formula of the coefficients of the product of two polynomials.

If a_0 is a unit, then we can solve the coefficient formula for f^{-1} one by one, and f is a unit.

ii) $f^m = 0$ implies $a_0^m = 0$. Suppose a_k is nilpotent for $0 \leq k \leq n$ then $g = a_0 + a_1 x + \dots + a_n x^n$ is nilpotent by Exercise 2 ii), and $f - g$ is still nilpotent. Suppose $(f - g)^r = 0$ then $a_{n+1}^r = 0$, and a_{n+1} is nilpotent. By induction we show that a_n is nilpotent for $n \geq 0$.

iii) If f is in the Jacobson radical of $A[[x]]$, then $\forall b \in A$, we have $1 - bf$ is a unit in $A[[x]]$ and this gives $1 - a_0 b$ is a unit in A by i), hence a_0 is in the Jacobson radical of A .

If a_0 is in the Jacobson radical of A , then $\forall g = b_0 + \dots \in A[[x]]$, we have $1 - fg$ is a unit since $1 - a_0 b_0$ is a unit, hence f is in the Jacobson radical of $A[[x]]$.

iv) The map is inclusion, and $M^c = i^{-1}(M)$. Suppose $b \notin M^c$, then $b \notin M$. By the maximality of M , $\exists f \in M$, such that $f + b = 1$, so this f must be in A , and hence in M^c , which implies that M^c is maximal in A . By the maximality of M , it must contain M^c and x , and $\forall f \in M$ where $f = \sum_{n=0}^{\infty} a_n x^n$, $a_0 \in M^c$ and let $g = \sum_{n=1}^{\infty} a_n x^{n-1}$, then $f = a_0 + xg$. Hence M is generated by M^c and x .

v) Let P be a prime ideal in A . It's obvious that $P = (i(P), x)^c$, and it's sufficient to show that $(i(P), x)$ is prime in $A[[x]]$. If $f = \sum_{n=0}^{\infty} a_n x^n$ and $g = \sum_{m=0}^{\infty} b_m x^m$, with $fg \in (i(P), x)$, then $a_0 b_0 \in P$ and $a_0 \in P$ or $b_0 \in P$, so $f \in (i(P), x)$ or $g \in (i(P), x)$, which completes the proof.

Exercise 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: Note that the nilradical is contained in the Jacobson radical. If there exists x in the Jacobson radical of A but not the nilradical of A , then (x) contains a nonzero idempotent, i.e. $\exists y \in A$, s.t. $(xy)^2 = x^2 y^2 = xy \neq 0$, then $1 - x^2 y^2 = 1 - xy = u$ which is a unit. $xy = 1 - u$, but $1 - u = (1 - u)^2$ gives $u(1 - u) = 0$ which contradicts to the fact that u is a unit.

Exercise 7

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

Solution: Let P be a prime ideal of A , and $x \notin P$, then $\exists n > 1$, s.t. $x^n = x$, which is $x(1 - x^{n-1}) = 0 \in P$. Since P prime, $1 - x^{n-1} \in P$, so $P + (x) = A$ and P is maximal.

Exercise 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: Every nonzero commutative ring with identity has a maximal ideal, so the set of all prime ideals is not empty. We shall prove that for every chain $P_1 \supset P_2 \supset \cdots \supset P_n \supset \cdots$, there is a prime ideal P contained in every P_i . By Zorn's Lemma we claim that there is a minimal prime ideal. To see this, let $P = \cap P_i$. It's sufficient to show that P is a prime ideal. It's an ideal indeed. If $xy \in P$, then $\forall i$, $x \in P_i$ or $y \in P_i$. If $y \in P_i \forall i$, then done. If not, suppose that $y \notin P_n$, then $y \notin P_k \forall k \geq n$, and this implies $x \in P_k \forall k \geq n$, so $x \in P_i \forall i$ and P is a prime ideal.

Exercise 9

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

Solution: \Rightarrow is trivial since $r(I)$ is itself prime.

\Leftarrow : Write $I = \cap P_\alpha$. $I \subset r(I)$ trivially. If $x \in r(I)$ then $\exists n > 0$ s.t. $x^n \in I$. This then gives that $x^n \in P_\alpha$ and then $x \in P_\alpha \forall \alpha$ since P_α prime, hence $x \in I$ and done.

Exercise 10

Let A be a ring, R 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/R is a field.

