

# Commutative Algebra

Alec Zabel-Mena

June 21, 2023



# Contents

<b>1</b>	<b>Rings and Ideals</b>	<b>5</b>
1.1	Definitions and Examples. . . . .	5
1.2	Polynomial Rings . . . . .	7
1.3	Ring Homomorphisms and Factor Rings. . . . .	8
1.4	Properties of Ideals . . . . .	10
1.5	Extension and Contraction of Rings . . . . .	13



# Chapter 1

## Rings and Ideals

### 1.1 Definitions and Examples.

**Definition.** A **commutative ring**  $A$  is a set together with two binary operations  $+$  :  $(a, b) \rightarrow a + b$  and  $\cdot$  :  $(a, b) \rightarrow ab$  called **addition** and **multiplication** such that:

- (1)  $A$  is an Abelian group over  $+$ , where we denote the identity element as  $0$  and the inverse of each  $a \in A$  as  $-a$ .
- (2) For any  $a, b \in A$ ,  $ab \in A$  and  $a(bc) = (ab)c$ . That is,  $A$  is closed under multiplication, and multiplication is associative.
- (3)  $a(b + c) = ab + ac$  and  $(a + b)c = ac + bc$ .
- (4)  $ab = ba$  for all  $a, b \in A$ .

If there exists an element  $1 \in A$  such that  $a1 = 1a = a$ , then we call  $A$  a ring with **identity**. If  $1 = 0$ , we call  $A$  the **zero ring** and write  $A = 0$ .

**Definition.** A commutative ring  $k$  with identity  $1 \neq 0$  is called a **field** if for all  $a \in k$ , where  $a \neq 0$ , there exists a  $b \in A$  such that  $ab = 1$ .

**Lemma 1.1.1.** *Let  $A$  be a commutative ring with identity. Then the following are true for all  $a, b \in A$ .*

- (1)  $0a = a0 = 0$ .
- (2)  $(-a)b = a(-b) = -(ab)$ .
- (3)  $(-a)(-b) = ab$
- (4)  $1 \neq 0$ , then  $1$  is unique and  $-a = (-1)a$ .

*Proof.* (1) Notice  $0a = (0 + 0)a = 0a + 0a$ , so that  $0a = 0$ . Likewise,  $a0 = 0$  by the same reasoning.

- (2) Notice that  $b - b = 0$ , so  $a(b - b) = ab + a(-b) = 0$ , so that  $a(-b) = -(ab)$ . The same argument with  $(a - a)b$  gives  $(-a)b = -(ab)$ .

- (3) By the inverse laws of addition in  $A$ , we have  $-(a(-b)) = -(-(ab))$ , so that  $(-a)(-b) = ab$ .
- (4) Suppose  $A$  has identity  $1 \neq 0$ , and suppose there is an element  $2 \in A$  for which  $2a = a2 = a$  for all  $a \in A$ . Then we have that  $1 \cdot 2 = 1$  and  $1 \cdot 2 = 2$ , making  $1 = 2$ ; so 1 is unique. Now, we have that  $a + (-a) = 0$ , so that  $1(a + (-a)) = 1a + 1(-a) = 1a + (-a) = 0$ . So  $(-a) = -(1a) = (-1)a$  by (2). ■

**Definition.** Let  $A$  be a ring. We call an element  $a \in A$  a **zero divisor** if  $a \neq 0$  and there exists an element  $b \neq 0$  such that  $ab = 0$ . Similarly, we call  $a \in A$  a **unit** if there is a  $b \in A$  for which  $ab = ba = 1$ . We call an element  $a$  **nilpotent** if there exists some  $n \in \mathbb{Z}^+$  for which  $a^n = 0$ .

**Definition.** Let  $A$  be a ring. We call the set of all units in  $A$  the **group of units** and denote it  $\mathcal{U}(A)$ , or  $A^*$ .

