

MA3202

# Algebra II

Spring 2022

Satvik Saha  
19MS154

*Indian Institute of Science Education and Research, Kolkata,  
Mohanpur, West Bengal, 741246, India.*

## Contents

<b>1</b>	<b>Rings</b>	<b>2</b>
1.1	Basic definitions . . . . .	2
1.2	Subrings . . . . .	3
1.3	Ideals . . . . .	4
1.4	Integral domains . . . . .	5
1.5	Simple rings . . . . .	6
1.6	Homomorphisms and isomorphisms . . . . .	6
1.7	Quotient fields . . . . .	9
1.8	Prime and maximal ideals . . . . .	10
1.9	Divisibility . . . . .	11
1.10	Factorisation domains . . . . .	13
1.11	Principal ideal domains . . . . .	14
1.12	Euclidean domains . . . . .	15
1.13	Polynomial rings . . . . .	16
<b>2</b>	<b>Modules</b>	<b>17</b>
2.1	Basic definitions . . . . .	17

# 1 Rings

## 1.1 Basic definitions

**Definition 1.1.** A ring is a set  $R$  equipped with two binary operations, namely addition and multiplication, such that

1.  $(R, +)$  is an abelian group.
  - (a)  $a + b \in R$  for all  $a, b \in R$ .
  - (b)  $(a + b) + c = a + (b + c)$  for all  $a, b, c \in R$ .
  - (c)  $a + b = b + a$  for all  $a, b \in R$ .
  - (d) There exists  $0 \in R$  such that  $a + 0 = a$  for all  $a \in R$ .
  - (e) For each  $a \in R$ , there exists  $-a \in R$  such that  $a + (-a) = 0$ .
2.  $(R, \cdot)$  is a semi-group.
  - (a)  $a \cdot b \in R$  for all  $a, b \in R$ .
  - (b)  $(a \cdot b) \cdot c = a \cdot (b \cdot c)$  for all  $a, b, c \in R$ .
3. Multiplication distributes over addition.
  - (a)  $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$  for all  $a, b, c \in R$ .
  - (b)  $(b + c) \cdot a = (b \cdot a) + (c \cdot a)$  for all  $a, b, c \in R$ .

*Remark.* The following properties follow immediately,

1.  $0 \cdot a = 0$  for all  $a \in R$ .
2.  $(-a) \cdot b = -(a \cdot b) = a \cdot (-b)$  for all  $a, b \in R$ .
3.  $(na) \cdot b = n(a \cdot b) = a \cdot (nb)$  for all  $a, b \in R$ .

*Example.* The integers  $\mathbb{Z}$  form a ring, under the usual addition and multiplication.

*Example.* All fields, for instance the rational numbers  $\mathbb{Q}$  or the real numbers  $\mathbb{R}$ , are rings.

*Example.* The integers modulo  $n$ , namely  $\mathbb{Z}/n\mathbb{Z}$ , form a ring.

*Example.* If  $R$  is a ring, then the algebra of polynomials  $R[X]$  with coefficients from  $R$  form a ring.

*Example.* If  $R$  is a ring, then the  $n \times n$  matrices  $M_n(R)$  with entries from  $R$  form a ring.

**Definition 1.2.** If  $R$  is a ring and  $(R, \cdot)$  is a monoid i.e. has an identity, then this identity is unique and called the unity of the ring  $R$ . Such a ring  $R$  is called a unit ring. Note that we typically demand that this identity be distinct from the zero element.

*Example.* The even integers  $2\mathbb{Z}$  form a ring, but do not contain the identity.

*Example.* The trivial ring  $\{0\}$  is typically not considered to be a unit ring, since 0 must serve as the additive identity as well as the multiplicative identity.

**Definition 1.3.** If  $R$  is a ring and  $(R, \cdot)$  is commutative, then  $R$  is called a commutative ring.

**Definition 1.4.** Let  $R$  be a unit ring. An element  $a \in R$  is called a unit if there exists  $b \in R$  such that  $a \cdot b = 1 = b \cdot a$ . This  $b \in R$  is unique, and denoted by  $a^{-1}$ .

*Example.* The units in  $\mathbb{Z}$  are  $\{1, -1\}$ .

## 1.2 Subrings

**Definition 1.5.** Let  $R$  be a ring, and let  $S \subseteq R$ . We say  $S$  is a subring of  $R$  if the structure  $(S, +, \cdot)$  is a ring, with addition and multiplication inherited from  $R$ .