Solution: i) \Rightarrow iii): Since A has exactly one prime ideal, it must be R and it's also a maximal ideal.

iii) \Rightarrow ii): If $x \in A - R$, then $[x] \in A/R$ is nonzero, hence is a unit, so x is also a unit in A .

ii) \Rightarrow i): The hypothesis implies that R is not contained in any proper ideal, and since R is the intersection of all prime ideals in A , R can not contain any prime ideal except itself. But R is itself a prime ideal by the hypothesis, so A has exactly one prime ideal.

Exercise 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 P is maximal, and A/P is a field with two elements;
- iii) every finitely generated ideal in A is principal.

Solution: i) $2x = (2x)^2 = 4x^2 = 4x$, so $2x = 0$.

ii) By Exercise 7, we know that P is maximal. To show the second part, it's sufficient to show that $\forall y \in A - P$, $y - 1 \in P$. Since $(y - 1)^2 = y - 1$, $(y - 1)y = 0 \in P$, and since P prime with $y \notin P$, we have $y - 1 \in P$ and done.

iii) It's sufficient to prove that (x, y) is principle. Notice that $x(x + y - xy) = x$ and $y(x + y - xy) = y$, we have $(x, y) = (x + y - xy)$.

Exercise 12

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

Solution: Suppose $\exists x \in A$, s.t. $x^2 = x$ and $x \neq 0, 1$, then easy computation show that $(1+x)^2 = 1+x$. Let M_1 and M_2 be two maximal ideals which contain x and $1+x$, respectively. M_1 and M_2 exists since neither x nor $1+x$ is unit. By the locality of A , $M_1 = M_2 = M$ and $1 = -x + (1+x) \in M$, which is absurd.

Exercise 13

(*Construction of an algebraic closure of a field*) 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 of each $f \in \Sigma$. Let I be the ideal of A generated by the polynomials $f(x_f)$ for all $f \in \Sigma$. Show that $I \neq (1)$.

Let M be a maximal ideal of A containing I , and let $K_1 = A/M$. 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: In fact, the only nontrivial claim is that $I \neq (1)$. If $I = (1)$, then there is $k_1, \dots, k_n \in A$ and $f_1(x_{f_1}), \dots, f_n(x_{f_n})$, s.t. $1 = \sum_{i=1}^n k_i f_i(x_{f_i})$. Add proper index if necessary, we may assume that $k_i = g_i(x_{f_1}, \dots, x_{f_n})$ (the added index j will have $g_j = 0$). That is, there exist irreducible $f_i(x_i)$, $1 \leq i \leq n$ s.t. $J = (f_1(x_1), \dots, f_n(x_n)) = K[x_1, \dots, x_n]$. We suppose that this n is the minimal number that satisfies this condition, then $I_0 = (f_1(x_1), \dots, f_n(x_{n-1})) \neq K[x_1, \dots, x_{n-1}]$. Let $R = K[x_1, \dots, x_{n-1}]$, and $S = R[x_n]$. Then $J = (I_0, f_n(x_n)) = S$. Let $\pi_1 : R[x_n] \rightarrow (R/I_0)[x_n]$, $\pi_2 : (R/I_0)[x_n] \rightarrow \frac{(R/I_0)[x_n]}{(f_n(x_n))}$. The two codomains are nonzero since $I_0 \neq R$ and $f_n(x_n)$. But $\pi_2 \circ \pi_1$ is surjective yet $J = R[x_n] \subset \text{Ker}(\pi_2 \circ \pi_1)$, which is a contradiction.

In addition, since K_1 contains a root \bar{x}_f for each f , and f has root no more than $\deg f$, L contains all roots of irreducible polynomials over K and \bar{K} is what we want.

Exercise 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-divisor in A is a union of prime ideals.

Solution: $(0) \in \Sigma$. If there is a sequence in Σ , $I_1 \subset I_2 \subset \dots \subset I_n \subset \dots$, let $I = \bigcup_{n=1}^{\infty} I_n$. We shall prove that I is an ideal that consists of zero-divisor. Then by Zorn's Lemma we show that Σ has maximal elements. The only thing needed to prove is that I is an ideal. If $a \in I$, $b \in I$, and $c \in A$ then $a \in I_n$, and $b \in I_m$ for some m, n . Then $a \in I_{m+n}$ and $b \in I_{m+n}$, so $a - b \in I_{m+n} \subset I$, and $ac \in I_n \subset I$. Hence I is an ideal.