**Lemma 1.1.2.** *Let  $A$  be a commutative ring with identity  $1 \neq 0$ . Then the group of units  $\mathcal{U}(A)$  forms an Abelian group under multiplication.*

*Proof.* Let  $a, b \in A$  be units in  $A$ . Then there are  $c, d \in A$  for which  $ac = ca = 1$  and  $bd = db = 1$ . Consider then  $ab$ . Then  $ab(dc) = a(bd)c = ac = 1$  and  $(dc)ab = d(ca)b = db = 1$  so that  $ab$  is also a unit in  $A$ . Moreover  $\mathcal{U}(A)$  inherits the associativity of  $\cdot$  and 1 serves as the identity element of  $A^*$ . Lastly, if  $a \in A^*$  is a unit there is a  $b \in A$  for which  $ab = ba = 1$ . This also makes  $b$  a unit in  $A$ , and the inverse of  $a$ . Now, since  $A$  is a commutative ring, the multiplication in  $\mathcal{U}(A)$  is commutative, making  $\mathcal{U}(A)$  Abelian. ■

**Corollary.**  *$a$  is a zero divisor if, and only if it is not a unit.*

*Proof.* Suppose that  $a \neq 0$  is a zero divisor. Then there is a  $b \in A$  such that  $b \neq 0$  and  $ab = 0$ . Then for any  $v \in A$ ,  $v(ab) = (va)b = 0$  so that  $a$  cannot be a unit. On the other hand let  $a$  be a unit, and  $ab = 0$  for some  $b \neq 0$ . Then there is a  $v \in A$  for which  $v(ab) = (va)b = 1b = b = 0$ . Then  $b = 0$  which is a contradiction. ■

**Corollary.** *If  $k$  is a field, then it has no zero divisors.*

*Proof.* Notice by definition of a field, every element is a unit, except for 0. ■

**Definition.** A commutative ring with identity  $1 \neq 0$  is called an **integral domain** if it has no zero divisors.

**Lemma 1.1.3.** *Any finite integral domain is a field.*

*Proof.* Let  $A$  be a finite integral domain and consider the map on  $A$ , by  $x \rightarrow ax$ . By above, this map is 1-1, moreover since  $A$  is finite, it is also onto. So there is a  $b \in A$  for which  $ab = 1$ , making  $a$  a unit. Since  $a$  is arbitrarily chosen, this makes  $A$  a field. ■

**Corollary.** *If  $k$  is a field it is a (not necessarily finite) integral domain.*

**Definition.** A **subring** of a ring  $A$  is a subgroup of  $A$  closed under multiplication.

## 1.2 Polynomail Rings

**Theorem 1.2.1.** *Let  $A$  be a commutative ring with identity, and define  $A[x] = \{f(x) = a_0 + a_1x + \cdots + a_nx^n : a_0, \dots, a_n \in A\}$ . Define the operations  $+$  and  $\cdot$  on  $A[x]$  for  $f(x) = a_0 + a_1x + \cdots + a_nx^n$  and  $g(x) = b_0 + b_1x + \cdots + b_nx^n$  by:*

$$f + g = (a_0 + b_0) + (a_1 + b_1)x + \cdots + (a_n + b_n)x^n$$

$$fg = c_0 + c_1x + \cdots + c_kx^k \text{ where } c_j = \sum_{i=0}^j a_ib_{j-i} \text{ and } k = n + m$$

*Then  $A[x]$  is a commutative ring with identity.*

**Definition.** Let  $A$  be a commutative ring with identity. We call the ring  $A[x]$  the **ring of polynomials** in  $x$  with **coefficients** in  $A$  whose elements of the form

$$f(x) = a_0 + a_1x + \cdots + a_nx^n$$

where  $n \geq 0$  are called **polynomails**. If  $a_n \neq 0$ , then the **degree** of  $f$  is denoted  $\deg f = n$ , and  $f$  is called **monic** if  $a_n = 1$ . We call  $+$  and  $\cdot$  the **addition** and **multiplication** of polynomials.

**Example 1.1.** (1) Take  $A$  any commutative ring with identity and form  $A[x]$ . One can verify that the polynomial  $0(x) = 0 + 0x + \cdots + 0x^n + \cdots = 0$ , in this case we call  $0$  the **zero polynomail**. Similarly, the additive inverse of  $f(x) = a_0 + a_1x + \cdots + a_nx^n$  is the polynomial  $-f(x) = -a_0 - a_1x - \cdots - a_nx^n$ . Now, since  $A[x]$  has identity, the **identity** polynomial is  $1(x) = 1 + 0x + \cdots = 1$ , that is, it is the identity in  $A$ . Lastly, we call a polynomial  $f$  with  $\deg f = 0$  a **constant polynomail**. Notice that  $0$  and  $1$  are constant polynomials.

