1 Introduction to Rings

1.1 Rings, Maps, and Ideals

Definition. *A ring is is the triple $(A, +, \cdot)$ such that*

- *$(A, +)$ is an abelian group (call this addition)*
- *$\cdot$ is associative (call this multiplication) and distributes over addition*

We will assume that the ring is commutative $xy = yx$ and that there exists a multiplicative identity element 1.

Note that there is nothing preventing the multiplicative identity 1 from being the same as the additive identity 0. This will imply that

$$x = 1x = 0x = 0$$

In other words $1 = 0$ means that we are dealing with a trivial zero ring.
While the standard image of a ring in our head might be something standard like $\mathbb{Z}$ or $\mathbb{R}$,

in general certain rings may have elements with strange properties. We've seen weird stuff happen in groups, for instance elements of finite order or non-commuting elements. There are similar special elements present in rings that we may discuss.

Definition. *A zero-divisor is an element x such that $xy = 0$ for another element y. A ring (with $1 \neq 0$) with no nonzero zero-divisors is called an integral domain.*

We may think of a zero-divisor as an element that "divides 0," an integral domain such as $\mathbb{Z}$ or $\mathbb{R}$ is generally considered as being nicer to deal with than rings with zero-divisors.

Definition. *A nilpotent element x is an element such that $x^n = 0$ for some $n > 0$.*

Note that a nilpotent element will automatically be a zero-divisor but the converse is not true in general. This definition may remind us of the concept of an order in group theory.

Definition. *A unit is an element x such that $xy = 1$ for some element y.*

While we stipulate additive inverses must exist for a set to be a group, there is no such requirement for rings. In fact, elements that are invertible are rather special (e.g. nonzero elements in $\mathbb{R}$) and thus we have given them a special name. We denote the set of units in a ring A as A^*.

Definition. *A ring homomorphism $f : A \to B$ is a map that satisfies*

$$f(x + yz) = f(x) + f(y)f(z)$$

Note that this will imply $f(0) = 0$ and $f(1) = 1$, so this is really a group homomorphism (it respects the additive group) which also respects multiplication. The compositions of ring homomorphisms will remain a homomorphism.

Definition. *A subring $S \subseteq A$ is a subset that is also a ring and contains* $1 \in A$

A subring must also include both identity elements, thus for any subring we can define the inclusion homomorphism

$$\iota : S \to A \quad \text{or may also be denoted} \quad \iota : S \hookrightarrow A$$

Definition. *An ideal $\mathfrak{a} \subset A$ is an additive subgroup such that*

$$A\mathfrak{a} = \{xa \mid x \in A, a \in \mathfrak{a}\} \subseteq \mathfrak{a}$$

This is the the ring-theoretic version of a normal subgroup, an ideal is a subring that "absorbs" any element multiplied but note that an ideal need not be a subring. Now we can produce quotient rings

$$A/\mathfrak{a} = \{x + \mathfrak{a} \mid x \in A\}$$

There is a canonical map from a ring into its quotient given by

$$\phi : A \to A/\mathfrak{a} \qquad x \mapsto \overline{x} = x + \mathfrak{a}$$

The kernel of any ring homomorphism is automatically an ideal, giving us the theorem

Theorem 1.1. (First Isomorphism Theorem)
Let $f : A \to B$ be a ring homomorphism, then there is an isomorphism

$$A/\text{Ker } f \cong \text{Im } f \subseteq B$$

Another useful isomorphism theorem is

Theorem 1.2. (Fourth Isomorphism Theorem)
There is a one-to-one, order preserving correspondence

$$\{\text{ideals containing } \mathfrak{a}\} \longleftrightarrow \{\text{ideals of } A/\mathfrak{a}\}$$

which can be realized using the canonical map.

The simplest way to create an ideal is to take some random element x from a ring and then make sure it absorbs every other element, in other words we define the ideal

$$(x) = Ax = \{ax \mid a \in A\}$$

This is known as a principal ideal, or ideal generated by one element. In principal (haha), we can create ideals generated by multiple elements in the same way.

Note that if x is a unit, then

$$xy = 1 \in (x) \longrightarrow (x) = A = (1)$$

There are two trivial principal ideals: $(1) = A$ and $(0) = 0$.

Definition. *A field is a ring (with $1 \neq 0$) such that every nonzero element is a unit.*

Fields are our best friend. They behave like we expect them to, their elements do things we want them to, and generally we've been around for most our lives ($\mathbb{R}$). For every (nonzero) element to be a unit, they cannot be zero-divisors. Thus a field will always be an integral domain but the converse is not true (e.g. $\mathbb{Z}$).

In this sense we see that integral domains are rings in which multiplication doesn't do anything wacky (like multiply to zero), giving us an "integer-like" ring. If we impose the addition condition of inverses existing, then we get the most well behaved rings ($\mathbb{Q}$ and $\mathbb{R}$).

Proposition 1.3. Let A be a nontrivial ring, then the following are equivalent

1. A is a field
2. The only ideals in A are the trivial ones (0) and (1)
3. Every homomorphism $A \to B$ is injective if $B \neq 0$

Proof. $1 \to 2$) The zero element will generate (0) while all nonzero elements are units and thus will generate (1).

$2 \to 3$) For a nontrivial homomorphism $\phi : A \to B$, the kernel is an ideal which is not (1). This leaves us only with $\operatorname{Ker} \phi = (0)$ i.e. ϕ is injective.

$3 \to 1$) Suppose $x \in A$ is not a unit, then there is a natural homomorphism

$$\phi : A \to B = A/(x) \neq 0 \qquad a \mapsto a + (x)$$

But ϕ must be injective, so $\operatorname{Ker} \phi = (x) = (0)$ which implies $x = 0$. Thus every nonzero element must be a unit and A is a field. □

Definition. *An ideal $\mathfrak{p} \neq (1)$ is prime if*

$$xy \in \mathfrak{p} \longrightarrow x \in \mathfrak{p} \textit{ or } y \in \mathfrak{p}$$

An ideal $\mathfrak{m} \neq (1)$ is maximal if there is no ideal $\mathfrak{a}$ such that

$$\mathfrak{m} \subset \mathfrak{a} \subset (1)$$

A prime ideal is a generalization of prime numbers to the language of rings, which we will see in an example soon. A maximal ideal is the "biggest" non-trivial ideal, however note that there may be multiple maximal ideals and (cardinality-wise), they might not even be that big.

Proposition 1.4. Prime and maximal ideals can be easily characterized:

- An ideal $\mathfrak{p} \subseteq A$ is prime if and only if $A/\mathfrak{p}$ is an integral domain.
- An ideal $\mathfrak{m} \subseteq A$ is prime if and only if $A/\mathfrak{m}$ is a field.

Proof. If we pass the definition of a prime ideal onto the quotient

$$xy \in \mathfrak{p} \to x \in \mathfrak{p} \text{ or } y \in \mathfrak{p} \quad \Longleftrightarrow \quad xy = 0 \to x = 0 \text{ or } y = 0 \in A/\mathfrak{p}$$

In other words, there are no nonzero zero-divisors and $A/\mathfrak{p}$ is an integral domain.

$\mathfrak{m}$ is maximal if and only if there are no other nontrivial ideals containing it. The ideals of $A/\mathfrak{m}$ are ideals containing $\mathfrak{m}$ so the only possible ones are (0) and (1), which means $A/\mathfrak{m}$ is a field by a previous proposition. □

Since every field is an integral domain (but not vice-versa), we see that every maximal ideal is prime but not the other way around. This also implies that A is an integral domain if and only if (0) is prime.

Prime ideals are incredibly important in algebra (and algebraic geometry as we'll see later), so we are interested making sure they exist. Because maximal ideals are also prime, if we can show that every ring has a maximal ideal then we can ensure that at the very least there is one prime ideal per ring.

Theorem 1.5. Every nontrivial ring $A \neq 0$ has at least one maximal ideal.

Proof. Let Σ be the set of all nontrivial ideals

$$\Sigma = \{\mathfrak{a} \neq (1) \mid \mathfrak{a} \subset A \text{ an ideal}\}$$

Note that it must include (0) so it is nonempty. To apply Zorn's lemma, we must show that every chain in Σ has an upper bound. A chain is a set of ideals $(\mathfrak{a}_\alpha)$ such that for any pair i, j, either $\mathfrak{a}_i \subseteq \mathfrak{a}_j$ or $\mathfrak{a}_j \subseteq \mathfrak{a}_i$. We will construct an upper bound, define

$$\mathfrak{a} = \bigcup_n \mathfrak{a}_n$$

Then $\mathfrak{a} \neq (1)$ because none of the component ideals contain 1. Let $x, y \in \mathfrak{a}$ which means that $x \in \mathfrak{a}_x, y \in \mathfrak{a}_y$. Suppose that $\mathfrak{a}_x \subseteq \mathfrak{a}_y$ without loss of generality, then $x - y \in \mathfrak{a}_y \subseteq \mathfrak{a}$. If $a \in A$ then $ax \in \mathfrak{a}_x \subseteq \mathfrak{a}$ and so it is an ideal. $\mathfrak{a}$ is the upper bound to the chain and so we can apply Zorn's lemma to obtain a maximal element of Σ, which is a maximal ideal. □

Corollary 1.6. If $\mathfrak{a} \neq (1) \subseteq A$ is a nontrivial ideal, then there is a maximal ideal of A which contains it.

Proof. The quotient $A/\mathfrak{a}$ must have some maximal ideal $\overline{\mathfrak{m}}$. By the fourth isomorphism theorem, there is a one-to-one correspondence between ideals of $A/\mathfrak{a}$ and ideals of A containing $\mathfrak{a}$. Thus we conclude that the pullback $\mathfrak{m} = \phi^{-1}(\overline{\mathfrak{m}})$ is a maximal ideal with contains $\mathfrak{a}$. □

This corollary gives us a convenient way to “enlarge” ideals and also more or less tells us why we call these maximal ideals. They also give us a convenient way to describe units.

Corollary 1.7. Every non-unit of A is contained in some maximal ideal.

Proof. If $x \in A$ is not a unit, then $(x) \neq 1$ and is contained within some maximal ideal. □

Example. Let $A = \mathbb{Z}$ where every ideal is of the form (m) for some $m \geq 0$. A ring like this where every ideal is principal is called a principal ideal domain (PID). We see that

$$x \in (m) \iff m \text{ divides } x\text{: } m \mid x$$

Suppose that (p) is a prime ideal, then

$$xy \in (p) \to x \in (p) \text{ or } y \in (p) \iff p \mid xy \text{ only if } p \mid x \text{ or } p \mid y$$

This implies p is a prime number (or 0), hence the name prime ideal. Furthermore (p) is maximal because

$$(m) \subseteq (n) \longrightarrow m \in (n) \to n \mid m$$

and the quotient $\mathbb{Z}/(m)$ is the field of p elements $\mathbb{F}_p$. Note that this does not work for non-prime numbers because the resulting quotient will have zero-divisors.

Now consider $A = k[x_1, \ldots, x_n]$ the polynomial ring over a field k. The ideal (f) is prime if and only if f is a irreducible polynomial in k. This fact forms the basis of algebraic geometry (see later exercises).

We mentioned previously that there is nothing stopping a ring from having multiple maximal ideals. However there is still something special about rings that do have only one.

Definition. *A local ring A is a ring with only one maximal ideal $\mathfrak{m} \subseteq A$. It's residue field is the quotient $k = A/\mathfrak{m}$. A ring with a finite number of maximal ideals is semi-local.*

Proposition 1.8. There are two ways to characterise a local ring:

1. If $\mathfrak{m} \neq (1) \subseteq A$ is an ideal such that every $x \in A \setminus \mathfrak{m}$ is a unit, then A is a local ring with unique maximal ideal $\mathfrak{m}$.

2. If $\mathfrak{m} \subseteq A$ is maximal such that $1 + x$ is a unit for all $x \in \mathfrak{m}$, then A is a local ring.

Proof. 1) Every nontrivial ideal can only contain non-units, so they will be contained in $\mathfrak{m}$ and thus it is the only maximal ideal.

2) Consider some $x \in A \setminus \mathfrak{m}$. Since $\mathfrak{m}$ is maximal, we have

$$(x, \mathfrak{m}) = (1) \longrightarrow xy + t = 1 \quad y \in A, t \in \mathfrak{m}$$

This means $xy = 1 - t \in 1 + \mathfrak{m}$ is a unit and thus so is x. Therefore A is local. □

We'll end our discussion of the different types of ideals by introducing two special ideals. First, the set of nilpotent elements actually form an ideal.

Proposition 1.9. The nilradical $\mathfrak{N}$, the set of all nilpotent elements, is an ideal. The reduction $A/\mathfrak{N}$ will have no nonzero nilpotent elements.