If I is a maximal element, with $x \notin I$, and $y \notin I$, then there are elements in $(x) + I$ and $(y) + I$, which are not zero-divisor. Then their product is in $(xy) + I$, which is not a zero-divisor, so $xy \notin I$. Hence I is prime.

Exercise 15

(*The prime spectrum of a ring*) 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 I is the ideal generated by E , then $V(E) = V(I) = V(r(I))$.
- ii) $V(0) = X$, $V(1) = \emptyset$.
- iii) if (E_i) is any family of subsets of A , then $V(\bigcup_i E_i) = \bigcap_i V(E_i)$.
- iv) $V(I \cap J) = V(IJ) = V(I) \cup V(J)$ for any ideals I, J of A .

This result show that the sets $V(E)$ satisfy the axioms for closed sets in a topological space. The

resulting topology is called *Zariski* topology. The topological space X is called the prime spectrum of A , and is written $\text{Spec}(A)$.

Solution: i) $V(I) \subset V(E)$ trivially, and since I is the smallest ideal which contains I , every ideal contains E should contain I , hence $V(I) \subset V(E)$. Again, $I \subset r(I)$ so $V(r(I)) \subset V(I)$, and since $r(I)$ is the intersection of all prime ideals which contain I , every prime ideal contains I will contain $r(I)$, hence $V(I) \subset V(r(I))$.

ii) Every prime ideal contains 0, hence $V(0) = X$. Every prime ideal (since proper by definition) do not contain 1, hence $V(1) = \emptyset$.

iii) Since $E_i \subset \cap_i E_i$, we have $V(\cup_i E_i) \subset V(E_i), \forall i$. If $P \in \cap_i V(E_i)$ then $E_i \in P \forall i$, so $\cup_i E_i \subset P$, and $P \in V(\cup_i E_i)$.

iv) $V(I) \cup V(J) \subset V(I \cap J)$ trivially. If $P \in V(I \cap J)$ then $I \cap J \subset P$. To show that either $I \subset P$ or $J \subset P$, suppose the contrary holds. Then $\exists a \in I$ and $b \in J$ s.t. $a \notin P$ and $b \notin P$, but $ab \in I \cap J \subset P$, which is a contradiction. Hence $V(I \cap J) = V(I) \cup V(J)$. The proof for $V(I \cap J) = V(IJ)$ is similar.

Exercise 16

Draw pictures of $\text{Spec}(\mathbb{Z})$, $\text{Spec}(\mathbb{R})$, $\text{Spec}(\mathbb{C}[x])$, $\text{Spec}(\mathbb{R}[x])$, $\text{Spec}(\mathbb{Z}[x])$.

Solution: We only give the descriptions of all these sets.

$\text{Spec}(\mathbb{Z}) = \{(p) : p \text{ prime or zero}\}$.

$\text{Spec}(\mathbb{R}) = \{(0)\}$.

$\text{Spec}(\mathbb{C}[x]) = \{(x+a) : a \in \mathbb{C}\} \cup \{(0)\}$.

$\text{Spec}(\mathbb{R}[x]) = \{(x+a) : a \in \mathbb{R}\} \cup \{(x^2+bx+c) : b^2-4c < 0\} \cup \{(0)\}$.

$\text{Spec}(\mathbb{Z}[x]) = \{(f(x)) : f(x) \text{ irreducible}\} \cup \{(p) : p \text{ prime or zero}\} \cup \{(f(x), p) : f(x) \text{ irreducible and } p \text{ prime}\}$. This one is nontrivial and there are references on the Internet.

Exercise 17

For each $f \in A$, let X_f denote the complement of $V(f)$ in $X = \text{Spec}(A)$. The set 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) $X_f = \emptyset \Leftrightarrow f$ 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 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 $X = \text{Spec}(A)$.

