

Commutative Algebra

Chapter 1: Rings and Ideals

Sichuan University, Fall 2022

Rings and Ring Homomorphisms

Definition (Rings)

A ring A is a set with an addition and a multiplication so that:

- 1 A is an Abelian group w.r.t. its addition, and so
 - A has a zero element, denoted 0 .
 - Every $x \in A$ has an additive inverse $-x$.
- 2 Multiplication is associative and distributive over addition,

$$\begin{aligned}(xy)z &= x(yz), \\ x(y+z) &= xy + xz, & (x+y)z &= xz + yz.\end{aligned}$$

Remarks

- 1 0 is absorbant, i.e., $0x = x0 = 0$ for all $x \in A$.
- 2 $x(y-z) = xy - xz$ and $(x-y)z = xz - yz$.

Rings and Ring Homomorphisms

Definition

- ① A ring A is commutative when

$$xy = yx \quad \text{for all } x, y \in A.$$

- ② An identity element $1 \in A$ is such that

$$1x = x1 = x \quad \text{for all } x \in A.$$

Such an element is unique.

Remark

By a ring we shall always mean a commutative ring with an identity element.

Remark

If $1 = 0$, then $x = 1x = 0x = 0$, and so 0 is the unique element. We called this ring the zero ring and denote it by 0 .

Rings and Ring Homomorphisms

Definition (Ring Homomorphisms)

Given rings A and B , a ring homomorphism $f : A \rightarrow B$ is a map such that

- ① $f(x + y) = f(x) + f(y)$.
- ② $f(xy) = f(x)f(y)$.
- ③ $f(1) = 1$.

Remark

The property (i) implies that

$$f(x - y) = f(x) - f(y), \quad f(-x) = -f(x), \quad f(0) = 0.$$

Remark

If $f : A \rightarrow B$ and $g : B \rightarrow C$ are ring homomorphisms, then the composition $g \circ f : A \rightarrow C$ is a ring homomorphism as well.

Definition (Subrings)

A subring of a ring A is a subset S that is closed under addition and multiplication and contains the unit. That is,

$$x, y \in S \implies x + y \in S \text{ and } xy \in S, \\ 1 \in S.$$

Remarks

- 1 Any subring is a ring.
- 2 If S is a subring of a ring A , then the inclusion map of S into A is a ring homomorphism.

Ideals. Quotient Rings

Definition (Ideals)

An ideal $\mathfrak{a}$ of a ring A is an additive subgroup such that $A\mathfrak{a} \subset \mathfrak{a}$. That is,

$$\begin{aligned}x, y \in \mathfrak{a} &\implies x + y \in \mathfrak{a}, \\x \in A \text{ and } y \in \mathfrak{a} &\implies xy \in \mathfrak{a}.\end{aligned}$$

Observation

The multiplication of A uniquely descends to a multiplication on the quotient $A/\mathfrak{a}$, with respect to which $A/\mathfrak{a}$ is a ring.

Remarks

- 1 $A/\mathfrak{a}$ is called a quotient ring. Its elements $x + \mathfrak{a}$ are called cosets (of $\mathfrak{a}$ in A).
- 2 The canonical map $\phi : A \rightarrow A/\mathfrak{a}$ is a surjective ring homomorphism.

Proposition (Proposition 1.1)

We have an order-preserving one-to-one correspondence,

$$\begin{aligned}\{\text{Ideals of } A \text{ containing } \mathfrak{a}\} &\longleftrightarrow \{\text{Ideals of } A/\mathfrak{a}\}, \\ \mathfrak{b} = \phi^{-1}(\bar{\mathfrak{b}}) &\longleftrightarrow \bar{\mathfrak{b}} = \phi(\mathfrak{b}).\end{aligned}$$

Remark

This result is used implicitly throughout Atiyah-MacDonald's book.

Proof of Proposition 1.1.

- Let $\mathfrak{b}$ be an ideal of A . Let $\bar{x} = \phi(x)$ with $x \in \mathfrak{b}$ and $\bar{y} = \phi(y) \in A/\mathfrak{a}$. Then

$$\overline{xy} = \phi(x)\phi(y) = \phi(xy) \in \phi(\mathfrak{b}).$$

Thus, $\phi(\mathfrak{b})$ is an ideal of $A/\mathfrak{a}$.

- Let $\bar{\mathfrak{b}}$ be an ideal of $A/\mathfrak{a}$. Then:
 - $\phi^{-1}(\bar{\mathfrak{b}}) \supseteq \phi^{-1}(0) = \mathfrak{a}$.
 - If $x \in \phi^{-1}(\bar{\mathfrak{b}})$ and $y \in A$, then $xy \in \phi^{-1}(\bar{\mathfrak{b}})$, since $\phi(x) \in \bar{\mathfrak{b}}$, and hence $\phi(xy) = \phi(x)\phi(y) \in \bar{\mathfrak{b}}$

Thus, $\phi^{-1}(\bar{\mathfrak{b}})$ is an ideal containing $\mathfrak{a}$.

- $\mathfrak{b} \rightarrow \phi(\mathfrak{b})$ and $\bar{\mathfrak{b}} \rightarrow \phi^{-1}(\bar{\mathfrak{b}})$ are inverses of each other:
 - If $\bar{\mathfrak{b}}$ is an ideal of $A/\mathfrak{a}$, then $\phi(\phi^{-1}(\bar{\mathfrak{b}})) = \bar{\mathfrak{b}}$, since ϕ is onto.
 - If $\mathfrak{b}$ is an ideal containing $\mathfrak{a}$, then $\phi^{-1}(\phi(\mathfrak{b})) = \mathfrak{b}$, since

$$x \in \phi^{-1}(\phi(\mathfrak{b})) \iff \phi(x) \in \phi(\mathfrak{b}) \iff x \in \mathfrak{b} + \mathfrak{a} \iff x \in \mathfrak{b}.$$

Therefore, we have a bijection (one-to-one correspondence) between ideals of A containing $\mathfrak{a}$ and ideals of $A/\mathfrak{a}$.



