

# Atiyah-MacDonald: Rings and Ideals

James Pagan

January 2024

## Contents

<b>1</b>	<b>Rings</b>	<b>3</b>
1.1	Ring Axioms . . . . .	3
1.2	Subrings and Ideals . . . . .	4
1.3	Ring Homomorphisms . . . . .	5
1.4	Isomorphism Theorems . . . . .	7
1.5	Assorted Rings . . . . .	8
<b>2</b>	<b>Types of Ideals</b>	<b>9</b>
2.1	Principal Ideals . . . . .	9
2.2	Prime Ideals . . . . .	9
2.3	Maximal Ideals . . . . .	10
<b>3</b>	<b>Special Rings and Ideals</b>	<b>11</b>
3.1	Local Rings . . . . .	11
3.2	Principal Ideal Domain . . . . .	12
3.3	The Nilradical . . . . .	12
3.4	The Jacobson Radical . . . . .	14
<b>4</b>	<b>Operations on Rings and Ideals</b>	<b>14</b>
4.1	Sum, Intersection, Product . . . . .	14
4.2	Relatively Prime Ideals . . . . .	14

4.3	Direct Product of Rings . . . . .	15
4.4	Inclusion and Prime Ideals . . . . .	16
4.5	The Ideal Quotient . . . . .	17
4.6	Radicals of Ideals . . . . .	19
4.7	Extension and Contraction . . . . .	21
<b>5</b>	<b>The Zariski Topology</b>	<b>22</b>
5.1	Definition . . . . .	22

# 1 Rings

## 1.1 Ring Axioms

A **ring**  $R$  is a set endowed with two binary operations, here denoted “+” and “ $\times$ ”, such that if  $a, b, c \in R$ , the following ten axioms are satisfied:

- **Additive Axioms**

1. **Closure:**  $a + b \in R$ .
2. **Associativity:**  $a + (b + c) = (a + b) + c$ .
3. **Identity:** There is  $0 \in R$  such that  $a + 0 = 0 + a = a$ .
4. **Invertability:** There is  $-a \in R$  such that  $a + (-a) = (-a) + a = 0$ .
5. **Commutativity:**  $a + b = b + a$ .

- **Multiplicative Axioms**

6. **Closure:**  $ab \in R$ .
7. **Associativity:**  $a(bc) = (ab)c$ .
8. **Identity:** There is  $1 \in R$  such that  $a1 = 1a = a$ .

- **Distributive Axioms**

9. **Left Distributivity:**  $a(b + c) = ab + ac$ .
10. **Right Distributivity:**  $(a + b)c = ac + bc$ .

Since  $(R, +)$  is an Abelian group, the following properties hold for  $a, b \in R$ : the additive identity  $0$  is unique, the additive inverse  $-a$  is unique,  $-(-a) = a$ , and  $-(a + b) = -a - b$ .

**Theorem 1.** *The following properties hold for any ring  $R$  and  $a, b \in R$ :*

1.  $1$  is the unique multiplicative inverse of  $R$ .
2. If  $a$  has a multiplicative inverse  $a^{-1}$ , it is unique.
3.  $a0 = 0a = a$ .
4.  $-a = (-1)a$ .
5.  $a(-b) = (-a)b = -ab$ .
6.  $(-a)(-b) = ab$ .

*Proof.* (1) and (2) follow from the monoid/group axioms. For the rest:

3. As  $0 + 0 = 0$ , we have that  $a0 = a(0 + 0) = a0 + a0$ ; subtracting by  $a0$  yields  $a0 = 0$ . Similarly,  $0a = 0$ .

4. We have that

$$(-1)a + a = (-1)a + 1a = (-1 + 1)a = 0a = 0,$$

so  $(-1)a = -a$ .

5. See that

$$a(-b) + ab = a(-b + b) = a0 = 0,$$

so  $a(-b) = -ab$ . Similarly,  $(-a)b = -ab$ .

6. Using (5), we find that

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

as desired.

This yields the desired six properties. □

## 1.2 Subrings and Ideals

A **subring**  $R'$  of  $R$  is a subset of  $R$  that is also a ring. This relation is denoted  $R' \subseteq R$ .

**Theorem 2.** *A subset  $R'$  of  $R$  is a subring if it is nonempty, closed under addition and multiplication, contains additive inverses, and contains the multiplicative identity.*

*Proof.* The conditions that  $(R', +)$  is nonempty, closed, and contains inverses ensures that it is a group. Note that  $(R', \times)$  is closed and contains the multiplicative identity.

The final properties are implied by the fact  $R'$  is a subset of  $R$ ; all the elements of  $R'$  satisfy both associative and distributive laws, plus additive commutativity. We deduce that  $R'$  is a subring. □

All rings contain at least two subrings: the 0 ring and  $R$  itself.

A **ideal**  $\mathfrak{a}$  of  $R$  is a subset of  $R$  that satisfies the following two properties:

1. **Additive:**  $\mathfrak{a}$  is an additive subgroup of  $R$ .
2. **Multiplicative:** For all  $a \in \mathfrak{a}$  and  $x \in R$ , we have  $ax, xa \in \mathfrak{a}$ .

All rings contain at least two ideals: one is  $R$  itself, one is a maximal ideal (Section 2.3).

**Theorem 3.** *If  $R'$  is both a subring and an ideal of  $R$  if and only if  $R'$  is  $R$  or  $0$ .*

*Proof.* Suppose that  $R' \neq 0$  is both a subring and an ideal of  $R$ . As  $R'$  is a subring,  $1 \in R'$ ; as  $R'$  is an ideal,  $a = a1 \in R'$  for all  $a \in R$ . Then  $R' = R$ . Clearly,  $R$  itself and  $0$  are both ideals and subrings — which yields the desired result.  $\square$

### 1.3 Ring Homomorphisms

A **ring homomorphism** between two rings  $R$  and  $R'$  is a mapping  $\phi : R \rightarrow R'$  such that for all  $a, b \in R$ ,

$$\begin{aligned}\phi(a + b) &= \phi(a) + \phi(b) \\ \phi(ab) &= \phi(a)\phi(b) \\ \phi(1) &= 1.\end{aligned}$$

By the group axioms,  $\phi(-a) = -\phi(a)$  and  $\phi(0) = 0$  for all  $a \in R$ . If  $a$  has a multiplicative inverse  $a^{-1}$ , then  $\phi(a^{-1}) = \phi(a)^{-1}$ .

The **image** of  $R$  under  $\phi$  is the set  $\{\phi(a) \mid a \in R\}$ , and is denoted  $\phi(R)$ .

**Theorem 4.** *The image of any ring homomorphism  $\phi : R \rightarrow R'$  is a subring of  $R'$ .*

*Proof.* Realize that  $\phi(R)$  is nonempty, and for all  $\phi(a), \phi(b) \in \phi(R)$ , we have that

1.  $\phi(a) + \phi(b) = \phi(ab) \in \phi(R)$ .
2.  $\phi(a)\phi(b) = \phi(ab) \in \phi(R)$ .
3.  $-\phi(a) = \phi(-a) \in \phi(R)$ .
4.  $\phi(1) \in \phi(R)$ .

Hence,  $\phi(R)$  is a subring of  $R'$ .  $\square$

The **kernel** of  $R$  under  $\phi$  is the set  $\{a \in R \mid \phi(r) = 0\}$  and is denoted  $\text{Ker } \phi$ .