Solution: i) It is sufficient to show that $V(f) \cup V(g) = V(fg)$. This is trivial by 15. i) and iv).

ii) Trivial since f nilpotent if and only if it's contained in all prime ideals of A .

iii) Every non-unit is contained in a maximal ideal, which is prime, hence if $X_f = X$ then f is a unit. If f is a unit, then no prime ideal contains f and $X_f = X$.

i) and iii) together imply that X_f form a basis of the Zariski topology of $\text{Spec}(A)$.

iv) If $X_f = X_g$, then every prime ideal containing f contains g , so $r((g)) \subset r((f))$, and we claim that $r((f)) = r((g))$ since they are symmetrically equivalent. The other direction is similar.

v) It's enough to consider a covering of X by basis $\{X_{f_i}\}$. That is, $\forall P \in \text{Spec}(A), \exists f_i \notin P$. Then $(f_i) = (1)$ since if not, then it must be contained in some maximal ideal, which is prime, and leads to a contradiction. Hence $\sum_{j=1}^n g_{ij} f_{ij} = 1$ for some i_j and $\{X_{f_{ij}}\}$ is a finite subcovering of $\{X_{f_i}\}$.

vi) If $X - V(I_\alpha)$ is an open covering of X_f , then we have $\cup_\alpha (X - V(I_\alpha)) \supset X - V(f)$, which is $\cap_\alpha V(I_\alpha) = V(\sum I_\alpha) \subset V(f)$, so $r(f) \in r(\sum I_\alpha)$. There are $\alpha_1, \dots, \alpha_n$, and integer m s.t. $f^m \in \sum_{i=1}^n I_{\alpha_i}$, and this implies that $X - V(I_{\alpha_i})$ is a finite subcovering of $X - V(I_\alpha)$.

vii) If S is a finite union of some basic open sets, then it's obviously quasi-compact. Suppose S is open and quasi-compact, then it's the union of some basic open sets since they form a basis for X and S is open. This gives an open covering of S and can be reduced to a finite subcovering since S is quasi-compact, and each cover set is contained in S , which implies the claim.

Exercise 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 $X = \text{Spec}(A)$. When thinking of x as a prime ideal of A , we denote it by 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 $\text{Spec}(A) \Leftrightarrow P_x$ is maximal;

ii) $\overline{\{x\}} = V(P_x)$;

iii) $y \in \overline{\{x\}} \Leftrightarrow P_x \subset P_y$;

iv) X is a T_0 -space.

Solution: i) If $\{x\}$ is closed, then $\exists E \subset A$, s.t. $\{x\} = V(E)$. This only happens when P_x is maximal. If P_x is maximal, then $V(P_x) = \{x\}$ and $\{x\}$ is closed.

ii) $\{x\} \subset V(P_x)$ and $V(P_x)$ is closed, so $\overline{\{x\}} \subset V(P_x)$. $\forall P \in V(P_x)$ and $X_f \ni P$, $P_x \subset P$ and $f \notin P$, then $f \notin P_x$, and $X_f \cap \{x\} \neq \emptyset$. Hence $V(P_x) = \{x\}$.

iii) If $y \in \overline{\{x\}}$ then $\overline{\{y\}} \subset \overline{\{x\}}$, so $V(P_y) \subset V(P_x)$ and $r(P_x) \subset r(P_y)$, that is, $P_x \subset P_y$ since they are prime, and vice versa.

iv) Suppose $x \neq y$ and there is no open set which contains y but do not contain x , then $y \in \overline{\{x\}}$, and by iii) we have $P_x \subset P_y$ but $P_x \neq P_y$. Hence $x \notin \overline{\{y\}}$ and our claim follows.

Exercise 19

A topological space X is said to be irreducible if $X \neq \emptyset$ 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 $\text{Spec}(A)$ is irreducible if and only if the nilradical of A is a prime ideal.

Solution: First we show that the two definitions for irreducible space are equivalent. Suppose that every pair of non-empty open subsets of X intersect. If U is a non-empty open subset, then every neighborhood of every point in X intersect U , so every point in X is a limit point of U , and $\bar{U} = X$. Suppose that $\bar{U} = X$ for every non-empty open set U . For every pair of non-empty open sets U and V , $V \subset \bar{U}$, and every point in V is a limit point of U , hence $U \cap V \neq \emptyset$.

We observe that a topological space is irreducible if the union of every pair of proper closed subsets is not the whole space. Suppose that $\text{Spec}(A)$ is irreducible, and fg is nilpotent, but f is not nilpotent, then $V(fg) = \text{Spec}(A)$, and $V(f) \neq \text{Spec}(A)$, but we have that $V(fg) = V(f) \cup V(g)$, so $V(g) = \text{Spec}(A)$ and g is nilpotent. Hence the nilradical is prime.

If the nilradical R of A is prime, then every nonempty X_f (where f is not nilpotent by 17 ii)) contains R . Hence A is irreducible.