Facts

Let $f : A \rightarrow B$ is a ring homomorphism. Then

- 1 The kernel $f^{-1}(0)$ is an ideal of A .
- 2 The image $f(A)$ is a subring of B .
- 3 f induces a ring isomorphism $A/f^{-1}(0) \simeq f(A)$.

Remark

The notation $x \equiv y \pmod{a}$ means that $x - y \in a$.

Definition (Zero-Divisors, Integral Domains)

- A zero-divisor of a ring A is any element x that divides 0, i.e., there is $y \neq 0$ such that $xy = 0$.
- A (non-zero) ring with no non-zero divisors is called an *integral domain*. That is, we have

$$x \neq 0 \text{ and } xy = 0 \implies y = 0.$$

Examples

The following rings are integral domains:

- The ring of integers $\mathbb{Z}$.
- Any polynomial rings $k[x_1, \dots, x_n]$, where k is a field.

Definition (Nilpotent Elements)

An element $x \in A$ is nilpotent when $x^n = 0$ for some $n \geq 1$.

Remark

Any nilpotent element is a zero-divisor (unless $A = 0$). The converse is not true in general.

Definition (Units)

- A unit of A is any element x that divides 1 , i.e., there is $y \in A$ such that $xy = 1$.
- In this case y is unique and is denoted x^{-1} .

Fact

The set of units of A is a (multiplicative) Abelian group.

Definition (Principal Ideals)

A *principal ideal* is any ideal generated by a single element, i.e., it is of the form Ax for some $x \in A$.

Remarks

- 1 We shall also denote Ax by (x) . It consists of all multiples ax , $a \in A$.
- 2 x is a unit if and only if $(x) = A = (1)$.
- 3 The zero ideal (0) is denoted 0 .

Definition (Field)

A field is a ring A in which $1 \neq 0$ and every $x \neq 0$ is a unit.

Remark

Every field is an integral domain. The converse is not true (e.g., $\mathbb{Z}$).

Proposition (Proposition 1.2)

Let A be a non-zero ring. TFAE:

- (i) A is a field.
- (ii) The only ideals in A are 0 and A .
- (iii) Every ring homomorphism of A into a non-zero ring is one-to-one.

Prime Ideals and Maximal Ideals

Definition (Prime Ideals)

An ideal $\mathfrak{p} \subsetneq A$ is prime when $xy \in \mathfrak{p} \Rightarrow x \in \mathfrak{p}$ or $y \in \mathfrak{p}$.

Fact

$\mathfrak{p}$ is prime $\iff A/\mathfrak{p}$ is an integral domain.

Definition (Maximal Ideal)

An ideal $\mathfrak{m} \subsetneq A$ is maximal when there is no ideal $\mathfrak{a}$ such that $\mathfrak{m} \subsetneq \mathfrak{a} \subsetneq A$.

Fact (Proposition 1.1 + Proposition 1.2)

$\mathfrak{m}$ is maximal $\iff A/\mathfrak{m}$ is a field.

In particular, any maximal ideal is prime.

Remark

The zero ideal is prime if and only if A is an integral domain.

Prime Ideals and Maximal Ideals

Fact

Let $f : A \rightarrow B$ be a ring homomorphism and $\mathfrak{q}$ a prime ideal. Then $f^{-1}(\mathfrak{q})$ is a prime ideal in A .

Proof.

We have

$$xy \in f^{-1}(\mathfrak{q}) \iff f(xy) \in \mathfrak{q} \iff f(x)f(y) \in \mathfrak{q}.$$

As $\mathfrak{q}$ is prime, $f(x)$ or $f(y)$ is in $\mathfrak{q}$, i.e., x or y is in $f^{-1}(\mathfrak{q})$, and hence $\mathfrak{q}$ is prime. □

Remark

If $\mathfrak{n}$ is a maximal ideal in A , then $f^{-1}(\mathfrak{n})$ is prime, but it need not be maximal (e.g., $A = \mathbb{Z}$, $B = \mathbb{Q}$, $\mathfrak{n} = 0$).

Prime Ideals and Maximal Ideals

Theorem (Theorem 1.3; see Atiyah-MacDonald + Carlson)

Every ring $A \neq 0$ admits a maximal ideal.

Corollary (Corollary 1.4)

For any ideal $\mathfrak{a} \subsetneq A$, there is a maximal ideal that contains $\mathfrak{a}$.

Proof.

Apply Theorem 1.3 to $A/\mathfrak{a}$ and use Proposition 1.1. □

Corollary (Corollary 1.5)

Every non-unit of A is contained in a maximal ideal.

Prime Ideals and Maximal Ideals

Remark

There are rings with exactly one maximal ideal, e.g., fields (in which 0 is the unique maximal ideal).

Definition

- 1 A ring with exactly one maximal ideal $\mathfrak{m}$ is called a local ring.
- 2 The field $k = A/\mathfrak{m}$ is called the residual field of A .

Proposition (Proposition 1.6)

- (i) Let $\mathfrak{m} \subsetneq A$ be an ideal such that any $x \in A \setminus \mathfrak{m}$ is a unit. Then A is local ring and has $\mathfrak{m}$ is its unique maximal ideal.
- (ii) Let $\mathfrak{m}$ be a maximal ideal such that every element of $1 + \mathfrak{m}$ is a unit. Then A is a local ring.

Prime Ideals and Maximal Ideals

Example

Let $A = k[x_1, \dots, x_n]$, k field. If $f \in A$ is irreducible, then the ideal (f) is prime.

Example

Let $A = \mathbb{Z}$. Then

- 1 Every ideal of $\mathbb{Z}$ is a principal ideal (m) for some $m \geq 0$.
- 2 (m) is a prime ideal if and only if $m = 0$ or m is a prime number.
- 3 All the ideals (p) with p prime are maximal, since $\mathbb{Z}/(p) = \mathbb{Z}/p\mathbb{Z}$ is a field.
- 4 The same holds for $A = k[x_1]$, but not for $A = k[x_1, \dots, x_n]$ with $n \geq 2$.