Proof. Let $x, y \in \mathfrak{N}$ with $x^n = y^m = 0$. For any $a \in A$

$$(ax)^n = a^n x^n = 0 \longrightarrow ax \in \mathfrak{N}$$

By the binomial theorem

$$(x+y)^{n+m-1} = \sum c_{r,s} x^r y^s = 0$$

where $r + s = n + m - 1$. So if $r < n$ then $s > m$ and vice-versa so all terms in the sum will vanish $x + y \in \mathfrak{N}$.

Suppose $\overline{x} \in A/\mathfrak{N}$, then

$$\overline{x}^n = 0 \to \overline{x}^n \in \mathfrak{N} \to (x^n)^k = x^{nk} = 0 \to x \in \mathfrak{N} \to \overline{x} = 0$$

Thus there are no nonzero nilpotent elements. □

There is also another way to characterize the nilradical and by extension nilpotent elements in general.

Proposition 1.10. The nilradical is the intersection of all prime ideals.

Proof. If x is nilpotent with $x^n = 0$, then it must be in every prime ideal as

$$x^n = x \cdot x \cdots x = 0 \in \mathfrak{p} \longrightarrow x \in \mathfrak{p} \qquad \forall \mathfrak{p} \text{ prime}$$

$$\therefore \mathfrak{N} \subseteq \bigcap_{\mathfrak{p} \text{ prime}} \mathfrak{p}$$

Conversely suppose x is not nilpotent and define the set

$$\Sigma = \{\mathfrak{a} \subseteq A \mid x^n \notin \mathfrak{a}\ \forall n > 0\} \qquad 0 \in \Sigma$$

If we order Σ by inclusion, then every chain has an upper bound (see proof of existence of maximal ideals) and we can apply Zorn's lemma to get some maximal element $\mathfrak{p}$. Let $y, z \notin \mathfrak{p}$ and consider two new ideals

$$\mathfrak{p} \subset \mathfrak{p} + (y), \mathfrak{p} + (z) \longrightarrow \mathfrak{p} + (y), \mathfrak{p} + (z) \notin \Sigma$$

This means that for some m, n we have $x^m \in \mathfrak{p} + (y), x^n \in \mathfrak{p} + (z)$. Thus

$$x^{m+n} \in \mathfrak{p} + (yz) \longrightarrow \mathfrak{p} + (yz) \notin \Sigma \to yz \notin \mathfrak{p}$$

This shows that $\mathfrak{p}$ is prime and does not contain x, therefore inclusion is equality. □

Recall that maximal ideals are also prime but not vice-versa, thus we may ask if there is something special by taking the intersection to only be between maximal ideals.

Proposition 1.11. The Jacobson radical $\mathfrak{R}$ is the intersection of all maximal ideals and is characterized

$$x \in \mathfrak{R} \iff 1 - xy \in A \text{ is a unit for all } y \in A$$

Proof. Let $x \in \mathfrak{R}$ but suppose $1 - xy$ is not a unit. All non-units belong in some maximal ideal $\mathfrak{m}$ and we know that $\mathfrak{m} \subseteq \mathfrak{R}$ so $xy \in \mathfrak{m}$. But this means $1 \in \mathfrak{m}$ which is impossible so $1 - xy$ must be a unit.

Conversely suppose $x \notin \mathfrak{R}$ which is equivalent to saying that $x \notin \mathfrak{m}$ for some maximal ideal $\mathfrak{m}$. This is also equivalent to saying $(x, \mathfrak{m}) = (1)$, thus $m + xy$ for some $m \in \mathfrak{m}$ and $y \in A$. Therefore $1 - xy \in \mathfrak{m}$ is not a unit. □

1.2 Operations on Ideals

Let $\mathfrak{a}, \mathfrak{b} \subseteq A$ be two ideals, we can define two arithmetic operations on them

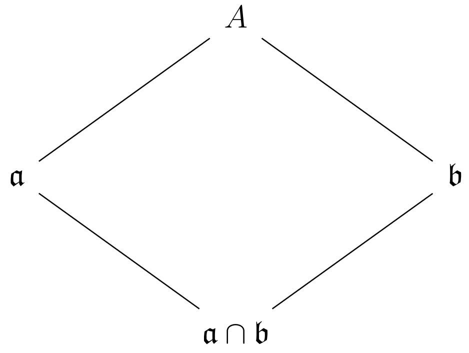
$$\mathfrak{a} + \mathfrak{b} = \{x + y \mid x \in \mathfrak{a}, y \in \mathfrak{b}\}$$
$$\mathfrak{a}\mathfrak{b} = \left\{\sum x_i y_i \mid x_i \in \mathfrak{a}, y_i \in \mathfrak{b}\right\}$$

These definitions and be generalized to include families of ideals. For a (possible infinite) family of ideal $\mathfrak{a}_i$, the sum of those ideals consists of elements $\sum x_i$ where all but finitely many terms $x_i \in \mathfrak{a}_i$ are zero. We can interpret the ideal sum as the smallest ideal which contains all the constituent $\mathfrak{a}_i$.

While infinite sums of ideals exist, we may only take *finite* products of ideals. This way, we can define arbitrary powers of an ideal with the convention that $\mathfrak{a}^0 = (1)$ is trivial. The product of a family of ideals is the ideal generated by elements of the form $\prod x_i$ where $x_i \in \mathfrak{a}_i$. Note that both arithmetic operations are commutative and associative, they also obey the distributive law

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

The intersection of ideals will remain an ideal, which means we can create a lattice for ideals under inclusion as shown below.



Note, however, that the same is not true for unions. Recall that we've used the union of ideals previously in a proof, but that was a special case where the constituent ideals formed a chain

$$\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \cdots \subseteq \mathfrak{a}_n$$

Intersection is clearly commutative and associative, however they do not necessarily distribute over the arithmetic operations. One may check to see that they do distribute in the ring $\mathbb{Z}$, but in general we must impose some additional conditions to get the modular law.

$$\mathfrak{a} \cap (\mathfrak{b} + \mathfrak{c}) = \mathfrak{a} \cap \mathfrak{b} + \mathfrak{a} \cap \mathfrak{c} \qquad \text{only if } \mathfrak{b} \subseteq \mathfrak{a} \text{ or } \mathfrak{c} \subseteq \mathfrak{a}$$

Example. It is always useful to look at examples from the integers when talking about ideals. Recall that $\mathbb{Z}$ is a PID, so consider two ideals $\mathfrak{a} = (m)$ and $\mathfrak{b} = (n)$. Then

$$\mathfrak{a} + \mathfrak{b} = \big(gcd(m, n)\big) \qquad \mathfrak{a}\mathfrak{b} = (mn) \qquad \mathfrak{a} \cap \mathfrak{b} = \big(lcm(m, n)\big)$$

where *gcd* and *lcm* denote the greatest common divisor and least common multiple respectively. There is a relationship between addition, multiplication, and intersections of ideals in $\mathbb{Z}$

$$(\mathfrak{a} + \mathfrak{b})(\mathfrak{a} \cap \mathfrak{b}) = \mathfrak{a}(\mathfrak{a} \cap \mathfrak{b}) + \mathfrak{b}(\mathfrak{a} \cap \mathfrak{b}) = \mathfrak{a}\mathfrak{b}$$

As usual, this relationship is not true in general. It's easy to see that we'll have inclusion on one side since

$$\mathfrak{a}(\mathfrak{a} \cap \mathfrak{b}) + \mathfrak{b}(\mathfrak{a} \cap \mathfrak{b}) \subseteq \mathfrak{a}\mathfrak{b}$$

Note that $\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{a} \cap \mathfrak{b}$ since ideals absorb multiplication, so if $\mathfrak{a} + \mathfrak{b} = (1)$, then

$$(\mathfrak{a} + \mathfrak{b})(\mathfrak{a} \cap \mathfrak{b}) \subseteq \mathfrak{a}\mathfrak{b} \longrightarrow \mathfrak{a} \cap \mathfrak{b} \subseteq \mathfrak{a}\mathfrak{b} \longrightarrow \mathfrak{a} \cap \mathfrak{b} = \mathfrak{a}\mathfrak{b}$$

If we return to the integers for a moment, $\mathfrak{a} + \mathfrak{b} = (1)$ essentially says that $gcd(m, n) = 1$ i.e. they are coprime. We'll lift this notion to ideals in general.

Definition. *Two ideals $\mathfrak{a}, \mathfrak{b}$ are coprime (or comaximal) if $\mathfrak{a} + \mathfrak{b} = (1)$, so that they satisfy*

$$\mathfrak{a} \cap \mathfrak{b} = \mathfrak{a}\mathfrak{b}$$

An easy way to see if two ideals are coprime is if there exists $x \in \mathfrak{a}, y \in \mathfrak{b}$ such that $x + y = 1$.

We take a brief break from our discussion of ideals to discuss products of rings. One may recall that a direct product of groups is just tuples with the group operation applied component-wise. The direct product of rings is exactly the same, if $A_1, \dots, A_n$ are rings, then we define

$$A = \prod_{i=1}^{n} A_i = \{(x_1, \dots, x_n) \mid x_i \in A_i\}$$

A is a commutative ring with identity $(1, \dots, 1)$ and component-wise addition and multiplication. It comes equipped with projection maps

$$p_i : A \to A_i \qquad (x_1, \dots, x_n) \mapsto x_i$$

We can form a product with just one ring by taking the ideals $\mathfrak{a}_1, \dots, \mathfrak{a}_n \subseteq A$ and taking the product of the quotients. This comes equipped with a canonical homomorphism

$$\phi : A \to \prod_{i=1}^{n} A/\mathfrak{a}_i \qquad x \mapsto (x + \mathfrak{a}_1, \dots, x + \mathfrak{a}_n)$$

This map can be used to determine properties of an entire family of ideals at once. We will first generalize the a previous property of coprime ideals before discussing properties of ϕ.

Proposition 1.12.

1. If a family of ideals $\mathfrak{a}_i$ are pairwise coprime, then
$$\prod_{i=1}^{n} \mathfrak{a}_i = \bigcap_{i=1}^{n} \mathfrak{a}_i$$

2. ϕ is surjective if and only if $\mathfrak{a}_i$ are pairwise coprime

3. ϕ is injective if and only if $\bigcap \mathfrak{a}_i = (0)$[1]

Proof. 1) We will proceed by induction on n, the base case $n = 2$ was discussed previously. Suppose the result holds true for some $n > 2$ and let

$$\mathfrak{b} = \prod_{i=1}^{n} \mathfrak{a}_i = \bigcap_{i=1}^{n} \mathfrak{a}_i$$

We know that $\mathfrak{a}_i + \mathfrak{a}_{n+1} = (1)$ for all i, which means there exists $x_i \in \mathfrak{a}_i, y_i \in \mathfrak{a}_{n+1}$ such that $x_i + y_i = 1$ for all i. This means

$$\prod_{i=1}^{n} x_i = \prod_{i=1} (1 - y_i) = 1 + (\text{terms in } \mathfrak{a}_{n+1}) \equiv 1 \mod \mathfrak{a}_{n+1}$$

This means $\mathfrak{a}_{n+1} + \mathfrak{b} = (1)$ and thus

$$\prod_{i=1}^{n+1} \mathfrak{a}_i = \mathfrak{b}\mathfrak{a}_{n+1} = \mathfrak{b} \cap \mathfrak{a}_{n+1} = \bigcap_{i=1}^{n+1} \mathfrak{a}_i$$

completing the induction.

2) Assume ϕ is surjective, we will show that $\mathfrak{a}_1$ and $\mathfrak{a}_2$ are coprime. The same procedure works for every pair i, j. Note that there exists and x such that

$$\phi(x) = (1, 0, \dots, 0) \longrightarrow x \equiv 1 \mod \mathfrak{a}_1 \equiv 0 \mod \mathfrak{a}_2$$

In other words $1 - x \in \mathfrak{a}_1$ and $x \in \mathfrak{a}_2$ so that

$$1 = (1 - x) + x \in \mathfrak{a}_1 + \mathfrak{a}_2$$

[1] This essentially constitutes a proof of the Chinese Remainder Theorem

Conversely, we will show that there exists a $x \in A$ such that $\phi(x) = (1, 0, \dots, 0)$. The same argument applies for the other coordinates. Note that since $\mathfrak{a}_1 + \mathfrak{a}_i = (1)$ for all $i \neq 1$, we can find elements such that

$$x_i + y_i = 1 \qquad x_i \in \mathfrak{a}_1, y_i \in \mathfrak{a}_i$$

Then our desired element $x \in A$ is just

$$x = \prod_{i=2}^{n} y_i = \prod_{i=2}^{n} (1 - x_i) \equiv 1 \mod \mathfrak{a}_1 \equiv 0 \mod \mathfrak{a}_i$$

3) Simply note that Ker $\phi = \bigcap \mathfrak{a}_i$ □

Note that ϕ is an isomorphism if and only if the ideals are pairwise coprime with trivial intersection.

We will conclude this discussion on intersections of ideals with the following useful proposition about prime ideals and inclusions.

Proposition 1.13.