(2)  $\mathbb{Z}[x]$ ,  $\mathbb{Q}[x]$ ,  $\mathbb{A}[x]$  and  $\mathbb{C}[x]$  are the polynomial rings in  $x$  with coefficients in  $\mathbb{Z}$ ,  $\mathbb{Q}$ ,  $\mathbb{A}$ , and  $\mathbb{C}$  respectively.

(3) Notice that the rings  $\mathbb{Z}[\omega]$  and  $\mathbb{Z}[i]$  are polynomial rings in  $\omega$  and  $i$ , respectively, with coefficients in  $\mathbb{Z}$ , and where  $\omega = \sqrt{D}$  if  $D \not\equiv 1 \pmod{4}$  or  $\omega = \frac{1+\sqrt{D}}{2}$  otherwise, and  $i^2 = -1$ . Notice that the highest degree a polynomial in  $\mathbb{Z}[i]$  can achieve is  $\deg = 1$ ; however, one may be able to form polynomial rings in other variables with coefficients in  $\mathbb{Z}[i]$ , i.e. take  $Z[x]$ , where  $Z = \mathbb{Z}[i]$ .

(4)  $\mathbb{Z}/_3\mathbb{Z}[x]$  is the polynomial ring with coefficients in  $\mathbb{Z}/_3\mathbb{Z}$ .

**Theorem 1.2.2.** *Let  $A$  be an integral domain, and let  $p, q \neq 0$  be polynomials in  $A[x]$ . Then the following are true:*

(1)  $\deg pq = \deg p + \deg q$ .

(2) *The units of  $A[x]$  are precisely the units of  $A$*

(3)  $A[x]$  is an integral domain.

*Proof.* Consider the leading terms  $a_n x^n$  and  $b_m x^m$  of  $p$  and  $q$  respectively. Then  $a_n b_m x^{m+n}$  is the leading term of  $pq$ ; moreover we require  $a_n b_m \neq 0$ . Now, if  $\deg pq < m + n$ , then  $ab = 0$ , making  $a$  and  $b$  zero divisors of  $A$ ; impossible. Therefore  $ab \neq 0$ . It also follows that since no term of  $p$  is a zero divisor, then  $p$  cannot be a zero divisor of  $A[x]$ . Lastly, if  $pq = 1$ , then  $\deg p + \deg q = 0$ , so that  $pq$  is a constant polynomial. Noticing that constant polynomials are simply just elements of  $A$ , then  $p$  and  $q$  are units. ■

### 1.3 Ring Homomorphisms and Factor Rings.

**Definition.** Let  $A$  and  $B$  be commutative rings with identity. We call a map  $\phi : A \rightarrow B$  a **ring homomorphism** if

- (1)  $\phi$  is a group homomorphism with respect to addition.
- (2)  $\phi(ab) = \phi(a)\phi(b)$  for any  $a, b \in A$ .
- (3)  $\phi(1_A) = 1_B$ .

We denote the **kernel** of  $\phi$  to be the kernel of  $\phi$  as a group homomorphism. That is

$$\ker \phi = \{r \in A : \phi(r) = 0\}$$

Moreover, if  $\phi$  is 1-1 and onto, we call  $\phi$  an **isomorphism** and say that  $A$  and  $B$  are **isomorphic**, and write  $A \simeq B$ .

**Lemma 1.3.1.** *Let  $A$  and  $B$  be commutative rings with identity, and  $\phi : A \rightarrow B$  a ring homomorphism. Then*

- (1)  $\phi(A)$  is a subring of  $B$ .
- (2)  $\ker \phi$  is a subring of  $A$ .

*Proof.* Let  $s_1, s_2 \in \phi(A)$ . Then  $s_1 = \phi(r_1)$  and  $s_2 = \phi(r_2)$  for some  $r_1, r_2 \in A$ . Then  $s_1 s_2 = \phi(r_1)\phi(r_2) = \phi(r_1 r_2) \in \phi(B)$ . Additionally,  $s^{-1} = \phi^{-1}(r) = \phi(r^{-1})$  for some  $s \in B$ ,  $r \in A$ . This is sufficient to make  $B$  a subring of  $B$ .