Prime Ideals and Maximal Ideals

Example

Every ideal of $\mathbb{Z}$ is a principal ideal (m) for some $m \geq 0$.

Proof.

Let $\mathfrak{a}$ be a non-zero ideal.

- Let m be the smallest positive element of $\mathfrak{a}$. Then $(m) \subseteq \mathfrak{a}$.
- Let $y \in \mathfrak{a} \setminus 0$. Assume $y > 0$ and $y = qm + r$ with $0 \leq r \leq m - 1$.
- Assume $r \neq 0$. Then $0 < r < m$, and so $r \notin \mathfrak{a}$,
- However, $r = y - qm \in \mathfrak{a} + (m) = \mathfrak{a}$ (contradiction).
- Thus, $r = 0$, and so $y = qm \in (m)$.
- It follows that $\mathfrak{a} = (m)$.

The proof is complete. □

Prime Ideals and Maximal Ideals

Example

(m) is a prime ideal of $\mathbb{Z}$ if and only if $m = 0$ or m is a prime number.

Proof.

- Assume $m \geq 1$. If $x \neq 0$, then

$$x \in (m) \iff x \in m\mathbb{Z} \iff m \text{ divides } x.$$

- If m is a prime number, then (m) is a prime ideal, since

$$\begin{aligned} xy \in (m) &\iff m \text{ divides } xy \\ &\iff m \text{ divides } x \text{ or } y \\ &\iff x \in (m) \text{ or } y \in (m). \end{aligned}$$

- Suppose that m is not a prime number.
 - There are integers $x, y \geq 2$ such that $xy = m \in (m)$.
 - m does not divide x or y , and so $x, y \notin (m)$.
 - Thus, (m) is not a prime ideal.

This proves the result. □

Example (Principal Ideal Domain)

A *principal ideal domain* is an integral domain in which every ideal is principal (e.g., $\mathbb{Z}$, $k[x_1]$). In such an ideal every non-zero prime ideal is maximal.

Prime Ideals and Maximal Ideals

Reminder

Let $\mathfrak{a}$ be an ideal and $\phi : A \rightarrow A/\mathfrak{a}$ the canonical homomorphism. By Proposition 1.1 we have an order-preserving one-to-one correspondence between ideals of A containing $\mathfrak{a}$ and ideals of $A/\mathfrak{a}$,

$$\mathfrak{b} = \phi^{-1}(\bar{\mathfrak{b}}) \longleftrightarrow \bar{\mathfrak{b}} = \phi(\mathfrak{b}).$$

Proposition (Proposition 1.1*)

This correspondence induces one-to-one correspondences:

$$\begin{aligned} \{\text{Maximal ideals of } A \text{ containing } \mathfrak{a}\} &\longleftrightarrow \{\text{Maximal ideals of } A/\mathfrak{a}\}, \\ \{\text{Prime ideals of } A \text{ containing } \mathfrak{a}\} &\longleftrightarrow \{\text{Prime ideals of } A/\mathfrak{a}\}, \end{aligned}$$

Remark

The above result is not stated explicitly in Atiyah-MacDonald's book. However, it is used throughout the book.

Proof of Proposition 1.1*.

- We have a correspondence between maximal ideals, because the correspondence between ideals is order-preserving.
- Let $\mathfrak{p}$ be an ideal containing $\mathfrak{a}$. Then

$$\begin{aligned}\phi(x) \in \phi(\mathfrak{p}) &\iff x \in \mathfrak{p} + \mathfrak{a} \iff x \in \mathfrak{p}, \\ \phi(x)\phi(y) \in \phi(\mathfrak{p}) &\iff \phi(xy) \in \phi(\mathfrak{p}) \iff xy \in \mathfrak{p}.\end{aligned}$$

- If $\mathfrak{p}$ is prime, then $\phi(\mathfrak{p})$ is prime, since

$$\begin{aligned}\phi(x)\phi(y) \in \phi(\mathfrak{p}) &\iff xy \in \mathfrak{p} \iff (x \in \mathfrak{p} \text{ or } y \in \mathfrak{p}) \\ &\iff (\phi(x) \in \phi(\mathfrak{p}) \text{ or } \phi(y) \in \phi(\mathfrak{p})).\end{aligned}$$

- Conversely, if $\phi(\mathfrak{p})$ is prime, then $\mathfrak{p}$ is prime, since

$$\begin{aligned}xy \in \mathfrak{p} &\iff \phi(x)\phi(y) \in \phi(\mathfrak{p}) \iff (\phi(x) \in \phi(\mathfrak{p}) \text{ or } \phi(y) \in \phi(\mathfrak{p})) \\ &\iff (x \in \mathfrak{p} \text{ or } y \in \mathfrak{p}).\end{aligned}$$

- This gives the correspondence between prime ideals.

The result is proved. □

Proposition (Proposition 1.7)

Let $\mathfrak{N}$ be the set of all nilpotent elements of A . Then:

- 1 $\mathfrak{N}$ is an ideal
- 2 The quotient ring $A/\mathfrak{N}$ has no non-zero nilpotent elements.

Definition

The ideal $\mathfrak{N}$ is called the nilradical of A .

Niradical and Jacobson Radical

Proposition (Proposition 1.8; see Atiyah-MacDonald)

The nilradical $\mathfrak{N}$ is the intersection of all the prime ideals of A .

Sketch of Proof.

Let $\mathfrak{N}'$ be the intersections of all prime ideals.