1. Let $\mathfrak{p}_1, \dots, \mathfrak{p}_n$ be prime ideals and $\mathfrak{a}$ an ideal such that $\mathfrak{a} \subseteq \bigcup \mathfrak{p}_i$. Then $\mathfrak{a} \subseteq \mathfrak{p}_i$ for some i.

2. Let $\mathfrak{a}_1, \dots, \mathfrak{a}_n$ be ideals and $\mathfrak{p}$ a prime ideal such that $\bigcap \mathfrak{a}_i \subseteq \mathfrak{p}$. Then $\mathfrak{p}$ contains one of the $\mathfrak{a}$, that is $\mathfrak{a}_i \subseteq \mathfrak{p}$ for some i. In particular if $\mathfrak{p} = \bigcap \mathfrak{a}_i$, then $\mathfrak{p} = \mathfrak{a}_i$ for some i.

Proof. 1) We will proceed by induction on n, in particular by proving the contrapositive

$$\mathfrak{a} \not\subseteq \mathfrak{p}_i \quad \forall i \longrightarrow \mathfrak{a} \not\subseteq \bigcup_{i=1}^{n} \mathfrak{p}_i$$

The base case $n = 1$ is clearly true, suppose now that the result holds for some $n > 1$. Then we can find elements $x_i \in \mathfrak{a}$ such that $x_i \notin \mathfrak{p}_j$ for all $j \neq i$. If $x_i \notin \mathfrak{p}_i$ for some i, then we're done. Otherwise consider the element

$$y = \sum_{i=1}^{n+1} x_1 x_2 \cdots x_{i-1} x_{i+1} \cdots x_{n+1}$$

Clearly we have $y \in \mathfrak{a}$ and $y \notin \mathfrak{p}_i$ for all i and so $\mathfrak{a} \not\subseteq \bigcup \mathfrak{p}_i$, completing induction.

2) We'll prove the contrapositive again. Suppose $p \not\supseteq \mathfrak{a}_i$ for all i, then there exists $x_i \in \mathfrak{a}_i \setminus \mathfrak{p}$ and so

$$y = \prod_{i=1}^{n} x_i \in \prod_{i=1}^{n} \mathfrak{a}_i \subseteq \bigcap_{i=1}^{n} \mathfrak{a}_i$$

Note that since $\mathfrak{p}$ is prime, we have $y \notin \mathfrak{p}$ which means $\mathfrak{p} \not\supseteq \bigcap \mathfrak{a}_i$. If $\mathfrak{p} = \bigcap \mathfrak{a}_i$, then we have $\mathfrak{p} \supseteq \mathfrak{a}_i$ from before and clearly $\mathfrak{p} \subseteq \mathfrak{a}_i$ since $\mathfrak{p} \subseteq \bigcap \mathfrak{a}_i$. Hence $\mathfrak{p} = \mathfrak{a}_i$ for some i. □

The first proposition states that if an ideal is contained in the union of some family of prime ideals then it is actually contained in just one prime ideal. This tells us that we may always restrict our focus down to a single prime ideal.

The second proposition considers the opposite scenario. If a prime ideal contains the intersection of some family of (not necessarily prime) ideals, then it must contain one of the constituent ideals entirely.

Definition. *Let $\mathfrak{a}, \mathfrak{b}$ be ideals, their ideal quotient is the ideal*

$$(\mathfrak{a} : \mathfrak{b}) = \{x \in A \mid x\mathfrak{b} \subseteq \mathfrak{a}\} = \{x \in A \mid xy \in \mathfrak{a} \quad \forall y \in \mathfrak{b}\}$$

We interpret this as a quotient because $\mathfrak{c}\mathfrak{b} \subseteq \mathfrak{a}$ if and only if $\mathfrak{c} \subseteq (\mathfrak{a} : \mathfrak{b})$. In particular, the annihilator is a quotient of the zero ideal

$$Ann(\mathfrak{b}) = (0 : \mathfrak{b}) = \{x \in A \mid x\mathfrak{b} = 0\}$$

This allows us to define the set of zero divisors as

$$D = \bigcup_{x \neq 0} Ann(x)$$

For a principal ideal (x), we will simply write $(\mathfrak{a} : x)$ for convenience instead of $(\mathfrak{a} : (x))$.

Proposition 1.14. Properties of the ideal quotient

1. The original ideal is always contained in the quotient

$$\mathfrak{a} \subseteq (\mathfrak{a} : \mathfrak{b})$$

2. The quotient behaves as we expect a quotient to behave like

$$(\mathfrak{a} : \mathfrak{b})\mathfrak{b} \subseteq \mathfrak{a}$$

3. It is commutative in a sense

$$((\mathfrak{a} : \mathfrak{b}) : \mathfrak{c}) = (\mathfrak{a} : \mathfrak{b}\mathfrak{c}) = ((\mathfrak{a} : \mathfrak{c}) : \mathfrak{b})$$

4. It obeys intersections in the first argument

$$\left(\bigcap_i \mathfrak{a}_i : \mathfrak{b}\right) = \bigcap_i (\mathfrak{a}_i : \mathfrak{b})$$

5. Sums in the second argument turn into intersections

$$\left(\mathfrak{a} : \sum_i \mathfrak{b}_i\right) = \bigcap_i (\mathfrak{a} : \mathfrak{b}_i)$$

Proof. 1) Consider $x \in \mathfrak{a}$, by definition we have

$$x\mathfrak{b} \subseteq \mathfrak{a} \longrightarrow x \in (\mathfrak{a} : \mathfrak{b})$$

2) For any $x \in (\mathfrak{a} : \mathfrak{b}), y \in \mathfrak{b}$. Since $x\mathfrak{b} \subseteq \mathfrak{a}$,

$$xy \in \mathfrak{a} \longrightarrow (\mathfrak{a} : \mathfrak{b})\mathfrak{b} \subseteq \mathfrak{a}$$

3) Note that since A is commutative

$$\begin{aligned}((\mathfrak{a} : \mathfrak{b}) : \mathfrak{c}) &= \{x \in A \mid x\mathfrak{c}\mathfrak{b} \subseteq \mathfrak{a}\} \\ &= \{x \in A \mid x\mathfrak{b}\mathfrak{c} \subseteq \mathfrak{a}\} \\ &= ((\mathfrak{a} : \mathfrak{c}) : \mathfrak{b}) = (\mathfrak{a} : \mathfrak{b}\mathfrak{c})\end{aligned}$$

4) For simplicity, consider the intersection of just two ideals

$$x \in (\mathfrak{a}_1 \cap \mathfrak{a}_2 : \mathfrak{b}) \iff x\mathfrak{b} \subseteq \mathfrak{a}_1 \cap \mathfrak{a}_2 \iff x\mathfrak{b} \subseteq \mathfrak{a}_1, \mathfrak{a}_2 \iff x \in (\mathfrak{a}_1 : \mathfrak{b}) \cap (\mathfrak{a}_2 : \mathfrak{b})$$

5) For simplicity, consider the sum of just two ideals

$$x \in (\mathfrak{a} : \mathfrak{b}_1 + \mathfrak{b}_2) \iff x\mathfrak{b}_1 + x\mathfrak{b}_2 \subseteq \mathfrak{a} \iff x\mathfrak{b}_1, x\mathfrak{b}_2 \subseteq \mathfrak{a} \iff x \in (\mathfrak{a} : \mathfrak{b}_1) \cap (\mathfrak{a} : \mathfrak{b}_2)$$

□

Definition. *For an ideal $\mathfrak{a}$, the radical of $\mathfrak{a}$ is*

$$r(\mathfrak{a}) = \sqrt{\mathfrak{a}} = \{x \in A \mid x^n \in \mathfrak{a} \textit{ for some } n > 0\}$$

Note that this is an ideal because it is the pullback of the nilradical under the quotient map

$$r(\mathfrak{a}) = \phi^{-1}(\mathfrak{N}_{A/\mathfrak{a}})$$

Proposition 1.15. Properties of the ideal radical

1. The ideal radical always returns a "larger" ideal

$$\mathfrak{a} \subseteq r(\mathfrak{a})$$

2. Radical is invariant under itself

$$r(r(\mathfrak{a})) = r(\mathfrak{a})$$

3. It obeys products and intersections (recall coprime ideals)

$$r(\mathfrak{a}\mathfrak{b}) = r(\mathfrak{a} \cap \mathfrak{b}) = r(\mathfrak{a}) \cap r(\mathfrak{b})$$

4. The radical of an ideal is trivial if and only if the ideal is trivial

$$r(\mathfrak{a}) = (1) \iff \mathfrak{a} = (1)$$

5. The addition formula
$$r(\mathfrak{a}+\mathfrak{b}) = r(r(\mathfrak{a})+r(\mathfrak{b}))$$

6. If $\mathfrak{p}$ is prime, $r(\mathfrak{p}^n) = \mathfrak{p}$ for all $n > 0$

Proof. 1) Trivial from definition

2) This is almost also trivial

$$x \in r(r(\mathfrak{a})) \iff x^n \in r(a) \iff (x^n)^m = x^{nm} \in \mathfrak{a} \iff x \in r(\mathfrak{a})$$

3) Note that $\mathfrak{ab} \subseteq \mathfrak{a} \cap \mathfrak{b}$, so we already know that $r(\mathfrak{ab}) \subseteq r(\mathfrak{a} \cap \mathfrak{b})$. For the other direction, note that we can simply multiply

$$x \in r(\mathfrak{a} \cap \mathfrak{b}) \iff x^n \in \mathfrak{a}, \mathfrak{b} \longrightarrow x^{2n} \in \mathfrak{ab} \iff x \in r(\mathfrak{ab})$$

The second inequality is trivial

$$x \in r(\mathfrak{a} \cap \mathfrak{b}) \iff x^n \in \mathfrak{a}, \mathfrak{b} \iff x \in r(\mathfrak{a}), r(\mathfrak{b}) \iff x \in r(\mathfrak{a}) \cap r(\mathfrak{b})$$

4) This is pretty simple to show as the identity 1 will be contained within any trivial ideal

$$1 \in r(\mathfrak{a}) \iff 1^n = 1 \in \mathfrak{a}$$

5) One direction is trivial, for the other one

$$x \in r(r(\mathfrak{a}) + r(\mathfrak{b})) \iff x^n = y + z$$

where $y^r \in \mathfrak{a}, z^s \in \mathfrak{b}$. We can expand

$$x^{n(r+s)} = (y+z)^{r+s} = \sum y^\alpha z^\beta$$

where $\alpha + \beta = r + s$ so that for every term, either $\alpha > r$ or $\beta > s$. Thus this will be a sum of terms from $\mathfrak{a}$ and $\mathfrak{b}$.

6) We will use (4) from above

$$r(\mathfrak{p}^n) = r(\mathfrak{p} \cap \cdots \mathfrak{p}) = r(\mathfrak{p})$$

Now note that
$$x \in r(\mathfrak{p}) \iff x^n \in \mathfrak{p} \iff x \in \mathfrak{p}$$

□

The last property seems to suggest some kind of connection between radicals and prime ideals. In fact there is another way to characterize the radical.

Proposition 1.16. $r(\mathfrak{a})$ is the intersection of all prime ideals which contain $\mathfrak{a}$

Proof. We know that the nilradical is the intersection of all prime ideals, which means $r(\mathfrak{a})$ is the intersection of all prime ideals of $A/\mathfrak{a}$ i.e. prime ideals which contain $\mathfrak{a}$. □

Note that we may define radicals of arbitrary sets, not just of radicals, but the result need not be an ideal. The radical also carries over the property of "coprime-ness."

Proposition 1.17. If $r(\mathfrak{a}), r(\mathfrak{b})$ are coprime, then so are $\mathfrak{a}, \mathfrak{b}$.

Proof. This is by simple calculation using various properties

$$r(\mathfrak{a}+\mathfrak{b}) = r(r(\mathfrak{a}) + r(\mathfrak{b})) = r(1) = (1) \longrightarrow \mathfrak{a}+\mathfrak{b} = (1)$$

□

Example. We'll return to our good friend the integers $\mathbb{Z}$. Consider two ideals $\mathfrak{a} = (m)$ and $\mathfrak{b} = (n)$. Then the quotient and radical are

$$(\mathfrak{a} : \mathfrak{b}) = \left(\frac{m}{gcd(m,n)}\right) \qquad r(\mathfrak{a}) = (p_1 p_2 \cdots p_r) = \bigcap_{i=1}^{r} (p_i)$$

where $p_1, \dots, p_r$ are the prime factors of m.

The final ideal operations we'll discuss the the extension and contraction of an ideal under arbitrary ring maps.