*Example.* The rings  $n\mathbb{Z}$  for  $n \in \mathbb{N}$  are all subrings of  $\mathbb{Z}$ .

*Example.* Consider the rings  $2\mathbb{Z} \subset \mathbb{Z}$ . Here,  $\mathbb{Z}$  is a unit ring but  $2\mathbb{Z}$  is not.

*Example.* Consider the rings  $4\mathbb{Z}/12\mathbb{Z} \subset 2\mathbb{Z}/12\mathbb{Z}$ . Here,  $2\mathbb{Z}/12\mathbb{Z}$  is not a unit ring but  $4\mathbb{Z}/12\mathbb{Z}$  is.

**Lemma 1.1.** Let  $S$  be a subring of  $R$ . Since  $(R, +)$  is an abelian group,  $(S, +)$  is a normal subgroup of  $(R, +)$ . Thus, we can make sense of the quotient group  $(R/S, +)$ .

**Lemma 1.2.** Let  $S$  be a subring of  $R$ . Then, the quotient  $(R/S, +, \cdot)$  is a ring with multiplication  $(a + S) \cdot (b + S) = ab + S$  if and only if  $ab - xy \in S$  for all  $a, b, x, y \in R$  such that the cosets  $a + S = x + S$ ,  $b + S = y + S$ .

*Example.* Consider the ring  $\mathbb{Z}$  and the subring  $n\mathbb{Z}$ . Then, the quotient  $\mathbb{Z}/n\mathbb{Z}$  is indeed a ring.

*Example.* Consider the ring  $\mathbb{Q}$  and the subring  $\mathbb{Z}$ . It can be shown that  $\mathbb{Q}/\mathbb{Z}$  is not a ring under the ‘natural’ multiplication.

### 1.3 Ideals

**Definition 1.6.** Let  $R$  be a ring and let  $I$  be a subset of  $R$ . We say that  $I$  is an ideal of  $R$  if  $(I, +)$  is a subgroup of  $(R, +)$ , and  $rx, xr \in I$  for all  $r \in R, x \in I$ .

*Example.* Consider the ring  $\mathbb{Z}$ , and the subring  $n\mathbb{Z}$ . This is an ideal of  $\mathbb{Z}$ , since  $m(n\mathbb{Z}) \subseteq n\mathbb{Z}$ . Indeed, every ideal of  $\mathbb{Z}$  is of the form  $n\mathbb{Z}$ . This will follow from Euclid's Division Lemma.

*Example.* The subsets  $\{0\}$  and  $R$  of any ring  $R$  are trivial ideals.

**Lemma 1.3.** Let  $R$  be a ring, and  $I$  be an ideal of  $R$ . Then, the quotient  $R/I$  is a ring.

*Proof.* Note that whenever  $a - x \in I, b - y \in I$ , we demand that  $ab - xy \in I$ . This can be rewritten as  $(a - x)b + x(b - y) \in I$ , which is clearly true by the properties of the ideal  $I$ .  $\square$

**Definition 1.7.** An ideal  $I \subset R$  is called finitely generated if there exist  $x_1, x_2, \dots, x_n \in I$  such that every element of  $I$  can be written as a finite linear combination

$$x = r_1x_1 + \dots + r_nx_n,$$

where  $r_i \in R$ . We denote  $I = (x_1, x_2, \dots, x_n)$ .

**Definition 1.8.** An ideal generated by a single element is called a principal ideal.

*Example.* Every ideal of  $\mathbb{Z}$  is a principal ideal.

**Lemma 1.4.** Let  $R$  be a unit ring, and  $I \subseteq R$  be an ideal. Then,  $I = R$  if and only if  $I$  contains the identity.

**Definition 1.9.** The sum of two ideals  $I, J \subset R$  is defined

$$I + J = \{x + y : x \in I, y \in J\}.$$

Their product is defined

$$IJ = \left\{ \sum_{i=1}^n x_i y_i : x_i \in I, y_i \in J \right\}.$$

**Lemma 1.5.** *The sum and product of two ideals of a ring are also ideals of that ring.*

**Lemma 1.6.** *Let  $I, J \subset R$  be ideals in the commutative ring  $R$ . Then,  $IJ \subset I \cap J$ .*

*Example.* Note that for  $2\mathbb{Z}, 2\mathbb{Z} \in \mathbb{Z}$ ,  $(2\mathbb{Z})(2\mathbb{Z}) = 4\mathbb{Z}$  but  $2\mathbb{Z} \cap 2\mathbb{Z} = 2\mathbb{Z}$ . A related example is  $R = 2\mathbb{Z}$ ,  $I = 4\mathbb{Z}$ ,  $J = 6\mathbb{Z}$ .