**Theorem 5.**  $\text{Ker } \phi$  is an ideal of  $R$ .

*Proof.* Since  $\phi$  is a homomorphism of the Abelian groups  $(R, +)$  and  $(R', +)$ , the kernel of  $\phi$  is an Abelian group with respect to addition. We need only verify the multiplicative condition; for all  $a \in R$  and  $k \in \text{Ker } \phi$ ,

$$\phi(ak) = \phi(a)\phi(k) = 0\phi(a) = 0 = \phi(a)0 = \phi(a)\phi(k) = \phi(ak).$$

Then  $ak \in \text{Ker } \phi$ . Thus,  $\text{Ker } \phi$  is an ideal. □

Categories of group homomorphisms — like monomorphisms, epimorphisms, isomorphisms, endomorphisms, automorphisms — have equivalent formulations for ring homomorphisms. An isomorphism between  $R$  and  $R'$  is denoted the same as groups:

$$R \cong R'.$$

We can extend the notion of a quotient group to a ring  $R$  with an ideal  $\mathfrak{a}$  as follows, yielding a **quotient ideal**:

**Theorem 6.** *The quotient group  $R/\mathfrak{a}$  is a ring under the product  $(a+\mathfrak{a})(b+\mathfrak{a}) = ab+\mathfrak{a}$  for  $a, b \in R$ .*

*Proof.* The quotient group  $R/\mathfrak{a}$  exists, since  $\mathfrak{a}$  is an additive subgroup of  $R$  and all subgroups of Abelian groups are normal. We must demonstrate that the product is well-defined.

Suppose  $a + \mathfrak{a} = a' + \mathfrak{a}$  and  $b + \mathfrak{a} = b' + \mathfrak{a}$ . Then since  $a - a' \in \mathfrak{a}$  and  $b - b' \in \mathfrak{a}$ ,

$$ab - a'b \in \mathfrak{a} \quad \text{and} \quad a'b - a'b' \in \mathfrak{a}.$$

Thus,  $ab - a'b' \in \mathfrak{a}$  and  $ab + \mathfrak{a} = a'b' + \mathfrak{a}$ . Then the product is well-defined. Proving that the product is closed and associative is trivial; the multiplicative identity of  $R/\mathfrak{a}$  is  $1 + \mathfrak{a}$ , and the distributivity with addition is trivial — so  $R/\mathfrak{a}$  is a ring. □

The canonical mapping  $\phi : R \rightarrow R/\mathfrak{a}$  is thus a surjective homomomorphism with kernel  $\mathfrak{a}$ . A similar definition exists for the quotient of two ideals — say,  $\mathfrak{a}/\mathfrak{b}$  for  $\mathfrak{a} \supseteq \mathfrak{b}$ .

## 1.4 Isomorphism Theorems

All three Isomorphism Theorems and the Correspondence Theorem have their equivalencies for rings.

**Theorem 7** (First Isomorphism Theorem). *For all homomorphisms  $\phi : R \rightarrow R'$  with kernel  $\mathfrak{k}$ ,*

$$R / \mathfrak{k} \cong \phi(R)$$

*by the mapping  $\psi(a + \mathfrak{k}) = \phi(a)$ .*

*Proof.* We must first demonstrate that  $\psi$  is a homomorphism. If  $a, b \in R$ , then the following three identities hold:

1.  $\psi(a + b + \mathfrak{k}) = \phi(a + b) = \phi(a) + \phi(b) = \psi(a + \mathfrak{k}) + \psi(b + \mathfrak{k})$ .
2.  $\psi(ab + \mathfrak{k}) = \phi(ab) = \phi(a)\phi(b) = \psi(a + \mathfrak{k})\psi(b + \mathfrak{k})$ .
3.  $\psi(1 + \mathfrak{k}) = \phi(1)$ .

Thus,  $\psi$  is a homomorphism. For all  $\phi(a) \in \phi(R)$ , realize that  $\psi(a + \mathfrak{k}) = \phi(a)$ ; thus  $\psi$  is surjective. Finally, let  $\psi(a + \mathfrak{k}) = \psi(b + \mathfrak{k})$ ; then  $\phi(a) = \phi(b)$ , so

$$\phi(a - b) = \phi(a) - \phi(b) = 0.$$

Hence,  $a - b \in \mathfrak{k}$  and  $a + \mathfrak{k} = b + \mathfrak{k}$ . We conclude that  $\psi$  is injective, implying the desired isomorphism.  $\square$

The Correspondence Theorem expands upon the result of the First Isomorphism Theorem.

**Theorem 8** (Correspondence Theorem). *There is a one-to-one correspondence between ideals of  $\phi(R)$  and ideals of  $R$  that contain  $\mathfrak{k}$ .*

*Proof.* For an ideal  $\mathfrak{a}'$  of  $\phi(R)$ , define  $\mathfrak{a} = \{a \in R \mid \phi(a) \in \mathfrak{a}'\}$ . By the Correspondence Theorem for groups,  $\mathfrak{a}$  is an additive subgroup of  $R$ . For all  $a \in \mathfrak{a}$  and  $b \in R$ , we have  $\phi(a) \in \mathfrak{a}'$ ; thus

$$\phi(ab) = \phi(a)\phi(b) \in \mathfrak{a}'$$

since  $\mathfrak{a}'$  is an ideal. Thus  $ab \in \mathfrak{a}$ , so  $\mathfrak{a}$  is an ideal of  $R$ . Since  $0 \in R'$ , we have that  $\mathfrak{k}$  is a subideal of  $\mathfrak{a}$ . It is now relatively trivial to establish a one-to-one correspondence.  $\square$

**Corollary 1.** *There is a one-to-one correspondence between ideals of  $R / \mathfrak{a}$  and ideals of  $R$  that contain  $\mathfrak{a}$ .*

The two remaining Isomorphism Theorems will be proven at another time.

## 1.5 Assorted Rings

We will consider the following three types of rings in this section:

1. A **commutative ring** is a ring  $R$  such that  $ab = ba$  for all  $a, b \in R$ .
2. An **integral domain** is a nonzero commutative ring  $R$  such that  $ab = 0$  implies  $a = 0$  or  $b = 0$  for all  $a, b \in R$ .
3. A **field** is a commutative division ring.

Note that integral domains and fields must be nonzero. **Henceforth, all rings we shall define are commutative unless stated otherwise.**

**Theorem 9.** *All finite domains are fields.*

*Proof.* Let  $R$  be a finite domain. Then for nonzero  $a \in R$ , consider the set

$$\{a, a^2, \dots, a^{|R|+1}\}.$$

By the Pigeonhole Principle, two elements of this set must be equal:  $a^i = a^j$  for  $i, j \in \{1, \dots, n\}$  with  $i < j$ . Thus  $a^j(a^{i-j} - 1) = 0$ , so  $a^{i-j} = 1$  and  $a^{i-j-1} = a^{-1}$ . Since all nonzero elements of  $R$  are invertible, we conclude that  $R$  is a field.  $\square$

**Theorem 10.**  *$R$  is a field if and only if the only ideals of  $R$  are  $0$  and  $R$  itself.*

*Proof.* Let  $R$  be a field and let  $\mathfrak{a}$  be nonzero ideal of  $R$ . Then for  $a \in \mathfrak{a}$ ,

$$R = (a) \subseteq \mathfrak{a} \subseteq R.$$

Thus,  $\mathfrak{a} = R$ . Now, suppose that the only ideals of  $R$  are  $0$  and  $R$  itself; then for all nonzero  $a \in R$ ,

$$(a) = R,$$

where  $(a)$  denotes the principal ideal (Section 2.1). Thus, there exists  $a^{-1} \in R$  such that  $aa^{-1} = 1$ , so  $R$  is a field.  $\square$

An element  $a \in R$  is a **unit** if it is invertible. It is trivial to verify that all the units of  $R$  constitute a multiplicative Abelian group (non-units form a commutative semigroup!)