By similar reasoning, if  $r_1, r_2 \in \ker \phi$ , then  $\phi(r_1)\phi(r_2) = \phi(r_1 r_2) = 0$  so that  $r_1 r_2 \in \ker \phi$ , and  $\phi(r^{-1}) = \phi^{-1}(r) = 0$  so  $\phi^{-1} \in \ker \phi$ . ■

**Corollary.** *For any  $r \in A$  and  $a \in \ker \phi$ , then  $ar \in \ker \phi$  and  $ra \in \ker \phi$ .*

*Proof.* We have  $\phi(ar) = \phi(a)\phi(r) = \phi(a)0 = 0$  so  $ar \in \ker \phi$ . The same happens for  $ra$ . ■

**Definition.** Let  $A$  be a comutative ring with identity. We call a subset  $\mathfrak{a}$  of  $A$  an **ideal** of  $A$  if it is a subgroup under  $+$ , and for any  $r \in A$ , and  $a \in \mathfrak{a}$ ,  $ra \in \mathfrak{a}$ .



**Theorem 1.3.2.** Let  $A$  be a commutative ring with identity, and  $I\mathfrak{a}$  an ideal in  $A$ . Let  $A/\mathfrak{a}$  be the set of all  $a + \mathfrak{a}$  with  $a \in A$ . Define operations  $+$  and  $\cdot$  by

$$\begin{aligned}(a + \mathfrak{a}) + (b + \mathfrak{a}) &= (a + b) + \mathfrak{a} \\ (a + \mathfrak{a})(b + \mathfrak{a}) &= ab + \mathfrak{a}\end{aligned}$$

Then  $A/\mathfrak{a}$  forms a commutative ring with identity under  $+$  and  $\cdot$ .

*Proof.* Notice that  $(a + \mathfrak{a}) + (b + \mathfrak{a}) = (a + b) + (\mathfrak{a} + \mathfrak{a}) = (a + b) + 2\mathfrak{a} = (a + b) + \mathfrak{a}$ . Moreover,  $A/\mathfrak{a}$  inherits associativity in  $+$  from addition in  $A$ . Now, take  $0 + \mathfrak{a} = \mathfrak{a}$  as the additive identity and  $-a + I$  as the inverse of  $a + \mathfrak{a}$  for each  $a$ .

Now, notice, that  $(a + \mathfrak{a})(b + \mathfrak{a}) = ab + a\mathfrak{a} + b\mathfrak{a} + \mathfrak{a}^2 = ab + (\mathfrak{a} + \mathfrak{a} + \mathfrak{a}) = ab + \mathfrak{a}$  by distribution of multiplication over addition in  $A$ . Moreover,  $A/\mathfrak{a}$  also inherits associativity and commutativity in  $\cdot$  from multiplication in  $A$ . Now, notice then

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

Observe also that if  $1$  is the identity of  $A$ , then  $1 + \mathfrak{a}$  is the identity of  $A/\mathfrak{a}$  as  $a + \mathfrak{a}$ . Since  $(a + \mathfrak{a})(1 + \mathfrak{a}) = a + \mathfrak{a}$ .

Lastly, notice that  $a + \mathfrak{a}$  is just the left coset of  $a$  by  $\mathfrak{a}$  in  $A$  as a group under addition. So that  $+$  and  $\cdot$  are coset addition and multiplication, which are well defined. ■

**Definition.** Let  $A$  be a commutative ring with identity and  $\mathfrak{a}$  an ideal in  $A$ . We call the ring  $A/\mathfrak{a}$  under addition and multiplication of cosets the **factor ring** (or **quotient ring**) of  $A$  over  $\mathfrak{a}$ .

**Theorem 1.3.3** (The First Isomorphism Theorem). If  $\phi : A \rightarrow B$  is a ring homomorphism from rings  $A$  into  $B$ , then  $\ker \phi$  is an ideal of  $A$  and

$$\begin{array}{ccc} & \phi(A) \simeq A/\ker \phi & \\ & \nearrow \bar{\phi} & \\ A & \xrightarrow{\phi} & B \\ \downarrow \pi & & \uparrow \\ A/\ker \phi & & \end{array}$$

*Proof.* By the first isomorphism theorem for groups,  $\phi$  is a group isomorphism. Now, let  $K = \ker \phi$  and consider the map  $\pi : A \rightarrow A/\mathfrak{a}$  by  $a \xrightarrow{\pi} a + K$ . Define the map  $\bar{\phi} : A/K \rightarrow \phi(A)$  such that  $\bar{\phi} \circ \pi = \phi$ , then  $\bar{\phi}$  defines the ring isomorphism. ■