Definition. *Let $f : A \to B$ be a ring homomorphism with $\mathfrak{a} \subseteq A, \mathfrak{b} \subseteq B$ ideals. The extension of $\mathfrak{a}$ is*

$$\mathfrak{a}^e = Bf(\mathfrak{a}) = \left\{\sum y_i f(x_i) \mid x_i \in \mathfrak{a}, y_i \in B\right\}$$

This is the ideal generated by the image of $\mathfrak{a}$, as the image itself isn't necessarily an ideal. The contraction of $\mathfrak{b}$ is

$$\mathfrak{b}^c = f^{-1}(\mathfrak{b})$$

Note that unlike the extension, the contraction requires no additional sums as the preimage of an ideal will always be an ideal. The contraction of a prime ideal will remain prime but this is not necessarily true for the extension.

Proposition 1.18. Let $f : A \to B$ be a ring homomorphism and $\mathfrak{a} \subseteq A, \mathfrak{b} \subseteq B$ ideals, then

1. $\mathfrak{a} \subseteq \mathfrak{a}^{ec}, \mathfrak{b} \supseteq \mathfrak{b}^{ce}$
2. Nested operations are invariant in a sense

$$\mathfrak{a}^e = \mathfrak{a}^{ece} \qquad \mathfrak{b}^c = \mathfrak{b}^{cec}$$

3. Let C denote the set of contracted ideals and E the set of extended ideals. Then they can be characterized

$$C = \{\mathfrak{a} \mid \mathfrak{a}^{ec} = \mathfrak{a}\} \qquad E = \{\mathfrak{b} \mid \mathfrak{b}^{cec} = \mathfrak{b}\}$$

and there is a bijection between the two given by

$$\mathfrak{a} \mapsto \mathfrak{a}^e \qquad \mathfrak{b}^c \mapsfrom \mathfrak{b}$$

Proof. 1) Trivial

2) Note that if $\mathfrak{a}_1 \subseteq \mathfrak{a}_2$, then

$$\mathfrak{a}_1^e = Bf(\mathfrak{a}_1) \subseteq Bf(\mathfrak{a}_2) = \mathfrak{a}_2^e$$

and likewise for contractions. In order words, they are order preserving so from (1) we get

$$\mathfrak{a}^e \subseteq \mathfrak{a}^{ece} \qquad \mathfrak{b}^c \supseteq \mathfrak{b}^{cec}$$

But $\mathfrak{a}^e \subseteq B$, so we can contract and extend to get the other direction. A similar process follows for $\mathfrak{b}$.

3) One side of the characterizations can be seen with

$$\mathfrak{a} \in C \longrightarrow \mathfrak{a} = \mathfrak{b}^c = \mathfrak{b}^{cec} = \mathfrak{a}^{ec} \qquad \mathfrak{b} \in E \longrightarrow \mathfrak{b} = \mathfrak{a}^e = \mathfrak{a}^{ece} = \mathfrak{b}^{ece}$$

The other direction is trivial. The bijection is established with (2). □

We will end this section by discussing how extensions and contractions interact with the five operations discussed previously.

Proposition 1.19. Let $\mathfrak{a}_1, \mathfrak{a}_2 \subseteq A$ and $\mathfrak{b}_1, \mathfrak{b}_2 \subseteq B$ be ideals, then

1. E is closed under sum

$$(\mathfrak{a}_1 + \mathfrak{a}_2)^e = \mathfrak{a}_1^e + \mathfrak{a}_2^e \qquad (\mathfrak{b}_1 + \mathfrak{b}_2)^c \supseteq \mathfrak{b}_1^c + \mathfrak{b}_2^c$$

2. C is closed under intersection

$$(\mathfrak{a}_1 \cap \mathfrak{a}_2)^e \subseteq \mathfrak{a}_1^e \cap \mathfrak{a}_2^e \qquad (\mathfrak{b}_1 \cap \mathfrak{b}_2)^c = \mathfrak{b}_1^c \cap \mathfrak{b}_2^c$$

3. E is closed under product

$$(\mathfrak{a}_1\mathfrak{a}_2)^e = \mathfrak{a}_1^e\mathfrak{a}_2^e \qquad (\mathfrak{b}_1\mathfrak{b}_2)^c \supseteq \mathfrak{b}_1^c\mathfrak{b}_2^c$$

4. C is closed under quotient

$$(\mathfrak{a}_1 : \mathfrak{a}_2)^e \subseteq (\mathfrak{a}_1^e : \mathfrak{a}_2^e) \qquad (\mathfrak{b}_1 : \mathfrak{b}_2)^c = (\mathfrak{b}_1^c : \mathfrak{b}_2^c)$$

5. C is closed under radical

$$r(\mathfrak{a})^e \subseteq r(\mathfrak{a}^e) \qquad r(\mathfrak{b})^c = r(\mathfrak{b}^c)$$

Proof. 1) The proof for E comes directly from definition

$$(\mathfrak{a}_1 + \mathfrak{a}_2)^e = Bf(\mathfrak{a}_1 + \mathfrak{a}_2) = Bf(\mathfrak{a}_1) + Bf(\mathfrak{a}_2) = \mathfrak{a}_1^e + \mathfrak{a}_2^e$$

For C, $x \in \mathfrak{b}_1^c + \mathfrak{b}_2^c$ if there exists $y_1 \in \mathfrak{b}_1, y_2 \in \mathfrak{b}_2$ such that

$$x = f^{-1}(y_1) + f^{-1}(y_2) \longrightarrow f(x) = y_1 + y_2 \longrightarrow x = f^{-1}(y_1 + y_2)$$

$$\therefore x \in (\mathfrak{b}_1 + \mathfrak{b}_2)^c$$

If we try to do this proof in reverse, then we see that $y_1 + y_2$ has a preimage, but there is no guarantee that y_1, y_2 by themselves have a preimage. Hence there is no equality.

2) The case for E is trivial, C is a well known property of preimages.

$$x \in (\mathfrak{b}_1 \cap \mathfrak{b}_2)^c \iff f(x) \in \mathfrak{b}_1 \cap \mathfrak{b}_2 \iff f(x) \in \mathfrak{b}_1, \mathfrak{b}_2 \iff x \in (\mathfrak{b}_1)^c \cap (\mathfrak{b}_2)^c$$

3) Proceed in exactly the same way as the proof for (1), note that $BB = B$

4) For E, if $y \in (\mathfrak{a}_1 : \mathfrak{a}_2)^e$, then there exists $x \in (\mathfrak{a}_1 : \mathfrak{a}_2)$ such that $f(x) = y$ which means

$$x\mathfrak{a}_2 \subseteq \mathfrak{a}_1 \longrightarrow f(x)Bf(\mathfrak{a}_2) \subseteq Bf(\mathfrak{a}_1) \longrightarrow y\mathfrak{a}_2^e \subseteq \mathfrak{a}_1^e \longrightarrow y \in (\mathfrak{a}_1^e : \mathfrak{a}_2^e)$$

We do not have equality because we cannot be sure that y has a preimage when we go the other way. But for C,

$$x \in (\mathfrak{b}_1 : \mathfrak{b}_2)^c \iff f(x)\mathfrak{b}_1 \subseteq \mathfrak{b}_2 \iff xf^{-1}(\mathfrak{b}_1) \subseteq f^{-1}(\mathfrak{b}_2) \iff x \in (\mathfrak{b}_1^c : \mathfrak{b}_2^c)$$

5) For E, if $y \in r(\mathfrak{a})^e$ then there exists a $x \in r(\mathfrak{a})$, that is

$$x^n \in \mathfrak{a} \longrightarrow f(x^n) = y^n \in f(\mathfrak{a}) \subseteq Bf(\mathfrak{a}) \longrightarrow y \in r(\mathfrak{a}^e)$$

As we've seen before, we cannot go backward because y^n having a preimage does not necessarily guarantee y has one. For C,

$$x \in r(\mathfrak{b})^c \iff f(x)^n = f(x^n) \in \mathfrak{b} \iff x^n \in f^{-1}(\mathfrak{b}) \iff x \in r(\mathfrak{b}^c)$$

Hence E is closed under addition and multiplication while C is closed under the remaining three ideal operations. □

1.3 Additional Exercises

Exercise 1. We know that the set of nilpotent elements form an ideal, the nilradical $\mathfrak{N}$. This ideal must be contained within some maximal ideal and thus is a subset of the Jacobson radical $\mathfrak{R}$. We can then use a proposition from the text

$$x \in \mathfrak{R} \longrightarrow 1 - (-1)x = 1 + x \in A \text{ is a unit}$$

Alternatively, suppose $x^n = 0$ and note

$$(1+x)(1 - x + x^2 - x^3 + \cdot - x^{2n-1}) = 1 - x^{2n} = 1$$

If u is a unit, then

$$u^{-1}(u+x) = 1 + u^{-1}x$$

is also a unit since $u^{-1}x$ is nilpotent. In particular

$$u^{-1}(1+u^{-1}x)^{-1}(u+x) = 1$$

so that the sum of a unit and a nilpotent element is a unit.

1.3.1 Polynomial Rings

Exercise 2. Let $f = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \in A[x]$
i) Suppose f is a unit, that is there exists some

$$g = b_0 + b_1x + \cdots + b_mx^m$$

such that $fg = 1$. Suppose we expand the product a bit

$$fg = a_0b_0 + (a_0b_1 + a_1b_0)x + \cdots + (a_{n-1}b_m + a_nb_{m-1})x^{n+m-1} + a_nb_mx^{n+m} = 1$$

We see right away that $a_0b_0 = 1$ (i.e. a_0 is a unit) and that the remaining coefficients must be zero. Using the hint in the book, we will prove

$$a_n^{r+1}b_{m-r} = 0 \qquad 0 \leq r < m$$

Clearly $a_nb_m = 0$ for f to be a unit, let's consider the next case

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

We can start to see how induction will work here, suppose that the proposition holds for all $r < k$. In other words, we have considered all coefficients down to x^{n+m-k}. The next one of interest will be

$$\begin{aligned} 0 &= \sum_{i=0}^{k+1} a_{n-k-1+i}b_{m-i} \\ &= \sum_{i=0}^{k+1} a_n^{k+1}a_{n-k-1+i}b_{m-i} \\ &= a_n^{k+2}b_{m-k-1} \end{aligned}$$

It is implied that the sum will not include negative indices, this completes the induction.

Now there are two possibilities

1. All the $b_i = 0$ and thus $g = 0$, which is impossible
2. a_n is nilpotent, i.e. $a_n^r = 0$ for at least one of the r's

We proved in exercise 1 that the sum (and thus also difference) of a unit and a nilpotent element remains a unit, so we can repeat the proposition on

$$f - a_n x^n = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1}$$

to show that a_{n-1} is nilpotent. Continuing in this way, we prove that a_0 is a unit and $a_1, \ldots, a_n$ are nilpotent.

Conversely if a_0 is a unit and $a_1, \ldots, a_n$ are nilpotent, then $a_i x^i \in A[x]$ is nilpotent for $i \neq 0$. Then a simple application of exercise 1 will show that f is a unit since the sum of nilpotent elements remains nilpotent.

ii) Suppose f is nilpotent and that $f^n = 0$, then

$$f^n = a_0^n + \cdots = 0$$

and we can conclude a_0 is nilpotent. But a_0 can also be thought of as a (constant) polynomial in $A[x]$ so $f - a_0$ is also nilpotent.

$$(f - a_0)^m = a_1^m x^m + \cdots = 0$$

and thus a_1 is also nilpotent. Continuing in this fashion shows that all the a_i are nilpotent.

The converse is almost trivial to prove by noting $a_i x_i$ is nilpotent if a_i is nilpotent and the sum of nilpotent elements remains nilpotent ($\mathfrak{N}$ is an ideal). This exercise implies

$$\mathfrak{N}_{A[x]} = \mathfrak{N}_A[x]$$

iii) Following the guidance in the book, suppose f is a zero-divisor and

$$g = b_0 + b_1 x + \cdots + b_m x^m$$

is the smallest degree polynomial such that

$$fg = a_0 b_0 + (a_0 b_1 + a_1 b_0)x + \cdots + a_n b_m x^{n+m} = 0$$

We see that $a_n b_m = 0$ which means that $a_n g$ is a polynomial of degree less than m. But $(a_n g)f = 0$, a contradiction to the minimality of g so we must have $a_n g = 0$. Note that

$$(f - a_n x^n)g = fg - (a_n g)x^n = 0$$

so that

$$f - a_n x^n = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1}$$

is still a zero-divisor. Suppose that

$$a_{n-r}g = 0 \qquad \forall r \leq k$$

Then we can proceed as before

$$f - \sum_{r=0}^{k} a_{n-r}x^{n-r} = a_0 + a_1 x + \cdots + a_{n-k-1}x^{n-k-1}$$

is a zero-divisor, so $a_{n-k-1}g = 0$ and thus $a_{n-r}g = 0$ for all $0 \leq r \leq n$ by induction. This means that either $f = 0$, $g = 0$, or one of the b_i annihilates all of a_i. In that case, it would be the a we are looking for.