## 2 Types of Ideals

### 2.1 Principal Ideals

For an  $x \in R$ , the **principal ideal** of  $x$  is the ideal given by  $(x) = \{ax \mid a \in R\}$ . We may alternatively denote  $(x)$  by  $Rx$ .

**Theorem 11.** *Principal ideals are ideals.*

*Proof.* Let  $x$  be any element of  $R$ . We must perform two rather routine calculations:

1. **Additivity:** For all  $ax, bx \in (x)$ , we have that  $ax + bx = (a + b)x \in (x)$ .
2. **Multiplicativity:** For all  $ax \in (x)$  and  $b \in R$  we have  $b(ax) = (ba)x \in (x)$ .

We conclude that  $(x)$  is an ideal. □

The principal ideal is the smallest ideal that contains  $(x)$ , in the following sense: if  $x \in \mathfrak{a}$  for an ideal  $\mathfrak{a}$  of  $R$ , then  $rx \in \mathfrak{a}$  for all  $a \in R$ , so  $(x) \subseteq \mathfrak{a}$ .

**Theorem 12.**  $(x) = R$  for  $x \in R$  if and only if  $x$  is a unit.

*Proof.* Suppose that  $(x) = R$ . Then  $1 \in (x)$ , so there exists  $x^{-1} \in R$  such that  $xx^{-1} = x^{-1}x = 1$ ;  $x$  is a unit. If we suppose that  $x$  is a unit, then  $x \in (x)$  implies  $1 = x^{-1}x \in (x)$  implies  $a = a1 \in (x)$  for all  $a \in R$ ; thus  $(x) = R$ . □

### 2.2 Prime Ideals

A **prime ideal**  $\mathfrak{p}$  of  $R$  is a principal ideal such that  $ab \in \mathfrak{p}$  implies  $a \in \mathfrak{p}$  or  $b \in \mathfrak{p}$ . This condition generalizes to a finite amount of elements;  $a_1 \cdots a_n \in \mathfrak{p}$  if and only if  $a_i \in \mathfrak{p}$  for some  $i$ .

**Theorem 13.** *An ideal  $\mathfrak{p}$  of  $R$  is prime if and only if  $R/\mathfrak{p}$  is an integral domain.*

*Proof.* Suppose that  $\mathfrak{p}$  is prime, and define  $\phi : R \rightarrow R/\mathfrak{p}$  by  $\phi(a) = a + \mathfrak{p}$ . Since the kernel of  $\phi$  is  $\mathfrak{p}$ , we have that

$$\phi(ab) = 0 \implies ab \in \mathfrak{p} \implies a \in \mathfrak{p} \text{ or } b \in \mathfrak{p} \implies \phi(a) = 0 \text{ or } \phi(b) = 0.$$

Conversely, suppose that  $R/\mathfrak{p}$  is an integral domain. Then

$$ab \in \mathfrak{p} \implies \phi(ab) = 0 \implies \phi(a) = 0 \text{ or } \phi(b) = 0 \implies a \in \mathfrak{p} \text{ or } b \in \mathfrak{p}.$$

This completes the proof.  $\square$

### 2.3 Maximal Ideals

A **maximal ideal**  $\mathfrak{m}$  of  $R$  is a proper ideal such that the only ideals of  $R$  that contain  $\mathfrak{m}$  are itself and  $R$ . Maximal ideals (along with prime and proper ideals) need not be mutually exclusive; they do not partition the non-units of  $R$ .

**Theorem 14.** *An ideal  $\mathfrak{m}$  of  $R$  is maximal if and only if  $R/\mathfrak{m}$  is a field.*

*Proof.* By the Correspondence Theorem, there is a one-to-one correspondence between ideals of  $R$  that contain  $\mathfrak{m}$  and ideals of  $R/\mathfrak{m}$ . Then using Theorem 10,

$$\begin{aligned} \mathfrak{m} \text{ is maximal} &\iff \text{The only ideals of } R/\mathfrak{m} \text{ are } (0) \text{ and } R/\mathfrak{m} \text{ itself.} \\ &\iff R/\mathfrak{m} \text{ is a field,} \end{aligned}$$

yielding the desired result  $\square$

All maximal ideals are prime. The following theorem ensures a wealth of maximal ideals:

**Theorem 15** (Krull's Theorem). *Every nonzero ring has a maximal ideal.*

*Proof.* The set of all proper ideals under  $\subseteq$  forms a partially ordered set — it is nonempty, as  $(0)$  is an ideal. To construct upper bounds, define  $(\mathfrak{a}_n)$  as a chain of ideals such that for indices  $\alpha$  and  $\beta$ , we have  $\mathfrak{a}_\alpha \subseteq \mathfrak{a}_\beta$  or  $\mathfrak{a}_\alpha \supseteq \mathfrak{a}_\beta$ .

**Claim 1.**  $\bigcup \mathfrak{a}_n$  is an ideal.

*Proof.* We must perform two rather routine calculations:

1. **Additivity:** If  $x, y \in \bigcup \mathfrak{a}_n$ , let  $x \in \mathfrak{a}_\alpha$  and  $y \in \mathfrak{a}_\beta$  for indices  $\alpha$  and  $\beta$ . Without loss of generality, let  $\mathfrak{a}_\alpha \subseteq \mathfrak{a}_\beta$ ; then  $x \in \mathfrak{a}_\beta$ . Thus  $x + y \in \mathfrak{a}_\beta \subseteq \bigcup \mathfrak{a}_n$ .
2. **Multiplicativity:** Suppose  $x \in \bigcup \mathfrak{a}_n$  and  $a \in R$ . Then  $x \in \mathfrak{a}_\alpha$  for some index; we have  $ax \in \mathfrak{a}_\alpha \subseteq \bigcup \mathfrak{a}_n$ .

We deduce that  $\bigcup \mathfrak{a}_n$  is an ideal.

Zorn's Lemma thus applies. The set of all proper ideals contains a maximal element with respect to inclusion — namely, a maximal ideal.  $\square$

Two corollaries follow from Krull's Theorem:

**Corollary 2.** *All proper ideals  $\mathfrak{a}$  are contained within some maximal ideal  $\mathfrak{m}$ .*

*Proof.* If  $\mathfrak{a}$  is a proper ideal, then the quotient ring  $R/\mathfrak{a}$  is nonzero — hence it contains a maximal ideal  $\mathfrak{a}'$ . By the Correspondence Theorem, there exists a corresponding ideal  $\mathfrak{a}$  in  $R$  that contains  $\mathfrak{a}$ . The maximality of  $\mathfrak{m}$  is ensured by the maximality of  $\mathfrak{m}'$  (say, via a contradiction argument).  $\square$

**Corollary 3.** *Each non-unit  $a \in R$  lies within some maximal ideal of  $R$ .*

### 3 Special Rings and Ideals

#### 3.1 Local Rings

A **local ring** is a ring with exactly one maximal ideal. They may have an arbitrary number of prime ideals. The following two theorems test whether  $R$  is local with maximal ideal  $\mathfrak{m}$ :

**Theorem 16.**  *$R$  is a local ring if and only if  $R - \mathfrak{m}$  consists of units.*

*Proof.* Suppose that  $R - \mathfrak{m}$  consists of units. Then  $\mathfrak{m}$  constitutes all units of  $R$ ; as all ideals are composed of non-units, ideals of  $R$  must lie within  $\mathfrak{m}$ . Then  $\mathfrak{m}$  is the sole maximal ideal of the local ring  $R$ .