*Proof.* The map  $\pi : A \rightarrow A/\mathfrak{a}$  defined by  $a \rightarrow a + \mathfrak{a}$ , for any ideal  $\mathfrak{a}$ , is onto, with  $\ker \pi = \mathfrak{a}$ . ■

**Theorem 1.3.4** (The Second Isomorphism Theorem). *Let  $\mathfrak{a} \subseteq A$  a subring of  $A$ , and let  $\mathfrak{b}$  an ideal in  $A$ . Define  $\mathfrak{a} + \mathfrak{b} = \{a + b : a \in \mathfrak{a} \text{ and } b \in \mathfrak{b}\}$ . Then  $\mathfrak{a} + \mathfrak{b}A$  is a subring and  $\mathfrak{a} \cap \mathfrak{b}$  is an ideal in  $A$ . Then*

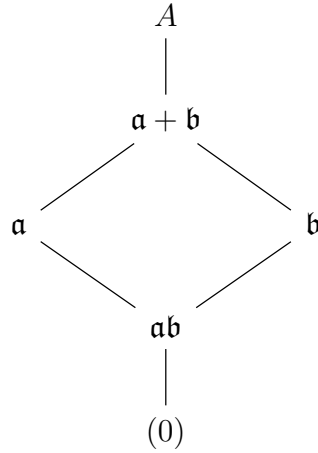
$$\mathfrak{a}\mathfrak{b}/\mathfrak{b} \simeq \mathfrak{a}/\mathfrak{a} \cap \mathfrak{b}$$

**Theorem 1.3.5** (The Third Isomorphism Theorem). *Let  $\mathfrak{a}$  and  $\mathfrak{b}$  be ideals in a ring  $A$ , with  $\mathfrak{a} \subseteq \mathfrak{b}$ . Then  $\mathfrak{b}/\mathfrak{a}$  is an ideal of  $A/\mathfrak{a}$  and*

$$A/\mathfrak{b} = (A/\mathfrak{a})/(\mathfrak{b}/\mathfrak{a})$$

**Theorem 1.3.6** (The Fourth Isomorphism Theorem). *Let  $\mathfrak{a}$  an ideal in a ring  $A$ , then the correspondence between  $A$  and  $A/\mathfrak{a}$ , for any subring of  $A$  is an inclusion preserving bijection between subrings of  $A$  containing  $\mathfrak{a}$  and  $A/\mathfrak{a}$ . Moreover,  $A$  is an ideal if, and only if  $A/\mathfrak{a}$  is an ideal.*

**Lemma 1.3.7.** *Let  $A$  be a ring with ideals  $\mathfrak{a}$  and  $\mathfrak{b}$ . Then  $\mathfrak{a} + \mathfrak{b}$ ,  $\mathfrak{a}\mathfrak{b}$  and  $\mathfrak{a}^n$ , for any  $n \geq 0$  are ideals of  $A$  and we have the lattice*



## 1.4 Properties of Ideals

**Definition.** Let  $A$  be a commutative ring with identity. We call the smallest ideal containing a nonempty subset  $S$  in  $A$  the **ideal generated** by  $S$ , and we write  $(S)$ . We call an ideal **principle** if it is generated by a single element of  $A$ , i.e.  $\mathfrak{a} = (a)$  for some  $a \in \mathfrak{a}$ . We say that the ideal  $(S)$  is **finitely generated** if  $|S|$  is finite, and if  $S = \{a_1, \dots, a_n\}$ , then we denote  $(S) = (a_1, \dots, a_n)$ .

**Example 1.2.** (1) In any commutative ring with identity, the trivial ideal and  $A$  are the ideals generated by 0 and 1, respectively, so we write them as  $(0)$  and  $A = (1)$ .