- Let $f \in \mathfrak{N}$ and $\mathfrak{p}$ a prime ideal. Then $f^n = 0 \in \mathfrak{p}$ for some n .
 - Let n_0 be the smallest integer such that $f^{n_0} \in \mathfrak{p}$.
 - If $n_0 \geq 2$. Then $f^{n_0-1} \notin \mathfrak{p}$ and $f \notin \mathfrak{p}$, but $f^{n_0-1}f = f^{n_0} \in \mathfrak{p}$.
 - As $\mathfrak{p}$ is prime, this implies that $f^{n_0-1} \in \mathfrak{p}$ or $f \in \mathfrak{p}$ (contradiction).
 - Thus, $f \in \mathfrak{p}$ for every prime ideal $\mathfrak{p}$, and hence $f \in \mathfrak{N}'$.

This shows that $\mathfrak{N} \subseteq \mathfrak{N}'$.

- Let $f \notin \mathfrak{N}$. Let Σ be the set of ideals $\mathfrak{a}$ s.t. $f^n \notin \mathfrak{a} \forall n \geq 1$.
 - By Zorn's lemma Σ has a maximal element $\mathfrak{p}$. Then $f \notin \mathfrak{p}$.
 - It can be shown that $\mathfrak{p}$ is a prime ideal, and so $f \notin \mathfrak{N}'$.

This shows that $A \setminus \mathfrak{N} \subseteq A \setminus \mathfrak{N}'$, and hence $\mathfrak{N}' \subseteq \mathfrak{N}$.

This gives the result.



Definition

The Jacobson radical $\mathfrak{R}$ of A is the intersection of all its maximal ideals.

Niradical and Jacobson Radical

Proposition (Proposition 1.9)

$$\mathfrak{N} = \{x \in A; 1 - xy \text{ is a unit for all } y \in A\}.$$

Proof.

- Let $x \in \mathfrak{N}$. If $y \in A$ is s.t. $1 - xy$ is not a unit, then:
 - By Corollary 1.5 there is a maximal ideal $\mathfrak{m} \ni 1 - xy$
 - As $x \in \mathfrak{N} \subseteq \mathfrak{m}$, and hence $xy \in \mathfrak{m}$, we see that $1 = (1 - xy) + xy \in \mathfrak{m}$, which is impossible ($\mathfrak{m}$ is maximal).

Therefore $1 - xy$ is a unit for all $y \in A$.

- Let $x \notin \mathfrak{N}$, i.e., $x \notin \mathfrak{m}$ for some maximal ideal $\mathfrak{m}$. Then:
 - As $\mathfrak{m}$ is maximal, the ideal generated by x and $\mathfrak{m}$ is A .
 - Thus, there are $u \in \mathfrak{m}$ and $y \in A$ such that $u + xy = 1$.
 - Therefore $1 - xy = u \in \mathfrak{m}$ is not a unit.

By contraposition, if $1 - xy$ is a unit for all y , then $x \in \mathfrak{N}$.

This proves the result. □

Operations on Ideals

Definition (Sum of Ideals)

If $\mathfrak{a}$ and $\mathfrak{b}$ are ideals in a ring A , their sum $\mathfrak{a} + \mathfrak{b}$ is the set all sums $x + y$ with $x \in \mathfrak{a}$ and $y \in \mathfrak{b}$.

Fact

$\mathfrak{a} + \mathfrak{b}$ is the smallest ideal that contains $\mathfrak{a}$ and $\mathfrak{b}$.

Definition (Sum of Ideals)

Given a (possibly infinite) family $\{\mathfrak{a}_i\}_{i \in I}$ of ideals of A , the sum $\sum_{i \in I} \mathfrak{a}_i$ consists of all finite sums $\sum x_i$ with $x_i \in \mathfrak{a}_i$.

Fact

$\sum_{i \in I} \mathfrak{a}_i$ is the smallest ideal that contains the $\mathfrak{a}_i$'s.

Fact

The intersection of any family of ideals $(\mathfrak{a}_i)_{i \in I}$ is an ideal.

Consequence

The ideals of A form a complete lattice with respect to inclusion, i.e., every subset has a supremum and an infimum.

Definition (Product of Ideals)

The product of two ideals $\mathfrak{a}$ and $\mathfrak{b}$ in A consists of all finite sums $\sum x_i y_i$ with $x_i \in \mathfrak{a}$ and $y_i \in \mathfrak{b}$.

Remark

- ① We similarly define the product of any finite family of ideals.
- ② In particular, the power $\mathfrak{a}^n$, $n \geq 1$, of an ideal $\mathfrak{a}$ is generated by products $x_1 \cdots x_n$ with $x_j \in \mathfrak{a}$.
- ③ By convention $\mathfrak{a}^0 = (1) = A$.

Operations on Ideals

Example

Suppose that $A = \mathbb{Z}$, $\mathfrak{a} = (m)$ and $\mathfrak{b} = (n)$. Then:

- ① $\mathfrak{a} + \mathfrak{b}$ is the ideal generated by $\gcd(m, n)$ (greatest common divisor, a.k.a. highest common factor).
- ② $\mathfrak{a} \cap \mathfrak{b}$ is the ideal generated by $\text{lcm}(m, n)$ (lowest common multiple).
- ③ $\mathfrak{a}\mathfrak{b} = (mn)$.

Example

$A = k[x_1, \dots, x_n]$, $\mathfrak{a} = (x_1, \dots, x_n)$ ideal generated by $x_1, \dots, x_n$. Then $\mathfrak{a}^m$, $m \geq 1$, consists of all polynomials with no terms of degree $< m$.

Remarks

- ① The three operations (sum, intersection, product) are all associative and commutative.
- ② We also have the distributive law,

$$a(b + c) = ab + ac.$$

- ③ In $\mathbb{Z}$ the laws $\cap$ and $+$ are distributive over each other. This is not true for a general ring. At best we have the modular law,

$$a \cap (b + c) = a \cap b + a \cap c \quad \text{if } a \supseteq b \text{ or } a \supseteq c.$$

- ④ In $\mathbb{Z}$ we have $(a + b)(a \cap b) = ab$. In general, we only have

$$(a + b)(a \cap b) \subseteq ab.$$

Operations on Ideals

Definition

Two ideals $\mathfrak{a}$ and $\mathfrak{b}$ are said to be coprime when $\mathfrak{a} + \mathfrak{b} = (1)$. That is, there are $x \in \mathfrak{a}$ and $y \in \mathfrak{b}$ such that $x + y = 1$.