Exercise 20

Let X be a topological space.

i) If Y is an irreducible subspace of X , then the closure \bar{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 irreducible components of X . What are the irreducible components of a Hausdorff space?

iv) If A is a ring and $X = \text{Spec}(A)$, then the irreducible components of X are closed sets $V(P)$,

where P is a minimal prime ideal of A .

Solution: i) If U and V are two non-empty open subsets of \bar{Y} , then $\exists U', V'$ open in X , s.t. $U = U' \cap \bar{Y}$, and $V = V' \cap \bar{Y}$. They are not empty, so U' and V' contain points in \bar{Y} and should intersect with Y . Since $U \cap Y = U' \cap Y$, $V \cap Y = V' \cap Y$, which are non-empty open subsets of Y , they intersect. Hence $U \cap V \cap Y$ is non-empty, so $U \cap V$ is non-empty and \bar{Y} is irreducible.

ii) Suppose that Y is a irreducible subspace of X , and let Σ be the set of all irreducible subspaces of X which contain Y . Y is contained in Σ so Σ is not empty. If $S_1 \subset S_2 \subset \cdots \subset S_n \subset \cdots$ is a sequence in Σ , let $S = \bigcup_{n=1}^{\infty} S_n$. We shall show that S is irreducible and by Zorn's lemma, we claim that Σ has a maximal element with respect to inclusion. If U, V are non-empty open subsets in S , then there must be an integer n , s.t. $U' = U \cap S_n \neq \emptyset$ and $V' = V \cap S_n \neq \emptyset$, and they are open subsets of S_n . Since S_n is irreducible, they must intersect, which implies that $U \cap V \neq \emptyset$.

iii) If Y is a maximal irreducible subspace of X , then Y must be closed since \bar{Y} is irreducible and contains Y . Since for every point x in X , which is also in a subspace $\{x\}$ of X , we can find a maximal irreducible subspace of X which contains x . Hence the irreducible components cover X . If X is Hausdorff, then the irreducible components are the single point sets.

iv) We claim that $V(I)$ is irreducible if and only if $r(I)$ is prime. Then since $V(I_1) \subset V(I_2) \Leftrightarrow r(I_2) \subset r(I_1)$, we know that if $V(I) = V(r(I))$ is maximal irreducible, then $r(I)$ is a minimal prime ideal, and complete the proof.

Suppose that $V(I) = V(r(I))$ is irreducible. If $fg \in r(I)$, then we have $X_{fg} \cap V(I) = (X_f \cap V(I)) \cap (X_g \cap V(I)) = \emptyset$, hence either $X_f \cap V(I) = \emptyset$ or $X_g \cap V(I) = \emptyset$. Suppose $X_f \cap V(I) = \emptyset$, then f belongs to all prime ideals which contains I , so $f \in r(I)$. Hence $r(I)$ is prime.

Suppose that $r(I)$ is prime. To prove that $V(I)$ is irreducible, it's sufficient to prove that $\forall f, g \in A$, satisfy $X_f \cap V(I) \neq \emptyset$, and $X_g \cap V(I) \neq \emptyset$, we have $X_{fg} \cap V(I) \neq \emptyset$. If so, then $f \notin r(I)$ and $g \notin r(I)$, then $fg \notin r(I)$ since $r(I)$ is prime. Hence $X_{fg} \cap V(I) \neq \emptyset$.

Exercise 21

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

i) If $f \in A$ then $\phi^{*-1}(X_f) = Y_{\phi(f)}$, and hence that ϕ^* is continuous.

ii) If I is an ideal of A , then $\phi^{*-1}(V(I)) = V(I^e)$.

iii) If J is an ideal of B , then $\phi^*(V(J)) = V(J^c)$.

iv) If ϕ surjective, then ϕ^* is a homeomorphism of Y onto the closed subset $V(\text{Ker}(\phi))$ of X . In particular, $\text{Spec}(A)$ and $\text{Spec}(A/R)$ (where R is the nilradical of A) are naturally homomorphic.

v) If ϕ injective, then $\phi^*(Y)$ is dense in X . More precisely, $\phi^*(Y)$ is dense in $X \Leftrightarrow \text{Ker}(\phi) \subset R$. Here R is the nilpotent radical of A .

vi) Let $\psi : B \rightarrow C$ 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 P , and let K be the field of fraction of A . Let $B = (A/P) \times K$. Define $\phi : A \rightarrow B$ by $\phi(x) = (\bar{x}, x)$, where \bar{x} is the image of x in A/P . Show that ϕ^* is bijective but not a homeomorphism.