(2) In  $\mathbb{Z}$ , we can write the ideals  $n\mathbb{Z} = (n) = (-n)$ . Notice that every ideal in  $\mathbb{Z}$  is a principle ideal. Moreover, for  $m, n \in \mathbb{Z}$ ,  $n|m$  if, and only if  $n\mathbb{Z} \subseteq m\mathbb{Z}$ . Notice that  $m\mathbb{Z} + n\mathbb{Z} = d\mathbb{Z}$  is the ideal generated by  $m$  and  $n$ , where  $d = (m, n)$  is the greatest

common divisor of  $m$  and  $n$ . Indeed, by definition,  $d|m, n$  so that  $d\mathbb{Z} \subseteq m\mathbb{Z} + n\mathbb{Z}$ , and if  $c|m, n$ , then  $c|d$ , making  $m\mathbb{Z} + n\mathbb{Z} \subseteq d\mathbb{Z}$ . Then  $m\mathbb{Z} + n\mathbb{Z} = d\mathbb{Z}$  is the ideal generated by the greatest common divisor  $(m, n)$  and consists of all diophantine equations of the form

$$mx + ny = (m, n)$$

In general, we can define the **greatest common divisor** for integers  $n_1, n_2, \dots, n_m$  to be the smallest such integer  $d$  generating the ideal  $n_1\mathbb{Z} + \dots + n_m\mathbb{Z} = d\mathbb{Z}$ . We then write  $d = (n_1, \dots, n_m)$ .

- (3) Consider the ideal  $(2, x)$  of  $\mathbb{Z}[x]$ .  $(2, x)$  is not a principle ideal. We have that  $(2, x) = \{2p_xq : p, q \in \mathbb{Z}[x]\}$ , and that  $(2, x) \neq \mathbb{Z}[x]$ . Suppose that  $(2, x) = (a)$  for some polynomial  $a \in \mathbb{Z}[x]$ , then  $2 \in (a)$ , so that  $2 = p(x)a(x)$ , of degree  $\deg p + \deg a$ . This makes  $p$  and  $a$  constant polynomials in  $\mathbb{Z}[x]$ . Now, since 2 is prime in  $\mathbb{Z}$ , then only values for  $p$  and  $q$  are  $p = \pm 1$  and  $a = \pm 2$ . If  $a(x) = \pm 1$ , then every polynomial in  $\mathbb{Z}[x]$  can be written as a polynomial in  $(a)$ , so that  $(a) = \mathbb{Z}[x]$ , impossible. If  $a(x) = \pm 2$ , then since  $x \in (a)$ , we get  $x = 2q(x)$  where  $q \in \mathbb{Z}[x]$ . This cannot happen, so that  $(a) \neq (2, x)$ .

**Lemma 1.4.1.** *Let  $\mathfrak{a}$  an ideal in ring  $A$  with identity. Then*

- (1)  $\mathfrak{a} = (1)$  if, and only if  $\mathfrak{a}$  contains a unit.
- (2) If  $A$  is commutative, then  $A$  is a field if, and only if its only ideals are  $(0)$  and  $(1)$ .

*Proof.* Recall that  $A = (1)$ . Now, if  $\mathfrak{a} = (1)$ , then  $1 \in \mathfrak{a}$ , and 1 is a unit. Conversely, suppose that  $u \in \mathfrak{a}$  with  $u$  a unit. By definition, we have that  $r = r \cdot 1 = r(uv) = r(vu) = (rv)u$ , so that  $1 \in \mathfrak{a}$ . This makes  $\mathfrak{a} = (1)$ .

Now, if  $A$  is a field, then it is a commutative ring, moreover every  $r \neq 0$  is a unit in  $A$ , which makes  $r \in \mathfrak{a}$  for some ideal  $\mathfrak{a} \neq (0)$ . This makes every  $\mathfrak{a} \neq (0)$  equal to  $(1)$ . Conversely, if  $(0)$  and  $(1)$  are the only ideals of the commutative ring  $A$ , then every  $r \neq 0 \in (1)$ , which makes them units. Hence all nonzero  $r$  is a unit in  $A$ . This makes  $A$  into a field. ■

**Corollary.** *If  $k$  is a field, then any nonzero ring homomorphism  $\phi$  defined on  $k$  is 1-1.*

*Proof.* If  $k$  is a field, then either  $\ker \phi = (0)$  or  $\ker \phi = (1)$ . Now, since  $\ker \phi \neq A$ , we must have  $\ker \phi = (0)$ . ■

**Definition.** For any ideal  $\mathfrak{m}$  in a ring  $A$ , we call  $\mathfrak{m}$  **maximal** if  $\mathfrak{m} \neq A$ , and if  $\mathfrak{a}$  is an ideal with  $\mathfrak{m} \subseteq \mathfrak{a} \subseteq A$ , then either  $\mathfrak{m} = \mathfrak{a}$  or  $\mathfrak{a} = A$ .