Suppose that  $R - \mathfrak{m}$  contains a non-unit  $a \in R$ . Then  $(a)$  is a proper ideal, and lies within some maximal ideal  $\mathfrak{n}$ . As  $a \in \mathfrak{n}$  and  $a \notin \mathfrak{m}$ , the ring  $R$  has two maximal ideals and is not local.  $\square$

**Theorem 17.**  *$R$  is a local ring if and only if  $\mathfrak{m} + 1$  consists of units for maximal  $\mathfrak{m}$ .*

*Proof.* Suppose that  $R$  is a local ring. Then if  $m \in \mathfrak{m}$ , we must have  $m + 1 \notin \mathfrak{m}$ ; otherwise,  $1 \in \mathfrak{m}$  implies that  $\mathfrak{m}$  is not a proper ideal. Hence,  $\mathfrak{m} + 1 \subseteq R - \mathfrak{m}$ , so  $\mathfrak{m} + 1$  consists of units.

Suppose that  $\mathfrak{m} + 1$  consists of units for maximal  $\mathfrak{m}$ . Let  $a \notin \mathfrak{m}$ ; then  $(a) + \mathfrak{m} = R$ , so there exists  $ab \in (a)$  and  $m \in \mathfrak{m}$  such that  $ab + m = 1$ . Then  $1 - m$  is a unit, so

$$R = (1 - m) = (ab) \subseteq (a) \subseteq R$$

We deduce that  $(a) = R$ , so  $a$  is a unit. As  $R - \mathfrak{m}$  consists of non-units, Theorem 16 implies that  $R$  is a local ring with maximal ideal  $\mathfrak{m}$ .  $\square$

A **semilocal ring** is a ring with a finite number of maximal ideals.

## 3.2 Principal Ideal Domain

A **principal ideal domain** is an integral domain in which all ideals are principal.

**Theorem 18.** *Let  $R$  be a principal ideal domain. Then all nonzero prime ideals of  $R$  are maximal.*

*Proof.* Let  $(a) \neq 0$  be prime and define  $(b)$  as the maximal ideal that contains  $(a)$ . Then  $a \in (b)$ , so there exists  $x \in R$  such that  $a = bx$ . We have  $bx \in (a)$ ; then either  $b \in (a)$  or  $x \in (a)$ .

Suppose for contradiction that  $x \in (a)$ . Then there exists  $y \in R$  such that  $x = ay$ ; substituting this into our earlier equation,

$$a = b(ay) \implies a(1 - by) = 0.$$

Since  $R$  is an integral domain — and since  $a \neq 0$  — we must have  $1 = by$ . Then  $b$  is a unit, so  $(b) = R$ ; this contradicts the fact that the maximal ideal  $(b)$  is proper.

Thus,  $b \in (a)$  and  $(a) = (b)$ . We conclude that  $(a)$  is maximal.  $\square$

These domains are unique factorization domains, and thus the techniques discussed in AbstractAlgebra/artin12.tex apply.

## 3.3 The Nilradical

An element  $a \in R$  is a **zero divisor** if there exists nonzero  $b \in R$  such that  $ab = 0$ . A zero divisor  $a$  is **nilpotent** if  $a^n = 0$  for some positive integer  $n$ . the set of all nonzero nilpotent elements of  $R$  is called the **nilradical** of  $R$ , often denoted by  $\mathfrak{N}$ .

**Theorem 19.** *The nilradical  $\mathfrak{N}$  of  $R$  is ideal of  $R$ .*

*Proof.* First, we must verify that  $\mathfrak{N}$  is an additive subgroup of  $R$ . Since  $0 \in \mathfrak{N}$ , we need only verify two conditions:

1. **Closure:** For  $a, b \in \mathfrak{N}$ , let  $n, m \in \mathbb{Z}$  such that  $a^n = b^m = 0$ . Then

$$(ab)^{nm} = a^{nm}b^{nm} = (a^n)^m(b^m)^n = 0^m 0^n = 0,$$

so  $ab \in \mathfrak{N}$ .

2. **Inverses:** If  $a^n = 0$ , then  $(-a)^n = 0$  as well; thus  $-a \in \mathfrak{N}$ .

Now, we need only verify the multiplicative condition. For  $a \in \mathfrak{A}$ , define  $n \in \mathbb{Z}$  such that  $a^n = 0$ ; then for all  $b \in R$ ,

$$(ab)^n = a^n b^n = 0b^n = 0,$$

so  $ab \in \mathfrak{A}$ . We deduce that  $\mathfrak{A}$  is an ideal. □

The following proof is my favorite in this document:

**Theorem 20.** *The nilradical  $\mathfrak{A}$  of a commutative ring  $R$  is the intersection of all the prime ideals of  $R$ .*

*Proof.* Suppose  $a^n = 0$  and  $\mathfrak{p}$  is a prime ideal of  $R$ . Then  $a^n \in \mathfrak{p}$ , so one of  $aa \cdots a$  must be in  $\mathfrak{p}$  (the prime condition inducts!).

Now, suppose that  $a^n \neq 0$  for all  $n \in \mathbb{Z}_{>0}$ . Let  $S$  be the set of all ideals  $\mathfrak{a}$  such that  $a^n \notin \mathfrak{a}$  for all  $n \in \mathbb{Z}_{>0}$ . This set is nonempty, since  $0 \in S$ ; then  $S$  is a partially ordered set under inclusion.

Using identical logic as in Theorem 15, we deduce that this set must have a maximal element  $\mathfrak{p}$  — however,  $\mathfrak{p}$  may not be maximal in the scale of *all* ideals of  $R$ .

**Claim 2.**  *$\mathfrak{p}$  is a prime ideal of  $R$ .*

*Proof.* Suppose  $b, c \notin \mathfrak{p}$ . Then  $(b) + \mathfrak{p}$  and  $(c) + \mathfrak{p}$  are ideals that contain  $\mathfrak{p}$ , so they do not lie within  $S$ . Then they contain a power of  $a$ ; for some  $m, n \in \mathbb{Z}_{>0}$ , for some  $x, y \in R$ , and for some  $p_1, p_2$  in  $\mathfrak{p}$ ,

$$a^m = bx + p_1 \quad \text{and} \quad a^n = cy + p_2.$$

Then  $a^{mn} = bcxy + bxp_2 + cyp_1 + p_1p_2$ . As  $\mathfrak{p}$  is an ideal, the entire expression  $bxp_2 + cyp_1 + p_1p_2$  lies within  $\mathfrak{p}$ ; thus  $a^{mn} \in (bc) + \mathfrak{p}$ . Then  $(bc) + \mathfrak{p}$  cannot lie within  $S$ ; thus  $bc \notin \mathfrak{p}$ .

Taking the contrapositive yields that  $bc \in \mathfrak{p}$  implies  $b \in \mathfrak{p}$  or  $c \in \mathfrak{p}$ .

Then as  $a$  is absent from the prime ideal  $\mathfrak{p}$ , it cannot lie within the intersection of all the prime ideals of  $R$ . □

If  $R$  is an integral domain, then  $\mathfrak{A}$  is the zero ideal.

### 3.4 The Jacobson Radical

The **Jacobson radical**  $\mathfrak{J}$  is the intersection of all the maximal ideals of  $R$ . As an intersection of ideals,  $\mathfrak{J}$  is an ideal (Section 4.1) — so it is a subideal of the nilradical.