Fact

We always have the inclusions,

$$(\mathfrak{a} + \mathfrak{b})(\mathfrak{a} \cap \mathfrak{b}) \subseteq \mathfrak{a}\mathfrak{b} \quad \text{and} \quad \mathfrak{a}\mathfrak{b} \subseteq \mathfrak{a} \cap \mathfrak{b}.$$

Thus, if $\mathfrak{a}$ and $\mathfrak{b}$ are coprime, then we have

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

Definition (Direct Product of Rings)

Let $A_1, \dots, A_n$ be rings ($n \geq 2$).

- ① The direct product $A := \prod_{i=1}^n A_i$ consists of sequences $(x_1, \dots, x_n)$ with $x_i \in A_i$.
- ② We equip it with the component-wise addition and multiplication.

Facts

- ① $\prod_{i=1}^n A_i$ is a commutative ring with identity $(1, \dots, 1)$.
- ② The projections $p_i : A \rightarrow A_i$ defined by $p_i(x) = x_i$ are ring homomorphisms.

Operations on Ideals

Let A be a ring $\mathfrak{a}_1, \dots, \mathfrak{a}_n$ ideals of A . Define $\phi : A \rightarrow \prod_{i=1}^n (A/\mathfrak{a}_i)$ by

$$\phi(x) = (x + \mathfrak{a}_1, \dots, x + \mathfrak{a}_n), \quad x \in A.$$

Fact

ϕ is a ring homomorphism.

Proposition (Proposition 1.10)

The following holds.

- ① If $\mathfrak{a}_i$ and $\mathfrak{a}_j$ are coprime whenever $i \neq j$, then $\prod \mathfrak{a}_i = \cap \mathfrak{a}_i$.
- ② ϕ is onto if and only if $\mathfrak{a}_i$ and $\mathfrak{a}_j$ are coprime for $i \neq j$.
- ③ ϕ is one-to-one if and only if $\cap \mathfrak{a}_i = 0$.

Operations on Ideals

Remark

The union $\mathfrak{a} \cup \mathfrak{b}$ need not be an ideal in general.

Proposition (Proposition 1.11)

- ① Assume that $\mathfrak{p}_1, \dots, \mathfrak{p}_n$ are prime ideals and $\mathfrak{a}$ is an ideal contained in $\bigcup \mathfrak{p}_i$. Then $\mathfrak{a} \subseteq \mathfrak{p}_i$ for some i .
- ② Assume that $\mathfrak{a}_1, \dots, \mathfrak{a}_n$ are ideals and $\mathfrak{p}$ is a prime ideal containing $\bigcap \mathfrak{a}_i$. Then $\mathfrak{p} \supseteq \mathfrak{a}_i$ for some i . If $\mathfrak{p} = \bigcap \mathfrak{a}_i$, then $\mathfrak{p} = \mathfrak{a}_i$ for some i .

Remark

Let $\mathfrak{p}$ be a prime ideal. By induction it can be shown that

$$x_1 \cdots x_n \in \mathfrak{p} \implies x_i \in \mathfrak{p} \text{ for some } i.$$

By contraposition we get

$$x_i \notin \mathfrak{p} \text{ for all } i \implies x_1 \cdots x_n \notin \mathfrak{p}.$$

Proof of Proposition 1.11(i).

We show by induction that

$$(*) \quad \mathfrak{a} \not\subseteq \mathfrak{p}_i \ (1 \leq i \leq n) \implies \mathfrak{a} \not\subseteq \bigcup \mathfrak{p}_i.$$

By contraposition this will give the result.

- For $n = 1$ the result is immediate.
- Assume $(*)$ is true for $n - 1$. Let $\mathfrak{a} \not\subseteq \mathfrak{p}_i$ for $i = 1, \dots, n$.
- As $(*)$ is true for $n - 1$, for each i , we have $\mathfrak{a} \not\subseteq \bigcup_{j \neq i} \mathfrak{p}_j$, i.e., there is $x_i \in \mathfrak{a}$ s.t. $x_i \notin \mathfrak{p}_j$ for $j \neq i$.
- If $x_i \notin \mathfrak{p}_i$ for some i , then we are done.
- Suppose that $x_i \in \mathfrak{p}_i$ for all i . Set

$$y = \sum_{1 \leq j \leq n} y_j, \quad \text{where } y_j = x_1 \cdots x_{j-1} x_{j+1} \cdots x_n.$$

- As $x_i \in \mathfrak{p}_i$, we see that $y_j = \prod_{k \neq j} x_k \in \mathfrak{p}_i$ for $j \neq i$.

Proof of Proposition 1.11(i), Continued.

- As $y_j \in \mathfrak{p}_i$ for $j \neq i$, we get

$$\begin{aligned}y &= y_1 + \cdots + y_n \\&\equiv y_i \pmod{\mathfrak{p}_i} \\&\equiv x_1 \cdots x_{i-1} x_{i+1} \cdots x_n \pmod{\mathfrak{p}_i}.\end{aligned}$$

- As $x_j \notin \mathfrak{p}_i$ for $j \neq i$ and $\mathfrak{p}_i$ is a prime ideal, we see that $x_1 \cdots x_{i-1} x_{i+1} \cdots x_n \notin \mathfrak{p}_i$ (see previous remark).
- It follows that $y \notin \mathfrak{p}_i$ for all i , and hence $\mathfrak{a} \not\subseteq \bigcup_{i=1}^n \mathfrak{p}_i$.

This shows that $(*)$ is true for n . The proof is complete. $\square$

Proof of Proposition 1.11(ii).