**Lemma 1.4.2.** *If  $A$  is a commutative ring with identity, every proper ideal is contained in a maximal ideal.*

*Proof.* Let  $\mathfrak{a}$  a proper ideal of  $A$ . Let  $\mathcal{S} = \{N : N \neq (1) \text{ is a proper ideal, and } \mathfrak{a} \subseteq N\}$ . Then  $\mathcal{S} \neq \emptyset$ , as  $\mathfrak{a} \in \mathcal{S}$ , and the relation  $\subseteq$  partially orders  $\mathcal{S}$ . Let  $\mathcal{C}$  be a chain in  $\mathcal{S}$  and define

$$J = \bigcup_{\mathfrak{a} \in \mathcal{C}} \mathfrak{a}$$

We have that  $J \neq \emptyset$  since  $(0) \in J$ . Now, let  $a, b \in J$ , then we have that either  $(a) \subseteq (b)$  or  $(b) \subseteq (a)$ , but not both. In either case, we have  $a - b \in J$  so that  $J$  is closed under additive inverse. Moreover, since  $\mathfrak{a} \in \mathcal{C}$  is an ideal, by definition,  $J$  is closed with respect to absorption. This makes  $J$  an ideal.

Now, if  $1 \in J$ , then  $J = (1)$  and  $J$  is not proper, and  $\mathfrak{a} = (1)$  by definition of  $J$ . This is a contradiction as  $\mathfrak{a}$  must be proper. Therefore  $J$  must also be a proper ideal. Therefore,  $\mathcal{C}$  has an upperbound in  $\mathcal{S}$ , therefore, by Zorn's lemma,  $\mathcal{S}$  has a maximal element  $\mathfrak{m}$ , i.e. it has a maximal ideal  $\mathfrak{m}$  with  $\mathfrak{a} \subseteq \mathfrak{m}$ . ■

**Lemma 1.4.3.** *Let  $A$  be a commutative ring with identity. An ideal  $\mathfrak{m}$  is maximal if, and only if  $A/\mathfrak{m}$  is a field.*

*Proof.* If  $\mathfrak{m}$  is maximal, then there is no ideal  $I \neq (1)$  for which  $\mathfrak{m} \subseteq \mathfrak{a} \subseteq A$ . By the fourth isomorphism theorem, the ideals of  $A$  containing  $\mathfrak{a}$  are in 1-1 correspondence with the those of  $A/\mathfrak{m}$ . Therefore  $\mathfrak{m}$  is maximal if, and only if the only ideals of  $A/\mathfrak{m}$  are  $(\mathfrak{m})$  and  $(1+\mathfrak{m})$ . ■

**Example 1.3.** (1) Let  $n \geq 0$  an integer. The ideal  $n\mathbb{Z}$  is maximal in  $\mathbb{Z}$  if and only if  $\mathbb{Z}/n\mathbb{Z}$  is a field. Therefore  $n\mathbb{Z}$  is maximal if, and only if  $n = p$  a prime in  $\mathbb{Z}$ . So the maximal ideals of  $\mathbb{Z}$  are those  $p\mathbb{Z}$  where  $p$  is prime.

(2)  $(2, x)$  is not principal in  $\mathbb{Z}[x]$ , but it is maximal in  $\mathbb{Z}[x]$ , as  $\mathbb{Z}[x]/(2, x) \simeq \mathbb{Z}/2\mathbb{Z}$  which is a field.

(3) The ideal  $(x)$  is not maximal in  $\mathbb{Z}/n\mathbb{Z}$ , since  $\mathbb{Z}/(x) \simeq \mathbb{Z}$ , which is not a field. Moreover,  $(x) \subseteq (2, x) \subseteq \mathbb{Z}[x]$ . We construct this isomorphism by identifying  $x = 0$ , then all polynomials of  $\mathbb{Z}[x]/(x)$  only have constant term in  $\mathbb{Z}$ .

**Definition.** We call an ideal  $\mathfrak{p}$  in a commutative ring  $A$  with identity **prime** if  $\mathfrak{p} \neq (1)$  and if  $ab \in \mathfrak{p}$  then either  $a \in \mathfrak{p}$  or  $b \in \mathfrak{p}$ . Alternatively, if  $(ab) \subseteq \mathfrak{p}$  then  $(a) \subseteq \mathfrak{p}$  or  $(b) \subseteq \mathfrak{p}$ .