**Theorem 21.**  *$j$  lies in the Jacobson radical  $\mathfrak{J}$  if and only if  $1 - ja$  is a unit across all  $a \in R$ .*

*Proof.* Suppose that there  $b \in R$  such that  $1 - jb$  is not a unit. Then there is a maximal ideal  $\mathfrak{m}$  that contains  $(1 - jb)$ ; such an ideal cannot contain  $b$ , or else it contains  $jb$  and thus 1. Hence  $b \notin \mathfrak{J}$ .

Suppose that  $j$  is not in the Jacobson radical. Then  $j \notin \mathfrak{m}$  for some maximal ideal  $\mathfrak{m}$  of  $R$ ; thus  $(j) + \mathfrak{m} = R$ , so there exists  $b \in R$  such that  $jb + m = 1$  for an arbitrary nonzero  $m \in M$ . Then  $1 - jb \in \mathfrak{m}$ , so it cannot be a unit.

Taking the contrapositive yields the desired result.  $\square$

## 4 Operations on Rings and Ideals

### 4.1 Sum, Intersection, Product

If  $\mathfrak{a}$  and  $\mathfrak{b}$  are ideals of a ring  $R$ , we may perform the following operations upon them to yield three new ideals.

1. **Sum:**  $\mathfrak{a} + \mathfrak{b} = \{a + b \mid a \in \mathfrak{a}, b \in \mathfrak{b}\}$ , the smallest ideal of  $R$  that contains  $\mathfrak{a}$  and  $\mathfrak{b}$ .
2. **Intersection:**  $\mathfrak{a} \cap \mathfrak{b}$ , the largest ideal of  $R$  contained within both  $\mathfrak{a}$  and  $\mathfrak{b}$ . In fact an infinite intesection of ideals is an ideal.
3. **Product:**  $\mathfrak{a}\mathfrak{b} = \{\sum a_i b_i \mid a_i \in \mathfrak{a}, b_i \in \mathfrak{b}\}$ . We denote  $\mathfrak{a}\mathfrak{a} \cdots \mathfrak{a}$  as  $\mathfrak{a}^n$  and set  $\mathfrak{a}^0 = R$ .

Ideals under sums and intersections form a complete lattice. Sums may be infinite; products must be finite. All of the above are commutative and associative; products and sums of ideals satisfy the distributive law.  $\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{a} \cap \mathfrak{b}$ , with equality if  $\mathfrak{a} + \mathfrak{b} = R$  (Theorem 22).

### 4.2 Relatively Prime Ideals

Two ideals  $\mathfrak{a}$  and  $\mathfrak{b}$  are **relatively prime** if  $\mathfrak{a} + \mathfrak{b} = R$ . Clearly, this holds if and only if there exists  $a \in \mathfrak{a}$  and  $b \in \mathfrak{b}$  such that  $a + b = 1$ .

We have invokea facts about relatively prime ideals several times thus far throughout this document — notably that if  $\mathfrak{m}$  is maximal and  $a \notin \mathfrak{m}$ , then  $\mathfrak{m} + (a) = R$ .

**Theorem 22.** Let  $\mathfrak{a}_1, \dots, \mathfrak{a}_n$  be ideals of  $R$ . If  $\mathfrak{a}_i$  and  $\mathfrak{a}_j$  are coprime whenever  $i \neq j$ , then  $\prod \mathfrak{a}_i = \cap \mathfrak{a}_i$

*Proof. Base case:* Consider ideals  $\mathfrak{a}$  and  $\mathfrak{b}$  of  $R$ . and let  $ab \in \mathfrak{a}\mathfrak{b}$ . Then as  $\mathfrak{a}$  is an ideal,  $ab \in \mathfrak{a}$ ; likewise,  $ab \in \mathfrak{b}$ . Then  $ab \in \mathfrak{a} \cap \mathfrak{b}$ . Now if  $x \in \mathfrak{a} \cap \mathfrak{b}$ , then  $x \in \mathfrak{a}$  and  $x \in \mathfrak{b}$ . Let  $a + b = 1$ ; then  $xa \in \mathfrak{b}\mathfrak{a}$  and  $xb \in \mathfrak{a}\mathfrak{b}$ , so  $x = xa + xb \in \mathfrak{a}\mathfrak{b}$ . We conclude that  $\mathfrak{a}\mathfrak{b} = \mathfrak{a} \cap \mathfrak{b}$  (this proof is wrong,  $\mathfrak{a}\mathfrak{b}$  consists of sums).

**Inductive step:** Let the theorem be true for  $n$ ; we wish to prove that if  $\mathfrak{a}_1, \dots, \mathfrak{a}_n, \mathfrak{b}$  are all pairwise coprime, then

$$\left( \bigcup_{i=1}^n \mathfrak{a}_i \right) \mathfrak{b} = \left( \bigcup_{i=1}^n \mathfrak{a}_i \right) \cap \mathfrak{b}$$

We have a sequence of equations from  $a_1 + b_1 = 1$  to  $a_n + b_n = 1$ , where  $a_i \in \mathfrak{a}_i$  and  $b_i \in \mathfrak{b}$  ( $i \in \{1, \dots, n\}$ ). We argue by cosets:

$$\left( \prod_{x=1}^n a_i \right) + \mathfrak{b} = \left( \prod_{x=1}^n (1 - b_i) \right) + \mathfrak{b} = 1 + \mathfrak{b}.$$

Thus there exists  $b \in \mathfrak{b}$  such that  $a_1 \cdots a_n + b = 1$ ; thus  $\mathfrak{b}$  is coprime to  $\prod \mathfrak{a}_i$ , which implies the given result by the base case.  $\square$

A rather trivial result is that if  $\mathfrak{a}_1, \dots, \mathfrak{a}_n$  are principal ideals, then their product is the ideal of all products  $a_1 \cdots a_n$  — no summations required.

### 4.3 Direct Product of Rings

For rings  $R_1, \dots, R_n$ , their **direct product**

$$R = \prod_{i=1}^n R_i$$

is the set of all sequences  $\bar{a} = (a_1, \dots, a_n)$  with  $a_i \in R_i$  for  $i \in \{1, \dots, n\}$ , endowed with componentwise addition and multiplication. It is a commutative ring; the mappings  $\phi : R \rightarrow R_i$  defined by  $\phi(a_1, \dots, a_n)$  are homomorphisms.

In the following theorem, let  $R$  be a ring with ideals  $\mathfrak{a}_1, \dots, \mathfrak{a}_n$ ; define a homomorphism

$$\phi : R \rightarrow \prod_{i=1}^n R / \mathfrak{a}_i$$

by  $\phi(a) = (a + \mathfrak{a}_1, \dots, a + \mathfrak{a}_n)$ .