- Suppose that $\mathfrak{p} \not\supseteq \mathfrak{a}_i$ for $i = 1, \dots, n$. Thus, for each i there is $x_i \in \mathfrak{a}$ s.t. $x_i \notin \mathfrak{p}$.
- As $\mathfrak{p}$ is prime $x_1 \cdots x_n \notin \mathfrak{p}$ (see previous remark).
- As $x_1 \cdots x_n \in \mathfrak{a}_1 \cdots \mathfrak{a}_n \subseteq \cap \mathfrak{a}_i$, we see that $\mathfrak{p} \not\supseteq \cap \mathfrak{a}_i$.
- By contraposition, we get

$$\mathfrak{p} \supseteq \bigcap \mathfrak{a}_i \implies \mathfrak{p} \supseteq \mathfrak{a}_i \text{ for some } i.$$

- If $\mathfrak{p} = \cap \mathfrak{a}_j$, then $\mathfrak{a}_i \subseteq \mathfrak{p} \subseteq \cap \mathfrak{a}_j \subseteq \mathfrak{a}_i$, and hence $\mathfrak{p} = \mathfrak{a}_i$.

The result is proved. □

Operations on Ideals

Definition (Ideal Quotient)

If $\mathfrak{a}$ and $\mathfrak{b}$ are ideals in a ring A , their ideal quotient is

$$(\mathfrak{a} : \mathfrak{b}) := \{x; x\mathfrak{b} \subseteq \mathfrak{a}\}.$$

Fact

$(\mathfrak{a} : \mathfrak{b})$ is an ideal.

Definition

$(0 : \mathfrak{b})$ is called the annihilator of $\mathfrak{b}$ and is also denoted by $\text{Ann}(\mathfrak{b})$. It consists of all $x \in A$ such that $x\mathfrak{b} = 0$.

Remarks

- 1 When $\mathfrak{b}$ is a principal ideal (x) we shall denote $(\mathfrak{a} : (x))$ and $\text{Ann}((x))$ by $(\mathfrak{a} : x)$ and $\text{Ann}(x)$, respectively.
- 2 $\text{Ann}(x) = \{y \in A; xy = 0\}$.
- 3 The set of all non-zero divisors in A is $D = \bigcup_{x \neq 0} \text{Ann}(x)$.

Example

$A = \mathbb{Z}$, $\mathfrak{a} = (m)$, $\mathfrak{b} = (n)$. Then

$$\begin{aligned}(m : n) &= \{x \in \mathbb{Z}; xn\mathbb{Z} \subseteq m\mathbb{Z}\}, \\ &= \{x \in \mathbb{Z}; m \text{ divides } nx\}, \\ &= (q), \quad \text{where } q = \frac{m}{\gcd(m, n)}.\end{aligned}$$

Here q is the greatest positive integer such that m divides qn (see Atiyah-MacDonald).

Exercise (Exercise 1.12; see Carlson)

- (i) $\mathfrak{a} \subseteq (\mathfrak{a} : \mathfrak{b})$.
- (ii) $(\mathfrak{a} : \mathfrak{b})\mathfrak{b} \subseteq \mathfrak{a}$.
- (iii) $((\mathfrak{a} : \mathfrak{b}) : \mathfrak{c}) = (\mathfrak{a} : \mathfrak{b}\mathfrak{c}) = ((\mathfrak{a} : \mathfrak{c}) : \mathfrak{b})$.
- (iv) $(\cap \mathfrak{a}_i : \mathfrak{b}) = \cap (\mathfrak{a}_i : \mathfrak{b})$.
- (v) $(\mathfrak{a} : \sum \mathfrak{b}_i) = \cap (\mathfrak{a} : \mathfrak{b}_i)$.

Operations on Ideals

Definition (Radical of an Ideal)

Let $\mathfrak{a}$ be an ideal of A . Its radical is

$$r(\mathfrak{a}) := \{x \in A; x^n \in \mathfrak{a} \text{ for some } n \geq 1\}.$$

Fact

If $\phi : A \rightarrow A/\mathfrak{a}$ is the canonical homomorphism, then $r(\mathfrak{a}) = \phi^{-1}(\mathfrak{N}_{A/\mathfrak{a}})$, where $\mathfrak{N}_{A/\mathfrak{a}}$ is the nilradical of $A/\mathfrak{a}$. In particular, $r(\mathfrak{a})$ is an ideal.

Proof.

We have

$$\begin{aligned} x \in r(\mathfrak{a}) &\iff x^n \in \mathfrak{a} \text{ for some } n, \\ &\iff \phi(x)^n = 0 \text{ for some } n, \\ &\iff \phi(x) \in \mathfrak{N}_{A/\mathfrak{a}} \iff x \in \phi^{-1}(\mathfrak{N}_{A/\mathfrak{a}}). \end{aligned}$$

This gives the result. □

Exercise (Exercise 1.13; see Carlson)

- (i) $r(\mathfrak{a}) \supseteq \mathfrak{a}$.
- (ii) $r(r(\mathfrak{a})) = r(\mathfrak{a})$.
- (iii) $r(\mathfrak{a}\mathfrak{b}) = r(\mathfrak{a} \cap \mathfrak{b}) = r(\mathfrak{a}) \cap r(\mathfrak{b})$.
- (iv) $r(\mathfrak{a}) = (1) \Leftrightarrow \mathfrak{a} = (1)$.
- (v) $r(\mathfrak{a} + \mathfrak{b}) = r(r(\mathfrak{a}) + r(\mathfrak{b}))$.
- (vi) If $\mathfrak{p}$ is prime, then $r(\mathfrak{p}^n) = \mathfrak{p}$ for all $n \geq 1$.

Operations on Ideals

Proposition (Proposition 1.14)

The radical $r(\mathfrak{a})$ is the intersection of the prime ideals that contains $\mathfrak{a}$.

Proof.

Let $\phi : A \rightarrow A/\mathfrak{a}$ be the canonical homomorphism.