**Example 1.4.** The prime ideals of  $\mathbb{Z}$  are  $p\mathbb{Z}$  with  $p$  prime together with  $(0)$ .

**Lemma 1.4.4.** *An ideal  $\mathfrak{p}$  in a commutative ring with identity,  $A$ , is prime if, and only if  $A/\mathfrak{p}$  is an integral domain.*

*Proof.* Suppose that  $\mathfrak{p}$  is prime, and let  $(a + \mathfrak{p})(b + \mathfrak{p}) = ab + \mathfrak{p} = \mathfrak{p}$ . This gives us that  $ab \in \mathfrak{p}$  and hence  $a \in \mathfrak{p}$  or  $b \in \mathfrak{p}$ . Then either  $a + \mathfrak{p} = \mathfrak{p}$  or  $b + \mathfrak{p} = \mathfrak{p}$  in  $A/\mathfrak{p}$ . Conversely, if  $A/\mathfrak{p}$  is an integral domain, then for any  $a + \mathfrak{p}, b + \mathfrak{p}$   $ab + \mathfrak{p} = \mathfrak{p}$  implies that either  $a + \mathfrak{p} = \mathfrak{p}$  or  $b + \mathfrak{p} = \mathfrak{p}$ . Then  $a \in \mathfrak{p}$  or  $b \in \mathfrak{p}$ , only when  $ab \in \mathfrak{p}$ . This makes  $\mathfrak{p}$  prime. ■

**Corollary.** *Every maximal ideal is a prime ideal.*

**Example 1.5.** (1) The prime ideals of  $\mathbb{Z}$  are  $p\mathbb{Z}$ , where  $p$  is prime, which are the maximal ideals of  $\mathbb{Z}$ .

(2) The ideal  $(x)$  in  $\mathbb{Z}[x]$  is a prime ideal, but it is not maximal as  $(x) \subseteq (2, x) \subseteq \mathbb{Z}[x]$ .

**Definition.** Let  $A$  be a commutative ring with identity. We call  $A$  a **local ring** if it has one, and only one maximal ideal. We define the **residue field** of  $A$  to be the field  $k = A/\mathfrak{m}$ . We call a commutative ring with identity a **semi-local ring** if it has only finitely many maximal ideals.

**Example 1.6.** The ring  $\mathbb{Z}$  is not a local ring, it is not even semi-local, since every prime ideal  $(p)$  of  $\mathbb{Z}$ , where  $p \in \mathbb{Z}^+$  is prime, is also maximal.

**Lemma 1.4.5.** *Let  $A$  be a commutative ring with identity. Then the following are true.*

- (1) *If  $\mathfrak{m} \neq (1)$  is an ideal of  $A$  such that every element of  $A \setminus \mathfrak{m}$  is a unit, then  $A$  is a local ring having  $\mathfrak{m}$  as its maximal ideal.*
- (2) *If  $\mathfrak{m}$  is a maximal ideal of  $A$  such that every element of  $1 + \mathfrak{m}$  is a unit, then  $A$  is a local ring.*

*Proof.* Suppose that  $\mathfrak{m} \neq (1)$ . We have by lemma 1.4.2 that  $\mathfrak{m}$  is contained in a maximal ideal. Moreover,  $\mathfrak{m}$  contains no units by lemma 1.4.1. Since  $x \in A \setminus \mathfrak{m}$  is a unit, we get  $(x) = (1)$ , which makes  $\mathfrak{m}$  the only maximal ideal of  $A$  and  $A$  is a local ring.

Now, suppose that  $\mathfrak{m}$  is maximal, and take  $x \in A \setminus \mathfrak{m}$ . Then the ideal  $(x, \mathfrak{m}) = (1)$ , so that there exists a  $y \in A$ , and  $t \in \mathfrak{m}$  for which  $xy - t = 1$ ; i.e.  $xy = 1 - t$ , which makes  $x$  a unit. By above, this makes  $A$  a local ring. ■



# Bibliography

- [1] D. Dummit, *Abstract algebra*. Hoboken, NJ: John Wiley & Sons, Inc, 2004.
- [2] I. N. Herstein, *Topics in algebra*. New York: Wiley, 1975.