**Theorem 23.** *The following two properties of  $\phi$  hold:*

1.  *$\phi$  is injective if and only if  $\cap \mathfrak{a}_i = 0$ .*
2.  *$\phi$  is surjective if and only if  $\mathfrak{a}_i$  and  $\mathfrak{a}_j$  are relatively prime whenever  $i \neq j$ .*

*Proof.* For (1), the following sequence of claims is easy to verify:

$$\begin{aligned} k \in \text{Ker } \phi &\iff \phi(k) = 0 \\ &\iff k \in \mathfrak{a}_i \text{ for each } i \in \{1, \dots, n\} \\ &\iff k \in \mathfrak{a}_1 \cap \dots \cap \mathfrak{a}_n. \end{aligned}$$

Thus,  $\text{Ker } \phi = 0$  if and only if  $\cap \mathfrak{a}_i = 0$ . Now for (2): suppose that  $\phi$  is surjective. For  $\mathfrak{a}_i$  and  $\mathfrak{a}_j$ , there exists  $a \in R$  such that  $\phi(a)$  returns  $(\dots, 0, 1, 0, \dots)$ , where 1 is in the  $i$ -th place. Then  $a - 1 \in \mathfrak{a}_i$  and  $a \in \mathfrak{a}_j$ , so

$$1 = (1 - a) + a \in (\mathfrak{a}_i + \mathfrak{a}_j),$$

so  $\mathfrak{a}_i$  and  $\mathfrak{a}_j$  are relatively prime. Now, suppose that  $\mathfrak{a}_i$  and  $\mathfrak{a}_j$  are relatively prime for each  $i \neq j$ . We need only show that the element  $(\dots, 0, 1, 0, \dots)$  lies in the image of  $\phi$ ; the 1 may be anywhere by similarity, so we can generate all elements of  $\prod R / \mathfrak{a}_i$ .

For each  $i \in \{1, \dots, n\}$ , we have  $\mathfrak{a}_i$  and  $\prod_{j \neq i} \mathfrak{a}_j$  are coprime; thus there exists  $a_i$  in the former and  $a$  in the latter such that

$$a_i + a = 1.$$

Thus,  $a \in (1 + \mathfrak{a}_i)$ . We conclude that  $\phi(a) = (\dots, 0, 1, 0, \dots)$ , from which we construct as aforementioned and demonstrate the surjectivity of  $\phi$ .  $\square$

#### 4.4 Inclusion and Prime Ideals

In general, the union of ideals is rarely an ideal — yet there is much to be said about them:

**Theorem 24.** *Let  $\mathfrak{p}_1, \dots, \mathfrak{p}_n$  be prime ideals in  $R$  and let  $\mathfrak{a}$  be an ideal contained in  $\bigcup_{i=1}^n \mathfrak{p}_i$ . Then  $\mathfrak{a} \subseteq \mathfrak{p}_i$  for some  $i \in \{1, \dots, n\}$ .*

*Proof.* We prove the contrapositive — that if  $\mathfrak{a} \not\subseteq \mathfrak{p}_i$  for each  $i$ , then  $\mathfrak{a} \not\subseteq \bigcup \mathfrak{p}_i$ . The result is clearly true for  $n = 1$ , so we utilize induction: let the result be true for  $n - 1$ , and consider the prime ideals  $\mathfrak{p}_1, \dots, \mathfrak{p}_n$ .



We have that  $\mathfrak{a} \not\subseteq \bigcup_{i=1}^{n-1} \mathfrak{p}_i$  by our inductive hypothesis, and  $\mathfrak{a} \not\subseteq \mathfrak{p}_n$ . Suppose for contradiction that  $\mathfrak{a} \subseteq \bigcup_{i=1}^n \mathfrak{p}_i$ ; then there exists  $a_1, a_2 \in \mathfrak{a}$  such that

$$a_1 \in \bigcup_{i=1}^{n-1} \mathfrak{p}_i \text{ but } a_1 \notin \mathfrak{p}_n,$$

$$a_2 \in \mathfrak{p}_n \text{ but } a_2 \notin \bigcup_{i=1}^{n-1} \mathfrak{p}_i.$$

Their sum lies in neither; thus  $a_1 + a_2 \notin \bigcup_{i=1}^n \mathfrak{p}_i$ , which yields the desired contradiction. We conclude that  $\mathfrak{a} \not\subseteq \bigcup_{i=1}^n \mathfrak{p}_i$ ; taking the contrapositive yields the required result.  $\square$

The following theorem does not concern unions, but it recasts the formulation of the above:

**Theorem 25.** *Let  $\mathfrak{a}_1, \dots, \mathfrak{a}_n$  be ideals and let  $\mathfrak{p}$  be a prime ideal containing  $\bigcap \mathfrak{a}_i$ . Then  $\mathfrak{p} \supseteq \mathfrak{a}_i$  for some  $i$ .*

*Proof.* Suppose  $\mathfrak{p} \not\supseteq \mathfrak{a}_i$  for all  $i \in \{1, \dots, n\}$ . Then there exist  $a_i \in \mathfrak{a}_i$  for each  $i$  that all do not belong to  $\mathfrak{p}$ ; the product

$$a = \prod_{i=1}^n a_i$$

lies inside every  $\mathfrak{a}_i$ , so  $a \in \bigcap \mathfrak{a}_i$ ; the primality of  $\mathfrak{p}$  yields  $a \notin \mathfrak{p}$ , so  $\mathfrak{p} \not\supseteq \bigcap \mathfrak{a}_i$ .  $\square$

**Corollary 4.** *Let  $\mathfrak{a}_1, \dots, \mathfrak{a}_n$  be ideals. If  $\bigcap \mathfrak{a}_i$  is prime, then  $\bigcap \mathfrak{a}_i = \mathfrak{a}_j$  for some  $j$ .*

## 4.5 The Ideal Quotient

For ideals  $\mathfrak{a}, \mathfrak{b}$  of  $R$ , their **ideal quotient** (which is trivially an ideal) is

$$(\mathfrak{a} : \mathfrak{b}) = \{x \mid x \in R, x\mathfrak{b} \subseteq \mathfrak{a}\},$$

The most important ideal quotient is the **annihilator**, defined as  $(0 : \mathfrak{b})$  — the set of all  $x \in R$  such that  $x(\mathfrak{b}) = 0$  — and denoted as  $\text{Ann } \mathfrak{b}$ . In this notation, the set  $D$  of all zero-divisors of  $R$  is

$$D = \bigcup_{a \neq 0} \text{Ann}(a).$$

If  $(b)$  is a principal ideal, we write  $(\mathfrak{a} : b)$  in place of  $(\mathfrak{a} : (b))$ .

**Theorem 26.** For all ideals  $\mathfrak{a}_i$ ,  $\mathfrak{b}_i$  and  $\mathfrak{c}$  of  $R$  for indices  $i \in I$ , the following five properties hold:

1.  $\mathfrak{a} \subseteq (\mathfrak{a} : \mathfrak{b})$ .
2.  $(\mathfrak{a} : \mathfrak{b})\mathfrak{b} \subseteq \mathfrak{a}$ .
3.  $((\mathfrak{a} : \mathfrak{b}) : \mathfrak{c}) = (\mathfrak{a} : \mathfrak{b}\mathfrak{c}) = ((\mathfrak{a} : \mathfrak{c}) : \mathfrak{b})$ .
4.  $(\bigcap_i \mathfrak{a}_i : \mathfrak{b}) = \bigcap_i (\mathfrak{a}_i : \mathfrak{b})$ .
5.  $(\mathfrak{a} : \sum_i \mathfrak{b}_i) = \bigcap_i (\mathfrak{a} : \mathfrak{b}_i)$ .