The converse is trivial, if $af = 0$ then since $a \in A[x]$ is a constant polynomial we have f is a zero-divisor.

iv) Consider $f, g \in A[x]$ as we have previously. Suppose fg is primitive, that is

$$(a_0 b_0, a_1 b_0 + a_0 b_1, \ldots, a_{n-1}b_m + a_n b_{m-1}, a_n b_m) = (1) = A$$

This is equivalent to saying that there is no maximal ideal $\mathfrak{m}$ which contains every coefficient. In other words, let $k = A/\mathfrak{m}$ be a field for any maximal ideal $\mathfrak{m}$. Then if fg is primitive

$$\overline{fg} = 0 \in k[x] \Longleftrightarrow \overline{f} = \overline{g} = 0 \in k[x]$$

since $k[x]$ is an integral domain. This is equivalent to saying that

$$fg \in \mathfrak{m}[x] \Longleftrightarrow f, g \in \mathfrak{m}[x]$$

In other words fg is primitive if and only if f, g, are both primitive.

Exercise 3. Let $f \in A[x_1, \ldots, x_r]$ be a polynomial in several variables. We'll adopt multi-index notation for sums

$$\alpha = (i_1, i_2, \ldots, i_r) \qquad x^\alpha = x_1^{i_1} x_2^{i_2} \cdots x_r^{i_r}$$

so that f can be written in summation notation as

$$f = \sum a_\alpha x^\alpha$$

i) If f is a unit, then a_0 is a unit and all other a_α are nilpotent. By induction, suppose this holds for r indeterminates and consider

$$f \in A[x_1, \ldots, x_r, y] \qquad f = \sum_{\alpha, n} a_{\alpha,n} x^\alpha y^n$$

We can rewrite this polynomial as

$$f \in A[y] \qquad f = \sum b_n y^n \quad b_n = \sum_{\alpha} a_{\alpha,n} x^\alpha \in A[x_1, \ldots, x_r]$$

By the previous exercise, this means that f is a unit if and only if $b_0 = a_{0,0}$ is a unit and all others are nilpotent.

ii) f is nilpotent only when all a_α are nilpotent. Using the same induction as before we see that f is nilpotent only if all the b_n are nilpotent. This is the case if and only if all the $a_{\alpha,n}$ are nilpotent by the inductive hypothesis. This finishes the proof of the previous statement as well.

iii) The $\Longleftarrow$ direction is trivial, for the other direction we induct as before. Tracing through the proof for the one indeterminate case, suppose by induction that g is the smallest degree polynomial which annihilates f ($f, g \in A[x_1, \ldots, x_r]$), then there is a constant $a \in A$ which also annihilates f. Using (2iii), if $f \in A[x_1, \ldots, x_r, y]$ is a zero divisor, then there exists some "constant" $g \in A[x_1, \ldots, x_r]$ which annihilates f.

This means that $gb_n = 0$ for all b_n, where we also have $b_n \in A[x_1, \ldots, x_r]$. Thus by the inductive hypothesis, there is some constant $a_n \in A$ which will annihilate each of the b_n and thus the product of all a_n (if they are different) will annihilate f.

iv) The same statement as before applies and the proof still works.

Exercise 4. We just need to show that the nilradical contains the Jacobson radical. Suppose $f \in \mathfrak{R}$, then $1 - fg$ is a unit for all $g \in A[x]$. Take $g = x$

$$1 - fg = 1 - a_0x - a_1x^2 - \cdots - a_nx^{n+1}$$

For this to be a unit, all the a_i must be nilpotent which is the same as saying f is nilpotent.

Exercise 5. Let $f \in A[[x]]$ be a formal power series

$$f = \sum_{n=0}^{\infty} a_nx^n$$

i) If f is a unit such that $fg = 1$, then

$$fg = a_0b_0 + (\deg \geq 1 \text{ terms}) = 1$$

so $a_0b_0 = 1$ and a_0 must be a unit.

Conversely suppose $a_0b_0 = 1$, we can construct $g = f^{-1}$ by taking

$$\begin{aligned} b_1 &= -b_0(a_0b_0) \\ b_2 &= -b_0(a_2b_0 + a_1b_1) \\ b_3 &= -b_0(a_3b_0 + a_2b_1 + a_1b_2) \\ \vdots b_n &= -b_0\sum_{i=0}^{n} a_{n-i}b_i \end{aligned}$$

ii) The proof in exercise (2ii) still works to show that if f is nilpotent, then all a_n is nilpotent. The converse is not true, suppose each coefficient a_n is nilpotent with $a_n^n = 0$ and $a_0 = 0$. Then $f^m \neq 0$ for any choice of m because there will always exists some coefficient a_n such that $n \nmid m$ so that $a_n^m x^m \neq 0$.

iii) $f \in \mathfrak{R}(A[[x]])$ if and only if $1 - fg$ is a unit for all $g \in A[[x]]$.

$$1 - fg = (1 - a_0 b_0) + (\text{degree} > 1 \text{ terms})$$

so by (i), this is equivalent to saying $1 - a_0 b_0$ is a unit for all $b_0 \in A$, i.e. $b_0 \in \mathfrak{R}(A)$.

iv) Note that by (iii), $x \in \mathfrak{R}(A[[x]])$ so that for any maximal ideal $\mathfrak{m} \subseteq A[[x]]$ we will have $(x) \subseteq \mathfrak{m}$. This means

$$\mathfrak{m}/(x) = \mathfrak{m}^c \subseteq A \longrightarrow \mathfrak{m} = (\mathfrak{m}^c, x)$$

Using the third isomorphism theorem, we can show that the contraction is maximal

$$A[[x]]/\mathfrak{m} \cong \frac{A[[x]]/(x)}{\mathfrak{m}/(x)} \cong A/\mathfrak{m}^c$$

v) If $\mathfrak{p}^c \subseteq A$ is prime, then $\mathfrak{p} = (\mathfrak{p}^c, x) \subseteq A[[x]]$ is also prime from the same argument above. In particular, given any prime ideal $\mathfrak{p}^c \subseteq A$, we can construct a prime ideal of $A[[x]]$ who's contraction is $\mathfrak{p}^c$.

1.3.2 More on Ideals

Exercise 6. Since every maximal ideal is prime, we already know that $\mathfrak{N} \subseteq \mathfrak{R}$. Now take some $x \notin \mathfrak{N}$. This generates an ideal $(x) \nsubseteq \mathfrak{N}$ so that there exists some idempotent e, that is $xy = e$ and

$$e^2 = e \longrightarrow e(1 - e) = 0$$

Since $1 - e$ is a zero divisor, it cannot be a unit, which means $e = xy \notin \mathfrak{R}$. $\mathfrak{R}$ is an ideal, so we must have $x \notin \mathfrak{R}$, establishing equality.

Exercise 7. Let $\mathfrak{p} \subseteq A$ be a prime ideal and $x \notin \mathfrak{p}$ so that $\overline{x} \neq 0 \in A/\mathfrak{p}$, which is an integral domain. We know that there exists some $n > 1$ such that

$$x^n = x \in A \longrightarrow \overline{x}(1 - \overline{x}^{n-1}) = 0 \in A/\mathfrak{p}$$

But zero divisors cannot exist in $A/\mathfrak{p}$ so either $\overline{x} = 0$, a contradiction, or

$$1 - \overline{x}^{n-1} = 0 \longleftrightarrow \overline{x}^{n-1} = \overline{x} \cdot \overline{x}^{n-2} = 1$$

Thus every nonzero element in $A/\mathfrak{p}$ is a unit so it is a field and $\mathfrak{p}$ is maximal.

Exercise 8. Let $(\mathfrak{p}_\alpha)$ be a chain of prime ideals so that for any pair i, j we have $\mathfrak{p}_i \subseteq \mathfrak{p}_j$ or $\mathfrak{p}_j \subseteq \mathfrak{p}_i$. Define

$$\mathfrak{p} = \bigcap \mathfrak{p}_i$$

The intersection of ideals is still an ideal and now we just need to show it's prime. Note

$$xy \in \mathfrak{p}, x \notin \mathfrak{p} \longrightarrow xy \in \mathfrak{p}_i, x \notin \mathfrak{p}_i \ \forall i \longrightarrow y \in \mathfrak{p}_i \ \forall i \longrightarrow y \in \mathfrak{p}$$

The same argument works for $y \notin \mathfrak{p}$ so $\mathfrak{p}$ is prime and the lower bound to the chain. Thus by Zorn's lemma, there is a minimal element under inclusion to the set of all prime ideals.

Exercise 9. If $r(\mathfrak{a}) = \mathfrak{a}$, then by definition

$$r(\mathfrak{a}) = \bigcap_{\mathfrak{p} \supseteq \mathfrak{a}} \mathfrak{p} = \mathfrak{a}$$

Conversely, if $\mathfrak{a}$ is the intersection of prime ideals, then

$$r(\mathfrak{a}) = r\left(\bigcap \mathfrak{p}\right) = \bigcap r(\mathfrak{p}) = \bigcap \mathfrak{p} = \mathfrak{a}$$

Exercise 10. 1 → 2) If A only has one prime ideal, it must also be the only maximal ideal. Since $\mathfrak{N}$ is the intersection of prime ideals, this means the nilradical is maximal so that every non-unit is nilpotent.

2 → 3) If every element is either a unit or nilpotent, then the reduction $A/\mathfrak{N}$ will contain only units, i.e. it is a field.

3 → 1) If the reduction is a field, $\mathfrak{N}$ is maximal. But the nilradical is contained within every prime ideal, which would be a contradiction, so the nilradical is the only prime ideal.

Exercise 11. i) In a Boolean ring,

$$(x+1)^2 = x^2 + 2x + 1 = x + 2x + 1 \longrightarrow 2x = 0$$

ii) If $\mathfrak{p}$ is prime, then $A/\mathfrak{p}$ is an integral domain. For any element

$$\overline{x}(\overline{x} - 1) = 0 \longrightarrow \overline{x} = 0, 1$$

So there can only be two elements in $A/\mathfrak{p}$ ($\cong \mathbb{F}_2$), it is a field, and $\mathfrak{p}$ is maximal.

iii) Suppose we have a finitely generated ideal

$$\mathfrak{a} = (x_1, x_2, \ldots, x_n) = Ax_1 + Ax_2 + \cdots + Ax_n$$

By induction suppose that $\mathfrak{a}$ is principal with $\mathfrak{a} = (x)$. Then

$$(x_1, \ldots, x_n, y) = (x, y) = (x + y - xy) = (z)$$

because we can write each generator as

$$xz = x^2 + xy - x^2y = x^2 = x \qquad yz = xy + y^2 - xy^2 = y^2 = y$$

so we see that every finitely generated ideal must be principal.

Exercise 12. Let A be local with $\mathfrak{m}$ its unique maximal ideal. Then if some $\overline{x} \in A/\mathfrak{m}$ is idempotent

$$\overline{x}^2 = \overline{x} \longrightarrow \overline{x}(\overline{x} - 1) = 0 \longrightarrow x = 0, 1$$

since there cannot be any zero divisors in a field. This means any idempotent must either be 1 or contained within the maximal ideal so suppose $x \in \mathfrak{m}$. Zero divisors cannot be units, so $1 - x$ must be contained within some maximal ideal, but there's only one maximal ideal. Furthermore $1 - x \in \mathfrak{m}$ would mean that

$$(1 - x) + x = 1 \in \mathfrak{m} \longrightarrow \mathfrak{m} = (1)$$

which is a contradiction, so we must have $x = 0$ if $x \in \mathfrak{m}$ or $x = 1$ otherwise.

1.3.3 Constructing an Algebraic Closure

Exercise 13. If $\mathfrak{a} = (1)$, then there exists $a_f \in K$ (all but finitely many are zero) such that

$$1 = \sum_{f \in \Sigma} a_f f(x_f)$$

But this is clearly impossible since the $f(x_f)$ are independent in that they are in different variables. Let $\mathfrak{m}$ be the maximal ideal which contains $\mathfrak{a}$ and $K_1 = A/\mathfrak{m}$. Then since $K \not\subseteq \mathfrak{m}$, K_1 is a field extension of K in which every f has one root since quotienting by $\mathfrak{m}$ is the same as identifying $f(x_f) = 0$ for all f.

Repeating this construction, K_2 is a field extension in which f has two roots. Let

$$L = \bigcup_{i=1}^{\infty} K_i$$

so f splits completely into linear factors in L. Let $\overline{K}$ be the elements of L which are algebraic in K (they are the root of some $f \in K[x]$), then $\overline{K}$ is an algebraic closure of K.

Exercise 14. Let Σ be the set of ideals whose elements are all zero divisors and order it by inclusion. Suppose we have a chain $(\mathfrak{a}_\alpha)$ and define

$$\mathfrak{a} = \bigcup \mathfrak{a}_\alpha$$

Then $\mathfrak{a}$ is clearly an ideal (see similar proof for existence of maximal ideals) and only consists of zero divisors. So it is an upper bound for the chain and thus Zorn's lemma guarantees the existence of maximal elements in Σ.