Solution: i) For $Q \in \phi^{*-1}(X_f)$, which is $f \notin \phi^{-1}(Q)$, then $\phi(f) \notin Q$, that is, $Q \in Y_{\phi(f)}$, so $\phi^{*-1}(X_f) \subset Y_{\phi(f)}$ and vice versa. Hence $\phi^{*-1}(X_f) = Y_{\phi(f)}$.

ii) If $Q \in \phi^{*-1}(V(I))$, $I \subset \phi^{-1}(Q)$, then $\phi(I) \subset Q$ and $I^e \subset Q$, so $Q \in V(I^e)$, and vice versa. Hence $\phi^{*-1}(V(I)) = V(I^e)$.

iii) If $P \in \phi^*(V(I))$, then we have $P = \phi^{-1}(Q)$ where $Q \supset J$, so $P = \phi^{-1}(Q) \supset \phi^{-1}(J)$. That is, $P \in \overline{V(J^c)}$. Since $V(J^c)$ is closed, we have that $\overline{\phi^*(V(J))} \subset V(J^c)$. To show that $V(J^c) \subset \overline{\phi^*(V(J))}$, it is sufficient to show that $X - \overline{\phi^*(V(J))} \subset X - V(J^c)$. That is, in algebraic word, if $\exists f \notin P$, s.t. $\forall Q \supset J$, $f \in \phi^{-1}(Q)$, then $\phi^{-1}(J)$ is not contained in P . $\forall Q \supset J$, $f \in \phi^{-1}(Q)$

implies $\phi(f) \in Q$, so $\phi(f) \in r(J)$. If $\phi^{-1}(J) \subset P$, then $\phi^{-1}(r(J)) \subset P$. Then $f^n \in P$ and $f \in P$, which is a contradiction!

iv) If ϕ is surjective, then ϕ^* is one-to-one and onto $V(Ker(\phi))$ by the correspondence theorem of ideals. ϕ^* is continuous by i). To prove that ϕ^* is an embedding, it's sufficient to verify that $\phi^*(\phi(I)) = V(I)$.

v) We only prove the last proposition. If $\phi^*(Y)$ is dense, then $V(R) = X = \overline{\phi^*(Y)} = \overline{\phi^*(V(0))} = V(Ker(\phi))$ by iii). We have $R = r(R) = r(Ker(\phi))$, so $Ker(\phi) \subset R$, and vice versa.

vi) $(\psi \circ \phi)^*(P) = (\psi \circ \phi)^{-1}(P) = \phi^{-1}(\psi^{-1}(P)) = \phi^* \circ \psi^*(P)$.

vii) A has two prime ideal, namely, P and (0) , while B has two prime ideals, namely, $Q_1 = \{\bar{0}\} \times K$ and $Q_2 = A/P \times \{0\}$. We see that $\phi^*(Q_1) = P$ and $\phi^*(Q_2) = (0)$, so ϕ^* is bijective. However, $\{(0)\}$ is open but not closed in $Spec(A)$ while $Spec(B)$ is equipped with discrete topology, so ϕ^* is not a homeomorphism.

Exercise 22

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

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

- i) $X = Spec(A)$ 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: Let $\pi : A \rightarrow A_i$ be the i th projection, denote the kernel of π_i by I_i , then $V(I_i)$ is homeomorphic to $Spec(A_i)$ by 21. iv). Since $\cap_{i=1}^n I_i = 0$, we have $\cup_{i=1}^n V(I_i) = V(\cap_{i=1}^n I_i) = V(0) = A$. Since $I_i + I_j = A$ for all $i \neq j$, $V(I_i) \cap V(I_j) = \emptyset$ for all $i \neq j$. This completes the proof.

i) \Rightarrow iii) By assumption, there is two ideals I, J , s.t. $V(I) \cup V(J) = V(I \cap J) = X$ and $V(I) \cap V(J) = V(I + J) = \emptyset$, that is, $I \cap J \subset R$ where R is the nilradical of A and $I + J = A$. Then $\exists a \in I$, s.t. $a \neq 0, 1$, $1 - a \in J$ and $a(1 - a) \in I \cap J$ is a nilpotent. $\exists n$, s.t. $a^n(1 - a)^n = a^{2n} - a^n = 0$. By (1.16), $(a^n) + ((1 - a)^n) = (1)$ since their radical are (a) and $(1 - a)$, respectively. Then $\exists e \in (a^n)$, s.t. $e \neq 0$, $1 - e \in ((1 - a)^n)$, and $e(1 - e) \in (a^n) \cap ((1 - a)^n) = (0)$. Hence e is an idempotent.

iii) \Rightarrow ii) If e is an idempotent $\neq 0, 1$, then so does $1 - e$. Verify that $A \cong eA \times (1 - e)A$. Here, eA is ring with identity e and $(1 - e)A$ is a ring with identity $1 - e$.

ii) \Rightarrow i) This is trivial from the previous claim.