*Proof.* The proofs are as follows:

1. Let  $a \in \mathfrak{a}$ . Then  $ab \in \mathfrak{a}$  for all  $b \in \mathfrak{b}$ , so  $a(\mathfrak{b}) \subseteq \mathfrak{a}$ ; hence  $a \in (\mathfrak{a} : \mathfrak{b})$ . We conclude that  $\mathfrak{a} \subseteq (\mathfrak{a} : \mathfrak{b})$ .
2. Let  $x \in (\mathfrak{a} : \mathfrak{b})$ . By definition,  $x\mathfrak{b} \subseteq \mathfrak{a}$ ; thus  $(\mathfrak{a} : \mathfrak{b})\mathfrak{b} \subseteq \mathfrak{a}$ .
3. The two sets are equivalent, since

$$\begin{aligned} x \in ((\mathfrak{a} : \mathfrak{b}) : \mathfrak{c}) &\iff x\mathfrak{c} \subseteq (\mathfrak{a} : \mathfrak{b}) \\ &\iff x\mathfrak{b}\mathfrak{c} \subseteq \mathfrak{a} \\ &\iff x \in (\mathfrak{a} : \mathfrak{b}\mathfrak{c}). \end{aligned}$$

Using this very identity yields  $(\mathfrak{a} : \mathfrak{b}\mathfrak{c}) = (\mathfrak{a} : \mathfrak{c}\mathfrak{b}) = ((\mathfrak{a} : \mathfrak{c}) : \mathfrak{b})$ .

4. The two sets are equivalent, since

$$\begin{aligned} x \in \left( \bigcap_i \mathfrak{a}_i : \mathfrak{b} \right) &\iff x\mathfrak{b} \subseteq \bigcap_i \mathfrak{a}_i \\ &\iff x\mathfrak{b} \subseteq \mathfrak{a}_i \text{ for each } i \\ &\iff x \in (\mathfrak{a}_i : \mathfrak{b}) \text{ for each } i \\ &\iff x \in \bigcap_i (\mathfrak{a}_i : \mathfrak{b}). \end{aligned}$$

5. The two sets are equivalent, since

$$\begin{aligned} x \in \left( \mathfrak{a} : \sum_i \mathfrak{b}_i \right) &\iff x \left( \sum_i \mathfrak{b}_i \right) \subseteq \mathfrak{a} \\ &\iff x\mathfrak{b}_i \subseteq \mathfrak{a} \text{ for each } i \\ &\iff x \in (\mathfrak{a} : \mathfrak{b}_i) \text{ for each } i \\ &\iff x \in \bigcap_i (\mathfrak{a} : \mathfrak{b}_i). \end{aligned}$$

This concludes the proof of all five properties. □

## 4.6 Radicals of Ideals

The **radical** of an ideal  $\mathfrak{a}$  of  $R$

$$r(\mathfrak{a}) = \{x \in R \mid x^n \in \mathfrak{a} \text{ for some } n \in \mathbb{Z}_{>0}\}.$$

If  $\phi : R \rightarrow R/\mathfrak{a}$  is the canonical surjection, then  $\phi(r(\mathfrak{a})) = \mathfrak{R}_{R/\mathfrak{a}}$ , the nilradical of  $R/\mathfrak{a}$ ; the Correspondence Theorem thus ensures that  $r(\mathfrak{a})$  is an ideal.

**Theorem 27.** *For all ideals  $\mathfrak{a}$  and  $\mathfrak{b}$  of  $R$ , the following six properties hold:*

1.  $\mathfrak{a} \subseteq r(\mathfrak{a})$ .
2.  $r(r(\mathfrak{a})) = r(\mathfrak{a})$ .
3.  $r(\mathfrak{a}\mathfrak{b}) = r(\mathfrak{a} \cap \mathfrak{b}) = r(\mathfrak{a}) \cap r(\mathfrak{b})$ .
4.  $r(\mathfrak{a}) = R$  if and only if  $\mathfrak{a} = R$ .
5.  $r(\mathfrak{a} + \mathfrak{b}) = r(r(\mathfrak{a}) + r(\mathfrak{b}))$ .
6. If  $\mathfrak{p}$  is prime, then  $r(\mathfrak{p}^n) = \mathfrak{p}$  for all  $n \in \mathbb{Z}_{>0}$ .

*Proof.* Since (1) is trivial, the proofs are as follows:

2. Observe that  $x \in r(r(\mathfrak{a})) \implies x^n \in r(\mathfrak{a})$  for some  $n \implies x^{mn} \in \mathfrak{a}$  for some  $m$ ; thus  $x \in r(\mathfrak{a})$ . If we suppose  $x \in r(\mathfrak{a})$  and  $r(r(\mathfrak{a})) \subseteq r(\mathfrak{a})$ , then a usage of (1) yields  $r(r(\mathfrak{a})) = \mathfrak{a}$ .
3. **First Equality:** Since  $\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{a} \cap \mathfrak{b}$ , we have  $r(\mathfrak{a}\mathfrak{b}) \subseteq r(\mathfrak{a} \cap \mathfrak{b})$ . If  $x \in r(\mathfrak{a} \cap \mathfrak{b})$ , then  $x^n \in \mathfrak{a} \cap \mathfrak{b}$  for some  $n$ ; then  $x^{n+1} \in \mathfrak{a}\mathfrak{b}$ , so  $r(\mathfrak{a}\mathfrak{b}) = r(\mathfrak{a} \cap \mathfrak{b})$ .  
**Second Equality:** Clearly  $x \in r(\mathfrak{a} \cap \mathfrak{b})$  implies  $x \in r(\mathfrak{a})$  and  $x \in r(\mathfrak{b})$ , so  $x \in r(\mathfrak{a}) \cap r(\mathfrak{b})$ . If we assume the latter, then let  $x^n \in \mathfrak{a}$  and  $x^m \in \mathfrak{b}$ ; then  $x^{nm} \in \mathfrak{a} \cap \mathfrak{b}$ , so  $x \in r(\mathfrak{a} \cap \mathfrak{b})$ . Hence,  $r(\mathfrak{a} \cap \mathfrak{b}) = r(\mathfrak{a}) \cap r(\mathfrak{b})$ .
4. Realize that

$$\begin{aligned} r(\mathfrak{a}) = R &\iff 1 \in r(\mathfrak{a}) \\ &\iff 1^n \in \mathfrak{a} \text{ for some } n \\ &\iff 1 \in \mathfrak{a} \\ &\iff \mathfrak{a} = R. \end{aligned}$$

5. We have  $r(\mathfrak{a} + \mathfrak{b}) \subseteq r(r(\mathfrak{a}) + r(\mathfrak{b}))$  by (1); the other direction is simple.
6. Realize that since

$$x \in r(\mathfrak{p}) \iff x^n \in \mathfrak{p} \text{ for some } n \iff x \in \mathfrak{p},$$

we have  $r(\mathfrak{p}) = \mathfrak{p}$ . The powers come from repeated application of (3).

□

More generally, we can define the radical  $r(E)$  for any subset  $E \subseteq R$ . It is not an ideal in general; it satisfies  $r(\bigcup_i E) = \bigcup_i r(E)$ .

**Theorem 28.** *The radical of an ideal  $\mathfrak{a}$  is the intersection of the prime ideals that contain  $\mathfrak{a}$ .*

*Proof.* Using the canonical surjection  $\phi : R \rightarrow R/\mathfrak{a}$ , we have for prime  $\mathfrak{p}$  that

$$\mathfrak{p} \text{ contains the radical of } \mathfrak{a} \text{ in } R \iff \phi(\mathfrak{p}) \text{ contains the nilradical in } R/\mathfrak{a}.$$

The latter is guaranteed by Theorem 20. It is easy to verify that  $\phi(\mathfrak{p})$  is prime.  $\square$

**Theorem 29.** *The set  $D$  of zero-divisors of  $R$  is equal to  $\bigcup_{a \neq 0} r(\text{Ann}(a))$ .*

*Proof.* The key is to realize that  $D = r(D)$ . This is because Theorem 27 ensures  $D \subseteq r(D)$ ; now if  $x \in r(D)$ , then  $x^n \in D$ , so  $x^n y = x(x^{n-1}y) = 0$  for some  $n \in \mathbb{Z}_{>0}$ , and  $x \in D$ . Hence  $D = r(D)$ .