- We know that

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

- By using Proposition 1.8 and Proposition 1.1* we get

$$\begin{aligned} r(\mathfrak{a}) &= \phi^{-1} \left(\bigcap \{ \bar{\mathfrak{p}}; \bar{\mathfrak{p}} \text{ prime ideal of } A/\mathfrak{a} \} \right) \\ &= \bigcap \{ \phi^{-1}(\bar{\mathfrak{p}}); \bar{\mathfrak{p}} \text{ prime ideal of } A/\mathfrak{a} \} \\ &= \bigcap \{ \mathfrak{p}; \mathfrak{p} \text{ prime ideal of } A \text{ containing } \mathfrak{a} \}. \end{aligned}$$

The proof is complete. □

Remark

Given any subset $E \subseteq A$ we may define its radical $r(E)$ as above. This is not an ideal in general (unless E is an ideal).

Fact

Given any family E_α of subsets of A , we have $r(\cup E_\alpha) = \cup r(E_\alpha)$.

Remark

Let D be the set of zero-divisors of A . We have

$$x \in D \iff xy = 0 \text{ for some } y \neq 0.$$

Thus,

$$(x \notin D \text{ and } xy = 0) \implies y = 0.$$

Operations on Ideals

Proposition (Proposition 1.15)

The set D of zero-divisors of A is equal to $\bigcup_{x \neq 0} r(\text{Ann}(x))$.

Proof.

- We claim that $r(D) = D$. We know that $D \subseteq r(D)$.
- Let $x \in r(D)$, i.e., $x^n \in D$ for some $n \geq 1$. Let n be the smallest such number.
 - Assume $n \geq 2$. Then $x \notin D$ and $x^{n-1} \notin D$.
 - As $x^n \in D$, there is $y \neq 0$ such that $0 = x^n y = x(x^{n-1}y)$.
 - As $x \notin D$, this implies that $x^{n-1}y = 0$, and so $x^{n-1} \in D$ (contradiction).

This shows that $x \in D$, and hence $r(D) \subseteq D$.

- By using the previous fact, we then get

$$D = r(D) = r\left(\bigcup_{x \neq 0} \text{Ann}(x)\right) = \bigcup_{x \neq 0} r(\text{Ann}(x)).$$

The result is proved. □

Example

$A = \mathbb{Z}$, $\mathfrak{a} = (m)$. Let $p_1, \dots, p_r$ be the prime divisors of m . Then

$$r(\mathfrak{a}) = (p_1 \cdots p_r) = \bigcap_{i=1}^r (p_i).$$

Proposition (Proposition 1.16)

If $\mathfrak{a}$ and $\mathfrak{b}$ are ideals of A such that $r(\mathfrak{a})$ and $r(\mathfrak{b})$ are coprime, then $\mathfrak{a}$ and $\mathfrak{b}$ are coprime.

Extension and Contraction

Let $f : A \rightarrow B$ be a ring homomorphism.

Fact

If $\mathfrak{a}$ is an ideal, then $f(\mathfrak{a})$ need not be an ideal.

Definition (Extension)

The extension $\mathfrak{a}^e$ of $\mathfrak{a}$ is the ideal $Bf(\mathfrak{a})$ generated by $\mathfrak{a}$. That is, $\mathfrak{a}^e$ consists of all finite sums $\sum y_i f(x_i)$ with $y_i \in B$ and $x_i \in \mathfrak{a}$.

Fact

If $\mathfrak{b}$ is an ideal of B , then $f^{-1}(\mathfrak{b})$ is an ideal of A .

Definition (Contraction)

$f^{-1}(\mathfrak{b})$ is called the contraction of $\mathfrak{b}$ and is denoted by $\mathfrak{b}^c$.

Extension and Contraction

Fact

If $\mathfrak{b}$ is prime, then its contraction $\mathfrak{b}^c$ is prime as well.

Proof.

If $\mathfrak{b}$ is prime, then

$$\begin{aligned} xy \in \mathfrak{b}^c &\iff f(xy) \in \mathfrak{b} \iff f(x)f(y) \in \mathfrak{b} \\ &\iff f(x) \in \mathfrak{b} \text{ or } f(y) \in \mathfrak{b} \\ &\iff x \in \mathfrak{b}^c \text{ or } y \in \mathfrak{b}^c. \end{aligned}$$

Thus, $\mathfrak{b}^c$ is a prime ideal. □

Fact

If $\mathfrak{a}$ is a prime ideal of A , then its extension $\mathfrak{b}^e$ need not be prime.

Example

Take $A = \mathbb{Z}$ and $B = \mathbb{Z}[i]$, where $i = \sqrt{-1}$.

- We have $(2)^e = (2\mathbb{Z})\mathbb{Z}[i] = 2\mathbb{Z}[i]$.
- However, $2\mathbb{Z}[i]$ is not prime, since

$$(1 + i) \notin 2\mathbb{Z}[i] \quad \text{and} \quad (1 + i)^2 = 2i \in 2\mathbb{Z}[i].$$

Definition

- C is the set of contracted ideals in A .
- E is the set of extended ideals in B .

Proposition (Proposition 1.17; see also Carlson)

- (i) $a \subseteq a^{ec}$ and $b \supseteq b^{ce}$.
- (ii) $a^e = a^{ece}$ and $b^c = b^{cec}$.
- (iii) $C = \{a; a^{ec} = a\}$, $E = \{b; b^{ce} = b\}$, and $a \rightarrow a^e$ is a bijection from C onto E with inverse $b \rightarrow b^c$.

Extension and Contraction

Proof of Proposition 1.17.

- For (i) we have

$$a^{ec} = f^{-1}(Bf(a)) \supseteq f^{-1}(f(a)) \supseteq a,$$

$$b^{ce} = Bf(f^{-1}(b)) \subseteq Bb = b.$$

- For (ii), by using (i) we get

$$a^e \subseteq (a^{ec})^e = (a^e)^{ce} \subseteq a^e.$$

Thus, $a^e = a^{ece}$. Likewise, $b^c = b^{cec}$.