Exercise 23

Let A be a Boolean ring, and let $X = Spec(A)$.

- i) For each $f \in A$, the set X_f 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) X_f is open by definition. To prove that X_f is closed, it's sufficient to show that $V(f)$ is open. If $P \in V(f)$, then $f \in P$ and $1 - f \notin P$. Since $f(1 - f) = 0$ is contained in all prime ideals, $P \in X_{1-f} \subset V(f)$ and done.

ii) It is sufficient to show that $V(f_1) \cap \dots \cap V(f_n) = V(\sum_{i=1}^n (f_i)) = V(f)$ for some $f \in A$. But this is trivial since every finitely generated ideal is principle in Boolean ring (Exercise 11 iii)).

iii) Let $Y \subset X$ be both open and closed. Since Y is open, it is a union of basic open sets X_f . Since Y is closed and X is quasi-compact, Y is quasi-compact. Hence Y is a finite union of basic open sets. By ii), $Y = X_f$ for some $f \in A$.

iv) If P, Q are two distinct prime ideals, then either there is $f \in P$, s.t. $f \notin Q$, or there is $g \in Q$, s.t. $g \notin P$. Suppose the first holds, then $P \in X_{1-f}$ and $Q \in X_f$, and $X_f \cap X_{1-f} = \emptyset$.

Exercise 24

Let L be a lattice, (that is, a partially ordered set L such that every subsets of two elements has superior and inferior element in L), in which the sup and inf of two elements a, b are denoted $a \vee b$ 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: $a \leq b$ means that $a = ab$. Show that, with respect to this ordering, A is a Boolean Lattice. [The sup and inf are given by $a \vee b = a + b + ab$ and $a \wedge b = ab$, and the complement by $a' = 1 - a$.] In the way we obtain a one-to-one correspondence between (isomorphism class of) Boolean rings and (isomorphism class of) Boolean lattices.

Solution: That $A(L)$ is a Boolean ring is trivial and omitted here.

Since $a(a + b + ab) = a^2 + ab + a^2b = a + 2ab = a$, and $b(a + b + ab) = ab + b^2 + ab^2 = b$, $a \leq a + b + ab$ and $b \leq a + b + ab$. If $a \leq c$ and $b \leq c$, then $ac = a$ and $bc = b$ which implies that $(a + b + ab)c = a + b + ab$, so $a + b + ab \leq c$. Hence $a \vee b = a + b + ab$ and the proof of $a \wedge b = ab$ is similar. $a \vee 1 - a = a + 1 - a + a(1 - a) = 1$ and $a \wedge 1 - a = a(1 - a) = 0$ hold. To show that this is a Boolean lattice, we shall verify i), ii) and iii), which is rather trivial and will be omitted here.

To show that this construction is a one-to-one correspondence, we shall show that if from L we construct the ring $A(L)$ and from $A(L)$ we construct the lattice L' , then $L' = L$ and if we start from a Boolean ring A with two steps of construction we are back to A . Still, this is omitted here.

Exercise 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 space.

Solution: By Exercise 24. we can just consider the Boolean lattice induces by a Boolean ring A . Define a map from A to all the open-and-closed subsets of $\text{Spec}(A)$ (which by 23. iv) is a compact Hausdorff space), namely, $a \rightarrow X_a$. This map is order-preserved and bijective.

Exercise 26

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

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

We shall show that μ is a homomorphism of X onto \tilde{X} .

i) Let M be any maximal ideal of $C(X)$, and let $V = V(M)$ be the set of common zeros of the functions in M : that is, $V = \{x \in X : f(x) = 0 \text{ for all } f \in M\}$. Suppose that V is empty. Then for each $x \in X$ there exists $f_x \in M$ 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_1}, \dots, U_{x_n} cover X . Let $f = f_{x_1}^2 + \dots + f_{x_n}^2$. Then f does not vanish at any point of X , hence is a unit in $C(X)$. But this contradicts $f \in M$, hence V is not empty.