Let $\mathfrak{a}$ be some maximal element and $xy \in \mathfrak{a}$. Then xy is a zero divisor and so x, y must both be zero divisors as well. If this is not the case then

$$(xy)z = (xz)y = x(yz) = 0$$

will imply that $z = 0$, which is a contradictions since xy is still a zero divisor. If $x \notin \mathfrak{a}$, then

$$\mathfrak{a} \subseteq (\mathfrak{a}, x) \in \Sigma$$

which is a contradiction since $\mathfrak{a}$ was maximal. Thus $x \in \mathfrak{a}$ and $\mathfrak{a}$ is prime.[2]

[2] In fact, both x and y must be in $\mathfrak{a}$ using the same argument.

1.3.4 Prime Spectrum and Topology

Exercise 15. Let $X = \operatorname{Spec} A$ be the set of all prime ideals of the ring A. For any subset $E \subseteq A$, define

$$V(E) = \{\mathfrak{p} \in X \mid E \subseteq \mathfrak{p}\}$$

We will prove that $V(E)$ form the closed sets for a topology on X, the Zariski topology.

i) If $\mathfrak{a}$ is the ideal generated by E, then $V(E) = V(\mathfrak{a})$ is trivial. Note that $\mathfrak{a} \subseteq r(\mathfrak{a})$, so $V(r(\mathfrak{a})) \subseteq V(\mathfrak{a})$. For the remaining direction

$$\mathfrak{p} \in V(\mathfrak{a}) \iff \mathfrak{a} \subseteq \mathfrak{p} \longrightarrow r(\mathfrak{a}) \subseteq r(\mathfrak{p}) = \mathfrak{p} \iff \mathfrak{p} \in V(r(\mathfrak{a}))$$

ii) Every ideal contains 0 and no nontrivial ideal can contain 1, thus

$$V(0) = X \qquad V(1) = \varnothing$$

iii) Note the following properties

$$\mathfrak{p} \in \left(\bigcup E_i\right) \iff E_i \subseteq \mathfrak{p}\ \forall i \iff \mathfrak{p} \in V(E_i)\ \forall i \iff \mathfrak{p} \in \bigcap V(E_i)$$

iv) Since $\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{a} \cap \mathfrak{b}$, we immediately know that

$$V(\mathfrak{a}) \cup V(\mathfrak{b}), V(\mathfrak{a} \cap \mathfrak{b}) \subseteq V(\mathfrak{a}\mathfrak{b})$$

For the other direction, suppose that $\mathfrak{p} \in V(\mathfrak{a}\mathfrak{b})$ so that $\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{p}$. Since $\mathfrak{p}$ is prime, either $\mathfrak{a}$ or $\mathfrak{b}$ must be contained within $\mathfrak{p}$. For instance if $\mathfrak{b} \not\subseteq \mathfrak{p}$, then for every $xy \in \mathfrak{a}\mathfrak{b}$ we must have $x \in \mathfrak{p}$ i.e. $\mathfrak{a} \subseteq \mathfrak{p}$. Thus $\mathfrak{p} \in V(\mathfrak{a}) \cup V(\mathfrak{b})$, which also means $\mathfrak{p} \in V(\mathfrak{a} \cap \mathfrak{b})$.

Exercise 16. For the first two, note that

$$\operatorname{Spec} \mathbb{Z} = \{p \in \mathbb{Z} \mid p \text{ prime}\} \cup \{0\} \qquad \operatorname{Spec} \mathbb{R} = \{0\}$$

In a polynomial ring, a prime ideal is generated by irreducible polynomials, for instance linear terms $x - \alpha$. By the fundamental theorem of algebra, all polynomials split into linear terms in $\mathbb{C}$, thus

$$\operatorname{Spec} \mathbb{C}[x] = \{x - z_0 \mid z_0 \in \mathbb{C}\} \cup \{0\}$$

So there is a correspondence between points of Spec $\mathbb{C}[x]$ and points on the complex plane, with a “fat” point at 0 (since (x) is prime, but so is (0)).

In $\mathbb{R}[x]$, all odd polynomials split into a linear term (in $\mathbb{R}[x]$) times a even power term which may be irreducible. These terms will always split into terms of the form $(x - z_0)(x + z_0)$ for some $z_0 \in \mathbb{C}$, so

$$\operatorname{Spec} \mathbb{R}[x] = \{x - x_0 \mid x_0 \in \mathbb{R}\} \cup \left\{x - |z_0|^2 \mid z_0 \in \mathbb{C}\right\} \cup \{0\}$$

Due to the presence of the absolute value, this can be imagined as the real plane plus (the positive) half of the complex plane. Again, we can interpret the origin as being “fat.”

Clearly Spec $\mathbb{Z}[x]$ will also contain Spec z. The remaining primes consist of those generated by irreducible polynomials f as well as ideals of the form (p, f).[3]

[3] There is a very nice picture by Mumford which is frequently passed around on the internet.

Exercise 17. Let X_f denote the complement of $V(f)$ in X, we will prove that they form a basis of open sets for the Zariski topology. The X_f are called the basic open sets of X.

First we will show that X_f indeed form a basis for X. Recall that a basis for a topological space X is a set $\mathcal{B}$ such that every $x \in X$ is contained within some basis element. Furthermore if $x \in B_1, B_2$, then there exists a third basis element B_3 such that $x \in B_3 \subseteq B_1 \cap B_2$.

Let $\mathfrak{p} \in \operatorname{Spec} A$. Since $\mathfrak{p} \neq (1)$, there exists some $f \in A \setminus \mathfrak{p}$. Then $\mathfrak{p} \in X_f$, satisfying the first properties of a basis. Now suppose $\mathfrak{p} \in X_f \cap X_g$, the we will prove in (i) that there exists a third basis element such that

$$\mathfrak{p} \in X_{fg} \subseteq X_f \cap X_g$$

Thus X_f is a basis of open sets for the Zariski topology on X.

i) This follows from definition

$$\mathfrak{p} \in X_f \cap X_g \iff f, g \notin \mathfrak{p} \iff fg \notin \mathfrak{p} \iff \mathfrak{p} \in X_{fg}$$

ii) $X_f = \varnothing$ if and only if f is in every prime ideal i.e. $f \in \mathfrak{N}$.

iii) Every non-unit is in some maximal (thus prime) ideal, so f is a unit if and only if it is in no prime ideal i.e. $X_f = X$.

iv) $X_f = X_g$ if and only if $V(f) = V(g)$. Recall that this is equivalent to $V((f)) = V((g))$. From this, we get two inclusions

$$\forall \mathfrak{p} \in V\big((f)\big); \quad (g) \subseteq \mathfrak{p} \qquad\qquad \forall \mathfrak{p} \in V\big((g)\big); \quad (f) \subseteq \mathfrak{p}$$

The ideal radical can be defined as the intersection of prime ideals, so

$$(g) \subseteq \bigcap_{(f)\subseteq \mathfrak{p}} \mathfrak{p} = r\big((f)\big) \qquad (f) \subseteq \bigcap_{(g)\subseteq \mathfrak{p}} \mathfrak{p} = r\big((g)\big)$$

$$\therefore r\big((f)\big) = r\big((g)\big)$$

v) Suppose X_{f_i} $(i \in I)$ is an (infinite) open covering of X. Then

$$X = X_1 = \bigcup_{i\in I} X_{f_i} = \bigcup_{i \in I} V(f_i)^c = V\left(\{f_i\}_{i\in I}\right)^c = X_{\{f_i\}}$$

Using (iv), this means that $r((f_i)_{i\in I}) = r(1) = (1)$ or, in other words, the f_i generate the unit ideal. Thus there exists a_i such that

$$\sum_{i\in I} a_i f_i = 1$$

But for this sum to converge, all but finitely many a_i must be zero. In other words, there is a finite subset J such that

$$\sum_{i\in J} a_i f_i = 1$$

Thus $(X_{f_i})_{i\in J}$ is a finite subcover and so X is quasi-compact.[4]

[4] Atiyah-Macdonald uses quasi-compact, this convention refers to compact Hausdorff spaces as "compact" while only compact spaces are "quasi-compact."

vi) Let X_{f_i} $(i \in I)$ cover X_f, so

$$X_f \subseteq X_{\{f_i\}} \iff V(\{f_i\}) \subseteq V(f) \iff f \in r((f_i))$$

So there exists some integer $m > 1$ and $a_i \in A$ such that

$$f^m = \sum_{i \in I} a_i f_i = \sum_{i \in J} a_i f_i$$

and thus we can reduce it to a finite sum. Then $(X_{f_i})_{i \in J}$ is a finite cover of X_f and it is quasi-compact.

vii) We just proved that every X_f is quasi-compact and we know that a finite union of quasi-compact sets remains compact.[5] Thus a finite union of X_f is open and quasi-compact.

Conversely, suppose some open subset $A \subseteq X$ is quasi-compact. Then there exists some finite subcover (since X as a whole is quasi-compact) X_{f_i} of A. So clearly we can write A as a finite union of basic open sets.

Exercise 18. When talking about points in X, we will simply denote then with a single letter $x, y \in X$. When talking about then as prime ideals however, we will denote them as $\mathfrak{p}_x, \mathfrak{p}_y \subseteq A$. Of course they are logically still the same thing.

i) A point $x \in \operatorname{Spec} A$ is closed if and only if $V(\mathfrak{a}) = x$ for some $\mathfrak{a}$. In other words, the only prime ideal which contains $\mathfrak{a}$ is $\mathfrak{p}_x$, so x is closed if and only if $\mathfrak{a} = \mathfrak{p}_x$ is maximal.

ii) The closure of a set is the smallest closed subset which contains it. Thus we can compute $\overline{\{x\}}$ by taking the intersection of all closed subsets $V(\mathfrak{a})$ which contain $\mathfrak{p}_x$.

$$\overline{\{x\}} = \bigcap_{x \in V(\mathfrak{a})} V(\mathfrak{a}) = V\left(\bigcup_{\mathfrak{a} \subseteq \mathfrak{p}_x} \mathfrak{a}\right) = V(\mathfrak{p}_x)$$

iii) Using what we just proved

$$y \in \overline{\{x\}} \iff \mathfrak{p}_y \in V(\mathfrak{p}_x) \iff \mathfrak{p}_x \subseteq \mathfrak{p}_y$$

iv) Let $x, y \in X$ be two distinct points and suppose that every neighborhood of x contains y and vice versa. Then

$$x \in V(\mathfrak{p}_y) = \overline{\{x\}} \iff \mathfrak{p}_y \subseteq \mathfrak{p}_x \qquad y \in V(\mathfrak{p}_x) = \overline{\{x\}} \iff \mathfrak{p}_x \subseteq \mathfrak{p}_y$$

which means $\mathfrak{p}_x = \mathfrak{p}_y$, a contradiction. Thus X is T_0.[6]

Exercise 19. Spec A is irreducible if and only if $X_f \cap X_g = X_{fg} \neq \varnothing$ when $X_f, X_g \neq \varnothing$. This is equivalent to saying that if $f, g \notin \mathfrak{N}$ then $fg \notin \mathfrak{N}$ i.e. Spec A is irreducible if and only if $\mathfrak{N}$ is prime.

[5] Standard topology exercise, simply union the finite subcovers

[6] This is because x is a limit point of $\{y\}$ and vice versa. An equivalent definition of closure is that it is the union of a set and its limit points.

Exercise 20. Let X be any topological space

i) Suppose $Y \subseteq X$ is irreducible and let $U, V \subseteq \overline{Y}$ be open subsets of its closure. Then $U \cap Y$ and $V \cap Y$ are nonempty open subsets of Y and since Y is irreducible

$$(U \cap Y) \cap (V \cap Y) = (U \cap V) \cap Y \neq \varnothing \longrightarrow U \cap V \neq \varnothing$$

Thus the closure is also irreducible

ii) Let Σ denote the set of irreducible subspaces of X and let (Y_α) be a chain in Σ. Define

$$Y = \bigcup Y_\alpha$$

and suppose $U, V \subseteq Y$ are nonempty open sets. Then there must exists indices i, j such that

$$U \cap Y_i \neq \varnothing \qquad V \cap Y_j \neq \varnothing$$

Since (Y_α), we either have $Y_i \subseteq Y_j$ or $Y_j \subseteq Y_i$. Without loss of generality, suppose it is is the former. Then since X_i is irreducible

$$(U \cap Y_i) \cap (V \cap Y_j) = (U \cap V) \cap Y_i \neq \varnothing \longrightarrow U \cap V \neq \varnothing$$

Thus Y is irreducible and an upper bound to the chain. By Zorn's lemma, we conclude that Σ has maximal elements and so every irreducible subspace will be contained in one. These are called the irreducible components of the space X.

iii) If Y is a maximal irreducible subspace, then $Y \subseteq \overline{Y}$ is also irreducible. Thus we must have $Y = \overline{Y}$ i.e. Y is closed. Since singleton sets are obviously irreducible, the irreducible components cover X.