Now, we simply utilize the properties discussed in Section 4.5 and this page:

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

$\square$

**Theorem 30.** *If  $\mathfrak{a}$  and  $\mathfrak{b}$  are ideals of  $R$ , then  $\mathfrak{a}$  and  $\mathfrak{b}$  are relatively prime if and only if  $r(\mathfrak{a})$  and  $r(\mathfrak{b})$  are relatively prime.*

*Proof.* Using (4) and (5) from Theorem 27, we have that

$$\begin{aligned} \mathfrak{a} + \mathfrak{b} = R &\iff r(\mathfrak{a} + \mathfrak{b}) = R \\ &\iff r(r(\mathfrak{a}) + r(\mathfrak{b})) = R \\ &\iff r(\mathfrak{a}) + r(\mathfrak{b}) = R, \end{aligned}$$

as required.  $\square$

## 4.7 Extension and Contraction

For a ring homomorphism  $\phi : R \rightarrow S$  and an ideal  $\mathfrak{a}$  of  $R$ , the image  $\phi(\mathfrak{a})$  need not be an ideal of  $S$ . We define the **extension**  $\mathfrak{a}^e$  as the principal ideal generated by  $A$ : namely,  $\sum_{a \in R} (f(a))$ . If  $\mathfrak{b}$  is an ideal of  $S$ , then the Correspondence Theorem ensures that  $\{a \in R \mid \phi(a) \in \mathfrak{b}\}$  is an ideal, called the **contraction** of  $\mathfrak{b}$  and denoted by  $\mathfrak{b}^c$ .

To motivate these definitions, factorize  $\phi$  as follows:

$$R \xrightarrow{p} \phi(R) \xrightarrow{j} S$$

The behavior of ideals under  $p$  is very simple: ideals of  $\phi(R)$  correspond precisely with ideals of  $R$  that contain the kernel of  $\phi$ . The situation with ideals under  $j$  is very complicated — in fact, it is among the central problems of Algebraic Number Theory.

**Example:** Consider the embedding  $\mathbb{Z} \rightarrow \mathbb{Z}[i]$ . For a prime ideal  $(p)$  of  $\mathbb{Z}$ , what is the extension of  $(p)$  in  $\mathbb{Z}[i]$ ? Well,  $\mathbb{Z}[i]$  is a principal ideal domain, and the situation is:

1.  $(2)^e$  is the principal ideal  $((1+i)^2)$ , the *square* of the principal ideal  $(1+i)$
2. If  $p \equiv 1 \pmod{4}$ , then  $(p)^e$  is the product of two distinct prime ideals.
3. If  $p \equiv 3 \pmod{4}$ , then  $(p)^e$  is prime in  $\mathbb{Z}[i]$ .

Observe the similarity between (2) and Fermat's theorem on sums of two squares.

**Theorem 31.** *For a homomorphism  $\phi : R \rightarrow S$  and ideals  $\mathfrak{a}$  and  $\mathfrak{b}$  like before:*

1.  $\mathfrak{a} \subseteq \mathfrak{a}^{ec}$  and  $\mathfrak{b} \supseteq \mathfrak{b}^{ce}$ .
2.  $\mathfrak{a}^e = \mathfrak{a}^{ece}$  and  $\mathfrak{b}^c = \mathfrak{b}^{cec}$ .
3. *If  $C$  is the set of contracted ideals in  $R$  and  $E$  is the set of extended ideals in  $S$ , then  $C = \{\mathfrak{a} \mid \mathfrak{a}^{ec} = \mathfrak{a}\}$  and  $E = \{\mathfrak{b} \mid \mathfrak{b}^{ce} = \mathfrak{b}\}$ . Furthermore,  $\mathfrak{a} \rightarrow \mathfrak{a}^e$  is a bijection from  $C$  to  $E$  with inverse  $\mathfrak{b} \rightarrow \mathfrak{b}^c$ .*

*Proof.* These proofs are omitted, in the interest of remaining productive. I will comment: (1) is quite trivial, and (2) follows directly afterward.  $\square$

In the interest of remaining productive, we will not prove the following fomulas:

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

The set of ideals  $E$  is thus closed under sum and product, while  $C$  is closed under ideal quotients, radicals, and intersections.

## 5 The Zariski Topology

### 5.1 Definition

Let  $R$  be a ring and let  $X$  denote the set of prime ideals of  $R$ . For each subset  $E \subseteq R$ , let  $V(E)$  denote the set of prime ideals which contain  $E$ .

**Theorem 32.** *Let  $(E_\alpha) \subseteq R$ , let  $E_1, E_2 \subseteq R$ . Define  $\mathfrak{a}_\alpha$ ,  $\mathfrak{a}_1$ , and  $\mathfrak{a}_2$  as the ideals generated by these sets. Then the following holds:*

1.  $V(E) = V(\mathfrak{a}) = V(r(\mathfrak{a}))$ .
2.  $\bigcap_{\alpha} V(\mathfrak{a}_\alpha) = V\left(\bigcup_{\alpha} \mathfrak{a}_\alpha\right)$ .
3.  $V(\mathfrak{a}_1) \cup V(\mathfrak{a}_2) = V(\mathfrak{a}_1 \mathfrak{a}_2) = V(\mathfrak{a}_1 \cap \mathfrak{a}_2)$ .

*Proof.* For (1), it is clear that

$$\mathfrak{p} \in V(E) \iff E \subseteq \mathfrak{p} \iff \mathfrak{a} \subseteq \mathfrak{p} \iff \mathfrak{p} \in V(\mathfrak{a}).$$

For (2), we similarly utilize such convenient chains of equivalencies:

$$\begin{aligned}
\mathfrak{p} \in \bigcap_{\alpha} V(\mathfrak{a}_\alpha) &\iff \mathfrak{a}_\alpha \subseteq \mathfrak{p} \text{ for each } \alpha. \\
&\iff \bigcup_{\alpha} \mathfrak{a}_\alpha \subseteq \mathfrak{p} \\
&\iff \mathfrak{p} \in V\left(\bigcup_{\alpha} \mathfrak{a}_\alpha\right).
\end{aligned}$$

The story for (3) is again quite similar: we have that

$$\begin{aligned}
\mathfrak{p} \in V(\mathfrak{a}_1) \cup V(\mathfrak{a}_2) &\iff \mathfrak{a}_1 \subseteq \mathfrak{p} \text{ or } \mathfrak{a}_2 \subseteq \mathfrak{p} \\
&\iff \mathfrak{a}_1 \cap \mathfrak{a}_2 \subseteq \mathfrak{p} \iff \mathfrak{p} \in V(\mathfrak{a}_1 \cap \mathfrak{a}_2) \\
&\iff \mathfrak{a}_1 \mathfrak{a}_2 A \subseteq \mathfrak{p} \iff \mathfrak{p} \in V(\mathfrak{a}_1 \mathfrak{a}_2).
\end{aligned}$$

This last step follows from the fact  $r(\mathfrak{a}_1 \cap \mathfrak{a}_2) = r(\mathfrak{a}_1 \mathfrak{a}_2)$ . This completes the proof.  $\square$

Further observe that  $V(0) = X$  and  $V(1) = \emptyset$ . Thus the sets  $V(\mathfrak{a})$  across all  $\mathfrak{a} \in X$  satisfy the closed set axioms of a topological space. The resulting topology is called the **Zariski topology**, and the set  $X$  is called the **prime spectrum** of  $R$ , denoted  $\text{Spec } R$ .