- For (iii), set $C' = \{a; a^{ec} = a\}$ and $E' = \{b; b^{ce} = b\}$.
 - Clearly, $C' \subseteq C$ and $E' \subseteq E$.
 - If $a = b^c$, then $a^{ec} = b^{cec} = b^c = a$.
 - Thus, $C = C'$. Likewise $E = E'$.
 - (ii) implies that $a \rightarrow a^e$ is a bijection from $C' = C$ onto $E' = E$ with inverse $b \rightarrow b^c$.

The result is proved. □

Extension and Contraction

Exercise (Exercise 1.18; see Carlson)

- ① Let $\mathfrak{a}_1$ and $\mathfrak{a}_2$ be ideals of A and let $\mathfrak{b}_1$ and $\mathfrak{b}_2$ be ideals of B .

$$\begin{aligned}(\mathfrak{a}_1 + \mathfrak{a}_2)^e &= \mathfrak{a}_1^e + \mathfrak{a}_2^e, & (\mathfrak{b}_1 + \mathfrak{b}_2)^c &\supseteq \mathfrak{b}_1^c + \mathfrak{b}_2^c, \\(\mathfrak{a}_1 \cap \mathfrak{a}_2)^e &\subseteq \mathfrak{a}_1^e \cap \mathfrak{a}_2^e, & (\mathfrak{b}_1 \cap \mathfrak{b}_2)^c &= \mathfrak{b}_1^c \cap \mathfrak{b}_2^c, \\(\mathfrak{a}_1 \mathfrak{a}_2)^e &= \mathfrak{a}_1^e \mathfrak{a}_2^e, & (\mathfrak{b}_1 \mathfrak{b}_2)^c &\supseteq \mathfrak{b}_1^c \mathfrak{b}_2^c, \\(\mathfrak{a}_1 : \mathfrak{a}_2)^e &\subseteq (\mathfrak{a}_1^e : \mathfrak{a}_2^e), & (\mathfrak{b}_1 : \mathfrak{b}_2)^c &\subseteq (\mathfrak{b}_1^c : \mathfrak{b}_2^c), \\r(\mathfrak{a})^e &\subseteq r(\mathfrak{a}^e), & r(\mathfrak{b})^c &= r(\mathfrak{b}^c).\end{aligned}$$

- ② The set of extended ideals E is closed under sum and product.
- ③ The set of contracted ideals C is closed under the other three operations (intersection, ideal quotient and radical).

Remark

The fact that C is closed under ideal quotient follows from the equality $(\mathfrak{b}_1^c : \mathfrak{b}_2^c) = (\mathfrak{b}_1^{ce} : \mathfrak{b}_2^{ce})^c$ (see Carlson).

Prime Spectrum

Definition

The set of all prime ideals of A is called the *prime spectrum* of A and is denoted $\text{Spec}(A)$.

Notation

In what follows we set $X = \text{Spec}(A)$.

Definition

If $E \subseteq A$, then $V(E)$ is the set of prime ideals containing E .

Prime Spectrum. Zariski Topology

Proposition (Problem 1.15; see Carlson)

- ① If $\mathfrak{a}$ is the ideal generated by E , then

$$V(E) = V(\mathfrak{a}) = V(r(\mathfrak{a})).$$

- ② $V(0) = X$ and $V(1) = \emptyset$.

- ③ $V(\cup_{i \in I} E_i) = \cap_{i \in I} V(E_i)$.

- ④ If $\mathfrak{a}$ and $\mathfrak{b}$ are ideals, then

$$V(\mathfrak{a} \cap \mathfrak{b}) = V(\mathfrak{a}\mathfrak{b}) = V(\mathfrak{a}) \cup V(\mathfrak{b}).$$

Consequence

- The collection $\{V(E)\}$ satisfies the axioms for the closed sets in a topological space.
- That is, the collection $\{X \setminus V(E)\}$ is a topology on X .
- It is called the *Zariski topology*.

Remark (see Problem 1.17 and Carlson)

If $f \in A$, set $X_f = X \setminus V(f)$. Then:

- ① Each X_f is an open set in X .
- ② The X_f form a basis for the Zariski topology.
- ③ Each X_f is compact (i.e., every open covering has a finite sub-covering; see Carlson).
- ④ In particular, $X = X_1$ is compact (but it need not be Hausdorff).

Example ($X = \operatorname{Spec}(\mathbb{Z})$)

- We have

$$\operatorname{Spec}(\mathbb{Z}) = \{0\} \cup \{(p); p \in \mathbb{N}, \text{prime}\}.$$

- The closed sets are

$$\emptyset, \quad X, \quad \{(p_i); 1 \leq i \leq n\}.$$

- The closure of $\{0\}$ is X , and hence $\operatorname{Spec}(\mathbb{Z})$ is not Hausdorff (since $\{0\}$ is contained in every non-empty open set).
- 0 is called a *generic* point.

Example ($X = \text{Spec}(\mathbb{C}[x])$)

- We have

$$\begin{aligned}\text{Spec}(\mathbb{C}[x]) &= \{0\} \cup \{(x - \alpha); \alpha \in \mathbb{C}\}, \\ &\simeq \{(0)\} \cup \mathbb{C}.\end{aligned}$$

- The closed sets are

$$\emptyset, \quad X, \quad \{(x - \alpha_i); 1 \leq i \leq n\}.$$

- The closure of $\{0\}$ is X , and so X is not Hausdorff.

Example ($X = \operatorname{Spec}(\mathbb{R}[x])$)

- The irreducible polynomials on $\mathbb{R}$ are

$$x - \alpha, \quad \alpha \in \mathbb{R}, \quad \text{and} \quad (x - \beta)(x - \bar{\beta}), \quad \Im \beta > 0.$$

- We have

$$\operatorname{Spec}(\mathbb{R}[x]) = \{0\} \cup \mathbb{C} \cup \{\Im \beta > 0\}.$$