Suppose X is Hausdorff and $x, y \in X$. Then by definition there exists two open sets U_x, U_y such that

$$x \in U_x, y \in U_y \qquad U_x \cap U_y = \varnothing$$

i.e. x, y have disjoint neighborhoods. Thus an irreducible Hausdorff space cannot have more than one point. Since any subspace of a Hausdorff space remains Hausdorff, we see that the irreducible components are the singletons.

iv) We just proved that the irreducible components are closed, so we will only look at the closed sets $V(E)$. Suppose $V(\mathfrak{a})$ is irreducible, then if $X_f, X_g \subseteq V(\mathfrak{a})$ are nonempty ($f, g \notin \mathfrak{a}$ and f, g not nilpotent), we must have

$$\varnothing \neq X_f \cap X_g \subseteq V(\mathfrak{a}) \iff fg \notin \mathfrak{a} \qquad (fg \text{ not nilpotent})$$

In other words, $\mathfrak{a}$ must be prime.

Now suppose $V(\mathfrak{p})$ is a maximal irreducible subspace. This means that there does not exist a prime ideal $\mathfrak{q}$ such that $V(\mathfrak{p}) \subseteq V(\mathfrak{q})$ or, equivalently, $\mathfrak{q} \subseteq \mathfrak{p}$. In other words, $V(\mathfrak{p})$ is maximal only if $\mathfrak{p}$ is minimal under inclusion.

Exercise 21. Let A, B be rings and $f : A \to B$ be a ring homomorphism. Then there is an induced map on the topological spaces $X = \text{Spec } A, Y = \text{Spec } B$ given by

$$\phi^* : Y \to X \qquad \phi^*(y) = \phi^{-1}(\mathfrak{q}_y)$$

i) Let $f \in A$, then we get the series of implications

$$y \in \phi^{*-1}(X_f) \iff f \notin \phi^*(y) = \phi^{-1}(\mathfrak{q}_y) \iff \phi(f) \notin \mathfrak{q}_y \iff y \in Y_{\phi(f)}$$

ii) Suppose $\mathfrak{a} \subseteq A$ is an ideal, then

$$y \in \phi^{*-1}(v(\mathfrak{a})) \iff \mathfrak{a} \subseteq \phi^{-1}(\mathfrak{q}_y) \iff \phi(\mathfrak{a}) \subseteq \mathfrak{a}^e \subseteq \mathfrak{q}_y \iff y \in V(\mathfrak{a}^e)$$

The last implication follows because if an ideal contains $\phi(\mathfrak{a})$ then it must also contain $A\phi(\mathfrak{a}) = \mathfrak{a}^e$.

iii) The closure of $\phi^*(V(\mathfrak{b}))$ is the intersection of all closed sets $V(\mathfrak{a})$ which contain it. In other words, every ideal in $\phi^*(V(\mathfrak{b}))$ must contain $\mathfrak{a}$ so

$$\mathfrak{a} \subseteq \bigcap \phi^*(V(\mathfrak{b}))$$

We can rewrite this using various rules

$$\bigcap \phi^*(V(\mathfrak{b})) = \bigcap_{\mathfrak{b}\subseteq\mathfrak{q}} \mathfrak{q}^c = \left(\bigcap_{\mathfrak{b}\subseteq\mathfrak{q}} \mathfrak{q}\right)^c = r(\mathfrak{b})^c = r(\mathfrak{b}^c)$$

Thus we see that

$$\overline{\phi^*(V(\mathfrak{b}))} = \bigcap_{\mathfrak{a}\subseteq r(\mathfrak{b}^c)} V(\mathfrak{a}) = V\left(\bigcup_{\mathfrak{a}\subseteq\mathfrak{r}(\mathfrak{b}^c)} \mathfrak{a}\right) = V(r(\mathfrak{b}^c)) = V(\mathfrak{b}^c)$$

iv) For ϕ^* to be a homeomorphism, we must show that it and its inverse are continuous. Note that

$$\phi^{*-1}(V(\text{Ker } \phi)) = V((\text{Ker } \phi)^e) = V(0) = Y$$

This, in conjunction with (i), shows that $\phi^* : Y \to V(\text{Ker } \phi)$ is continuous. Consider a closed set $V(\mathfrak{b}) \subseteq Y$. Since ϕ is surjective, the image $\phi(\mathfrak{p}_x)$ is prime for any $x \in X$. Thus

$$x \in \phi^*(V(\mathfrak{b})) \iff \phi(\mathfrak{p}_x) \in V(\mathfrak{b}) \iff \mathfrak{b} \subseteq \phi(\mathfrak{p}_x) \iff \mathfrak{b}^c \subseteq \mathfrak{p}_x \iff \mathfrak{p}_x \in V(\mathfrak{b}^c)$$

Thus the image of a closed set is still closed and so ϕ^{*-1} is continuous. Therefore ϕ^* is a homeomorphism.

v) A subset $Y \subseteq X$ is dense if and only if $\overline{Y} = X$. Using (iii), we can rewrite

$$\overline{\phi^*(Y)} = \overline{\phi^*(V_Y(0))} = V_X((0)^c) = V_X(\text{Ker } \phi)$$

So $\phi^*(Y)$ is dense if and only if $V(\text{Ker } \phi) = X$, which is the same as saying every prime ideal contains Ker ϕ. Since $\mathfrak{N}$ is the intersection of all prime ideals, $\phi^*(Y)$ is dense if and only if Ker $\phi \subseteq \mathfrak{N}$. Clearly $0 \subseteq \mathfrak{N}$, so the first statement follows.

vi) Let $\psi : B \to C$ be another ring homomorphism and $Z = \text{Spec } C$, then

$$(\psi \circ \phi)^*(z) = (\psi \circ \phi)^{-1}(\mathfrak{p}_z) = (\phi^{-1} \circ \psi^{-1})(\mathfrak{p}_z) = (\phi^* \circ \psi^*)(z)$$

vii) Let A be an integral domain so that (0) is prime. If $\mathfrak{p}$ is the only nonzero prime ideal

$$X = \text{Spec } A = \{(0), \mathfrak{p}\}$$

If we mod out $\mathfrak{p}$, then the only prime ideals of $A/\mathfrak{p}$ are the trivial ones. This is also true for a field, so for $B = A/\mathfrak{p} \times K$

$$Y = \text{Spec } B = \{(0) \times K, A/\mathfrak{p} \times (0)\} = \{\mathfrak{q}_1, \mathfrak{q}_2\}$$

Thus we see that $\phi^* : Y \to X$ is bijective

$$\phi^*(\mathfrak{q}_1) = \mathfrak{p} \qquad \phi^*(\mathfrak{q}_2) = (0)$$

However, in Y both $\mathfrak{q}_1$ and $\mathfrak{q}_2$ are maximal so they are closed. But (0) is not closed in X because it is clearly not maximal in A. So ϕ^* does not map closed sets to closed sets, thus it cannot be a homeomorphism.

Exercise 22. It's easy to see that Spec A is the disjoint union of subspaces.

$$\text{Spec } A = \left\{\prod \mathfrak{p}_i \mid \mathfrak{p}_i \subseteq A_i \text{ prime}\right\} = \bigsqcup(\ldots, 0, \mathfrak{p}_i, 0, \ldots) = \bigsqcup X_i$$

Each of the X_i are homeomorphic to Spec A_i under the standard projection map π_i. The extra remark comes from the fact that Spec A_i is both open and closed as shown from previous exercises.

Now consider some ring A. We will show the following are equivalent:

1. $X = \text{Spec } A$ is disconnected (can be written as the disjoint union of two non-empty open sets)
2. A is the product of two nonzero rings $A \cong A_1 \times A_2$
3. A contains a nontrivial ($\neq 0, 1$) idempotent

1 → 2) Suppose X is disconnected and is the disjoint union of two non-empty open sets X_1, X_2. Let their complements be $V(\mathfrak{a}), V(\mathfrak{b})$, then using various properties

$$X = X_1 \cup X_2 = V(\mathfrak{a}) \cup V(\mathfrak{b}) = V(\mathfrak{a} \cap \mathfrak{b}) = V(0)$$

$$0 = X_1 \cap X_2 = V(\mathfrak{a}) \cap V(\mathfrak{b}) = V(\mathfrak{a} \cup \mathfrak{b}) = V(\mathfrak{a}\mathfrak{b}) = V(1)$$

Consider the canonical homomorphism

$$\phi : A \to A/\mathfrak{a} \times A/\mathfrak{b} \qquad x \mapsto (x + \mathfrak{a}, x + \mathfrak{b})$$

ϕ is surjective if $\mathfrak{a}, \mathfrak{b}$ are coprime and injective if their intersection is the trivial ideal. Note

$$X = V(0) \subseteq V(\mathfrak{a} \cap \mathfrak{b}) \iff \mathfrak{a} \cap \mathfrak{b} \subseteq r(0) = (0) \to \mathfrak{a} \cap \mathfrak{b} = (0)$$

$$V(\mathfrak{a} \cup \mathfrak{b}) \subseteq V(1) \iff r(1) = (1) \subseteq \mathfrak{a} \cup \mathfrak{b} \to \mathfrak{a} \cup \mathfrak{b} = 1$$

Thus $(1) = \mathfrak{a} \cup \mathfrak{b} \subseteq \mathfrak{a} + \mathfrak{b}$, so they are coprime $\mathfrak{a} + \mathfrak{b} = (1)$ and ϕ gives an isomorphism of the form $A \cong A_1 \times A_2$.

$2 \to 3$) The element $(1, 0)$ is nonzero and idempotent.[7]

$3 \to 1$) Let $e \neq 0, 1$ be idempotent. Then

$$e(1-e) = 0 \in \mathfrak{p} \iff e \text{ or } 1-e \in \mathfrak{p}$$

This is true for every prime ideal so

$$X_e \cup X_{1-e} = X \qquad X_e \cap X_{1-e} = X_{e(1-e)} = X_0 = \varnothing$$

Thus X is a disjoint union of open sets

$$X = X_e \sqcup X_{1-e}$$

1.3.5 Boolean Lattices

Exercise 23. Recall that a Boolean ring A is such that for all $x \in A$, $x^2 = x$. Let $X = \operatorname{Spec} A$.

i) By definition X_f is open, but note that for all prime $\mathfrak{p}$

$$f(1-f) = 0 \in \mathfrak{p}$$

So if $f \in \mathfrak{p}$, then $1 - f \notin \mathfrak{p}$ and vice versa. This implies

$$V(1-f) = X_f$$

and thus X_f is also closed.

ii) Without loss of generality, consider just two open sets.

$$\mathfrak{p} \in X_f \cup X_g \iff f \text{ or } g \notin \mathfrak{p} \iff 1-f \text{ or } 1-g \in \mathfrak{p} \iff (1-f)(1-g) \in \mathfrak{p}$$

$$\therefore 1 - (1-f)(1-g) \notin \mathfrak{p} \iff \mathfrak{p} \in X_{1-(1-f)(1-g)}$$

iii) Let $Y \subseteq X$ be both open and closed. Since it's open, we can write

$$Y = \bigcup_{i \in I} X_{f_i}$$

But since Y is also closed and X is compact, closed subsets of a compact space are also compact so Y is compact and there must exist a finite subcover (I is finite). Thus we can use the earlier proposition to rewrite $Y = X_f$ and so the basic open sets are the only subsets which are both open and closed.

iv) Let $x, y \in X$ be two distinct points ($\mathfrak{p}_x \neq \mathfrak{p}_y$) and take $f \in \mathfrak{p}_y \setminus \mathfrak{p}_x$. Then $x \in X_f$ ($f \notin \mathfrak{p}_x$) and $y \in X_{1-f}$ since if $f \in \mathfrak{p}_y$, then it cannot contain $1 - f$, otherwise $1 \in \mathfrak{p}_y$ which is impossible. Note that

$$X_f \cap X_{1-f} = X_{f(1-f)} = X_0 = 0$$

so they are disjoint neighborhoods for x, y and thus X is Hausdorff. The spectrum of any ring is quasi-compact, so X is compact (quasi-compact Hausdorff).[8]

[7] The converse comes from the Peirce decomposition: If $e \in A$ is idempotent, then $A = eA + (1-e)A$.

[8] See note above about terminology used.