Let x be a point of V . Let $M \subset M_x$, hence $M = M_x$ because 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 point of X . Hence $x \neq y \Rightarrow M_x \neq M_y$, and therefore μ is injective.

iii) Let $U_f = \{x \in X : f(x) \neq 0\}$ and let $\tilde{U}_f = \{M \in \tilde{X} : f \notin M\}$. Show that $\mu(U_f) = \tilde{U}_f$. The open sets U_f (resp. \tilde{U}_f) form a basis of the topology of X (resp. \tilde{X}) and therefore μ is a homeomorphism. Thus X can be reconstructed from the ring of functions $C(X)$.

Solution: To use Urysohn's lemma here, we shall prove that every compact Hausdorff space is normal. This is not hard and I want to omit this here.

We shall prove that $\mu(U_f) = \tilde{U}_f$, and that the open sets U_f (resp. \tilde{U}_f) form a basis of the topology of X (resp. \tilde{X}). If $M \in \mu(U_f)$, then $\exists x \in U_f$, s.t. $M = M_x$. By the definition of U_f , $f(x) \neq 0$. By the definition of M_x , $f \notin M_x = M$, so $M \in \tilde{U}_f$. If $M \in \tilde{U}_f$, then $f \notin M$. Since μ is surjective, $\exists x \in \tilde{X}$ s.t. $M_x = M$. By the definition of M_x , $f(x) \neq 0$, so $x \in U_f$.

It's trivial that when $f(x) = 1 \forall x \in X$, $U_f = X$. Suppose that U is a non-empty open set of X , and $x \in U$. Both $\{x\}$ and $X - U$ are closed, and by Urysohn's lemma, we can find a continuous f s.t. $f(x) = 1$ and $f(y) = 0 \forall y \in X - U$. Then $U_f \subset U$. Hence U_f form a basis for X .

Let $Y = \text{Spec}(C(X))$. In fact, $\tilde{U}_f = Y_f \cap \tilde{X}$, so they form a basis for \tilde{X} .

Exercise 27

(Affine algebraic varieties) Let k be an algebraically closed field and let

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

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

Consider the set of all polynomials $g \in k[t_1, \dots, t_n]$ 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 $P(X) = k[t_1, \dots, t_n]/I(X)$ is the ring of 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 ($1 \leq i \leq n$) are the coordinate functions on X : if $x \in X$, then $\xi_i(x)$ is the i th 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 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 $\tilde{X} = \text{Max}(P(X))$, we have defined a mapping $\mu : X \rightarrow \tilde{X}$, namely $x \rightarrow M_x$.

It is easy to show that μ is injective: if $x \neq y$, we must have $x_i \neq y_i$ for some i ($1 \leq i \leq n$), and hence $\xi_i - x_i$ is in M_x but not in M_y , so that $M_x \neq M_y$. What is less obvious (but still true) is that μ is surjective. This is one form of Hilbert's Nullstellensatz.

Solution: IT SEEMS THAT THERE IS NOTHING TO PROVE.

Exercise 28

Let f_1, \dots, f_m be elements of $k[t_1, \dots, t_n]$. They determine a polynomial mapping $\phi : k^n \rightarrow k^m$: 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 $\phi : X \rightarrow Y$ 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 $P(Y) \rightarrow P(X)$, namely $\eta \rightarrow \eta \circ \phi$. Show that in this way we obtain a one-to-one correspondence between regular mappings $X \rightarrow Y$ and the k -algebra homomorphisms $P(Y) \rightarrow P(X)$.

Solution: It's not hard to verify that $\eta \rightarrow \eta \circ \phi$ is indeed a k -algebra homomorphism. If we are given a k -algebra homomorphism, say, $\phi^* : P(Y) \rightarrow P(X)$, then define $\phi = (\phi^*(\xi_1), \dots, \phi^*(\xi_m))$. This is a polynomial mapping from X to k^m and it restricts to a regular mapping from X to Y since $\forall \eta \in I(Y)$, $\eta \circ \phi = \phi^*(\eta(\xi_1, \dots, \xi_m)) = 0$. Since ϕ^* is a k -algebra homomorphism. This is the inverse of the map which sends ϕ to $\eta \rightarrow \eta \circ \phi$.