Exercise 24. Let L be a lattice and denote

$$a \vee b = \sup(a,b) \qquad a \wedge b = \inf(a,b)$$

L is a Boolean lattice (or Boolean algebra) if:

1. L has a least and greatest element, denoted 0 and 1 respectively
2. $\vee$ and $\wedge$ distribute over each other
3. For all $a \in L$, there is a unique complement $a' \in L$ such that

$$a \vee a' = 1 \qquad a \wedge a' = 0$$

Let L be a Boolean lattice and define addition and multiplication by

$$a + b = (a \wedge b') \vee (a' \wedge b) \qquad ab = a \wedge b$$

We will show that these operations make L into a Boolean ring. First note that

$$a \vee 0 = a \qquad a \vee 1 = 1 \qquad a \wedge 0 = 0 \qquad a \wedge 1 = a$$

$\vee, \wedge$ are commutative and associative, it is easy to see that $+, \cdot$ will be commutative and $\cdot$ associative. It is less clear that $+$ is associative, first we will prove De Morgan's law:

$$(a \wedge b)' = a' \vee b' \qquad (a \vee b)' = a' \wedge b'$$

We'll show that our expression satisfies the properties of complements

$$\begin{aligned}
(a \wedge b) \wedge (a' \vee b') &= [(a \wedge b) \wedge a'] \vee [(a \wedge b) \wedge b'] \\
&= (0 \wedge b) \wedge (a \wedge 0) = 0 \wedge 0 = 0 \\
(a \wedge b) \vee (a' \vee b') &= [(a \wedge b) \vee a'] \vee [(a \wedge b) \vee b'] \\
&= [(a \vee a') \wedge (b \vee a')] \vee [(a \vee b') \wedge (b \vee b')] \\
&= [1 \wedge (b \vee a')] \vee [(a \vee b') \wedge 1] \\
&= (b \vee a') \vee (a \vee b') \\
&= (a \vee a') \vee (b \vee b') = 1 \vee 1 = 1
\end{aligned}$$

The same proof applies to $a \vee b$, we just flip the arrows.

To show that $(L, +)$ is a group requires showing that inverses exists and $+$ is associative.[9]

$$\begin{aligned}
a + (b + c) &= a[(b' \vee c)(b \vee c')] \vee a'[bc' \vee b'c] \\
&= a(bc \vee b'c') \vee a'bc' \vee a'b'c \\
&= abc \vee ab'c' \vee a'bc' \vee a'b'c
\end{aligned}$$

[9] From here on, I will write ab instead of $a \wedge b$ for convenience.

Note that the end result is totally symmetric; any permutation of the arguments results in the same answer. This in addition with commutativity implies that + is associative

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

It is easy to see that $-a = a$ since

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

In fact this proves that $2a = 0$, which is something we showed must be true in a Boolean ring. Since + is commutative and associative, this proves $(L, +)$ is an abelian group.

To see that $(L, +, \cdot)$ is a ring, we need + and $\cdot$ to distribute over each other.

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

Thus these two operations make L into a ring.

We will also verify that 0 and 1 are the additive and multiplicative identities respectively.

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

Finally, we show that L is a Boolean ring

$$a^2 = a \wedge a = \inf(a, a) = a$$

Conversely, suppose we define an ordering on a Boolean ring A using

$$a \leq b \iff a = ab$$

First, we show that this ordering is valid.

1. Reflexive:
$$a = a^2 \rightarrow a \leq a$$

2. Anti-symmetric: If $a \leq b$ and $b \leq a$
$$a = ab \text{ and } b = ab \rightarrow a = b$$

3. Transitive: If $a \leq b$ and $b \leq c$
$$a = ab = abc = ac \rightarrow a \leq c$$

The sup and inf can be directly computed (as per the book)

$$a \wedge b = ab \qquad a \vee b = a + b + ab$$

We will verify that these are indeed the greatest lower bound and least upper bound.

$$ab = a(ab) = b(ab) \iff ab \leq a, b$$

$$a = a(a+b+ab), b = b(a+b+ab) \iff a, b \leq a+b+ab$$

Now suppose $d \leq a, b \leq c$ so that

$$d = ad = bd \qquad a = ac, b = bc$$

Then we see that these are indeed the greatest and least respectively as

$$(a \wedge b)d = abd = a(ad) = d \iff d \leq a \wedge b$$

$$(a \vee b)c = ac + bc + abc = a + b + ab = (a \vee b) \iff a \vee b \leq c$$

Thus this gives us a valid lattice, we now check the conditions for a Boolean lattice.

0 and 1 are still the least and greatest elements respectively.

$$0 \wedge a = 0 \cdot a = 0 \qquad 1 \vee a = a + 1 + a = 2a + 1 = 1$$

Next, we see that $\wedge$ and $\vee$ distribute

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

Finally, $a' = 1 - a$ is the (unique) complement for any $a \in A$

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

So this ordering turns any Boolean ring into a Boolean lattice.

Exercise 25. The previous problem gives us a one-to-one correspondence

$$\{\text{Boolean Rings } A\} \iff \{\text{Boolean Lattices } L\}$$

For a given lattice L, let $A(L)$ be the associated Boolean ring and $X = \text{Spec } A(L)$. The basic open sets X_f are the only open and closed subsets of X, which is compact Hausdorff.

Let X' denote the set of open and closed subsets of X, we just need to show that there is an order-preserving isomorphism

$$\phi : L \to X' \qquad f \mapsto X_f$$

ϕ is clearly surjective, it is also injective because

$$\text{Ker } \phi = \{f \in A \mid \phi(f) = X_f = \varnothing\} = \{f \in A \mid f \text{ nilpotent}\} = \{0\}$$

Since if x where nilpotent, then $x^n = x = 0$.

Finally, we show that it is order-preserving

$$f \leq g \iff f = fg \to f \in (g) \iff V(g) \subseteq V(f) \iff X_f \subseteq X_g$$

$$X_f \subseteq X_g \iff f \in (g) \iff f = ag = ag \cdot g = fg \iff f \leq g$$

This establishes Stone's theorem, every Boolean lattice L is isomorphic to the lattice of open and closed subsets X' of a compact Hausdorff space $X = \text{Spec } A(L)$.

1.3.6 Maximal Spectrum

Exercise 26. Let X be a compact Hausdorff space and define

$$C(X) = \{f : X \to \mathbb{R} \text{ continuous}\}$$

This is a ring under addition and multiplication of functions. For each $x \in X$, let

$$\mathfrak{m}_x = \{f \in C(X) \mid f(x) = 0\}$$

which is maximal because it is the kernel of the surjective homomorphism

$$\phi : C(X) \to \mathbb{R} \qquad f \mapsto f(x)$$

Let $\tilde{X} = \text{Max } C(X)$ be the subset of the prime spectrum consisting only of maximal ideals (the maximal spectrum). We have just defined a mapping

$$\mu : X \to \tilde{X} \qquad x \mapsto \mathfrak{m}_x$$

We will prove that this is a homeomorphism.

i) μ is surjective: Let $\mathfrak{m} \subseteq C(X)$ be any maximal ideal and

$$V = V(\mathfrak{m}) = \{x \in X \mid f(x) = 0; \forall f \in \mathfrak{m}\}$$

Suppose there are no common zeros so that V is empty, then for every $x \in X$ there exists some $f_x \in \mathfrak{m}$ such that $f_x(x) \neq 0$. Since f_x is continuous, there must exists some neighborhood U_x of x on which f_x is nonzero.

These clearly cover X, but X is compact so there must be some finite subset which also covers X. Let $U_{x_1}, \ldots, U_{x_n}$ be that finite subset and define

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

Then by our construction, f is nonzero on all of X and thus is a unit ($f^{-1} = 1/f$) in $C(X)$. But this would mean $1 \in \mathfrak{m}$, a contradiction, so V cannot be empty.

Let $x \in V$ be some point, then every $f \in \mathfrak{m}$ vanishes at x so

$$\mathfrak{m} \subseteq \mathfrak{m}_x \longrightarrow \mu(x) = \mathfrak{m}_x = \mathfrak{m}$$

ii) μ is injective: this follows from Urysohn's lemma:

Lemma 1.20. Let X be a compact Hausdorff space and A, B disjoint closed subsets of X. Let $[a, b]$ be a closed interval of $\mathbb{R}$, then there exists a continuous map

$$f : X \to [a, b]$$

such that $f(A) = a$ and $f(B) = b$.

This implies that the continuous functions $C(X)$ separate the points of X. Let $x \neq y$, then by Urysohn's lemma there exists functions $f, g : X \to [0, 1]$ such that

$$f(x) = 0 \quad f(y) = 1 \qquad g(x) = 1 \qquad g(y) = 0$$

Thus $\mathfrak{m}_x \neq \mathfrak{m}_y$.

iii) μ is continuous: For any $f \in C(X)$, define

$$U_f = \{x \in X \mid f(x) \neq 0\} \qquad \tilde{U_f} = \left\{\mathfrak{m} \in \tilde{X} \mid f \notin \mathfrak{m}\right\}$$

The U_f form a basis for X since $U_1 = X$ and if $x \in U_f, U_g$, then

$$x \in U_{fg} \subseteq U_f \cap U_g$$

Similarly, the $\tilde{U_f}$ form a basis for $\tilde{X}$. μ maps open sets to open sets since

$$x \in U_f \iff f(x) \neq 0 \iff f \notin \mathfrak{m}_x \iff \mathfrak{m}_x \in \tilde{U_f} = \mu(U_f)$$

Thus μ is a bijective continuous map, hence a homeomorphism. This implies we can construct any compact Hausdorff space X from just it's ring of functions $C(X)$.

1.3.7 Affine Varieties

Exercise 27. Let k be an algebraically closed field and consider a collection of polynomials $f_i \in k[t_1, \ldots t_n]$. An affine algebraic variety is the set

$$X = \{x \in k^n \mid f_i(x) = 0; \forall i\}$$

Given an affine algebraic variety X, we can pullback to an ideal

$$I(X) = \{f \in k[t_1, \dots, t_n] \mid f(x) = 0; \forall x \in X\}$$

This is the ideal of the variety X. The quotient ring

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

is the ring of polynomial functions defined on X. Two polynomials f, g define the same function on X if and only if $f - g$ vanishes for every $x \in X$, i.e. $f - g \in I(X)$. The i-th coordinate function ($1 \leq i \leq n$) is the image $\xi_i = \overline{x_i} \in P(X)$. $P(X)$ is generated by these coordinate functions, so it is called the coordinate ring (or affine algebra) of X.[10]

For each $x \in X$, let $\mathfrak{m}_x$ be the maximal ideal of $P(X)$ consisting of all functions which vanish at x. Just like the previous exercise, this gives a map

$$\mu : X \to \tilde{X} = \text{Max } P(X) \qquad x \mapsto \mathfrak{m}_x$$

If $x \neq y$, then one of their coordinates must differ. That is, there is some i such that $x_i \neq y_i$ and so we have

$$\xi_i - x_i \in \mathfrak{m}_x \setminus \mathfrak{m}_y \longrightarrow \mathfrak{m}_x \neq \mathfrak{m}_y$$

Thus μ is injective, surjectivity follows from Hilbert's Nullstellensatz.[11]

Proposition 1.21. With $I(X)$ defined as before and $V(\mathfrak{a})$ from the previous exercise, then for any ideal $\mathfrak{a} \subseteq k[t_1, \dots, t_n]$

$$V(\mathfrak{a}) \neq \varnothing$$

Let $\mathfrak{m} \in \tilde{X}$, recall that there is a one-to-one correspondence between ideals of $P(X) = k[t_1, \dots, t_n]/I(X)$ and ideals of $k[t_1, \dots, t_n]$ which contain $I(X)$. Let $\mathfrak{m}'$ be the corresponding ideal, then the weak Nullstellensatz tells us

$$V(\mathfrak{m}') \neq \varnothing$$

Let $x \in V(\mathfrak{m}')$ be some point and note that if a function f vanishes at x, $\overline{f} \in P(X)$ will also vanish at x. Thus $\mathfrak{m} = \mathfrak{m}_x$ and μ is surjective.

Exercise 28. Let $f_1, \dots, f_m \in k[t_1, \dots, t_n]$, then they determine a polynomial mapping

$$\phi : k^n \to k^m \qquad x \mapsto (f_1(x), \dots, f_m(x))$$

Let $X \subseteq k^n, Y \subseteq k^m$ be affine varieties. A map $\phi : X \to Y$ is regular if ϕ is a polynomial mapping from $k^n \to k^m$ restricted to ϕ. ϕ induces a homomorphism

$$\phi* : P(Y) \to P(X) \qquad \eta \mapsto \eta \circ \phi$$

[10] It is generated as a k-algebra, which we will define in Chapter 2.

[11] This is proved much, much later in Chapter 7. The weak version will suffice for this problem which is proved in Chapter 5.

Denote this correspondence

$$\Phi : \{\text{Regular Maps } X \to Y\} \to \{\text{Homomorphisms } P(Y) \to P(X)\}$$

$$\Phi(\phi) = \phi^*$$

If $\phi_1^* = \phi_2^*$ as homomorphisms, then by composing with the coordinate functions

$$\phi_{1_i} = \xi_i \circ \phi_1 = \phi_1^*(\xi_1) = \phi_2^*(\xi_1) = \xi_i \circ \phi_2 = \phi_{2_i}$$

Thus we must have $\phi_1 = \phi_2$ and Φ is injective.

Let $\psi : P(Y) \to P(X)$ be some homomorphism, it is uniquely determined by where it sends each of the y_i. Let ϕ_i be the map which sends $y_i \mapsto \psi(y_i)$, then $\phi^* = \psi$ and thus Φ is surjective.