**Lemma 1.7.** *If  $I, J \subset R$  are ideals in a commutative unit ring  $R$ , and  $I + J = R$ , then  $IJ = I \cap J$ .*

*Proof.* We already know that  $IJ \subseteq I + J$ . Since  $I + J = R$ , we can pick  $x \in I, y \in J$  such that  $x + y = 1$ . Now pick  $a \in I \cap J$ , hence  $a \cdot 1 = ax + ay \in I \cap J$ ; but this is also an element of  $IJ$  proving  $I \cap J \subseteq IJ$ .  $\square$

## 1.4 Integral domains

**Definition 1.10.** Let  $R$  be a ring and  $a, b \in R$ ,  $a, b \neq 0$ . If  $ab = 0$ , we call  $a$  a left zero divisor and  $b$  a right zero divisor.

*Example.* Consider  $2, 3 \in \mathbb{Z}/6\mathbb{Z}$ ; then  $2 \cdot 3 = 6 \equiv 0$ .

**Definition 1.11.** A commutative ring  $R$  is called an integral domain if it has no zero divisors.

*Example.* When  $p$  is prime, the rings  $\mathbb{Z}/p\mathbb{Z}$  are integral domains. Note that this set is a group under both  $+$  and  $\cdot$ .

**Lemma 1.8.** *Every field is an integral domain.*

**Theorem 1.9.** *Every finite integral domain is a field.*

*Proof.* Let  $R = \{x_1, \dots, x_n\}$  be a finite integral domain. We first show that  $R$  contains an identity 1. Pick  $x \neq 0$ , and note that  $xx_1, xx_2, \dots, xx_n$  must all be distinct: otherwise  $xx_i = xx_j$  would force  $x(x_i - x_j) = 0$ . This forces  $x = xx_k$  for some  $x_k \neq 0$ . Now, we claim that  $x_k$  is our identity. Indeed, given any  $y \neq 0$ , we write  $y = xx_l$  for some  $x_l \neq 0$ , hence  $yx_k = xx_lx_k = x_l(xx_k) = x_lx = y$ .

Next, we show that every non-zero  $x \in R$  has an inverse. Indeed,  $1 = xx_k$  must be one of the  $xx_1, \dots, xx_n$ , hence  $1 = xx_m$  for some non-zero  $x_m$ . This means that  $x_m = x^{-1}$ .  $\square$

**Definition 1.12.** Let  $R$  be a ring. The characteristic of  $R$  is the smallest positive integer  $n$  such that  $nx = 0$  for all  $x \in R$ . If no such number  $n$  exists, we say that the characteristic of  $R$  is zero. We denote the characteristic of  $R$  by  $\text{ch}(R)$ .

*Example.* We have  $\text{ch}(\mathbb{Z}) = 0$ ,  $\text{ch}(\mathbb{Z}/n\mathbb{Z}) = n$ .

**Lemma 1.10.** Let  $R$  be a unit ring. Then,  $\text{ch}(R)$  is the smallest positive integer  $n$  such that  $n \cdot 1 = 0$ ; if no such  $n$  exists, then  $\text{ch}(R)$  is zero.

**Theorem 1.11.** Let  $R$  be an integral domain. Then,  $\text{ch}(R)$  is either zero or a prime.

*Proof.* Let  $R$  be an integral domain such that  $\text{ch}(R) = n \neq 0$ . If  $n$  is not a prime, write  $n = n_1 n_2$  for  $n_1, n_2 < n$ . Then for any non-zero  $x \in R$ , write  $0 = n(x^2) = (n_1 x)(n_2 x)$ . This forces one of  $n_1 x, n_2 x = 0$ ; say  $n_1 x = 0$ . Now for any  $y \in R$ , we have  $x(n_1 y) = (n_1 x)y = 0$ . Since  $x \neq 0$ , we have  $n_1 y = 0$  for all  $y \in R$ , contradicting the minimality of  $n$ .  $\square$

## 1.5 Simple rings

**Definition 1.13.** A simple ring is one which has no non-trivial ideals. We typically demand that multiplication in  $R$  is non-trivial.

**Lemma 1.12.** Every field is a simple ring.

*Proof.* If  $R$  is a field and  $I \subset R$  is an ideal with non-zero  $a \in I$ , then  $a^{-1} \in R$  hence  $a^{-1}a = 1 \in I$ . This immediately forces  $I = R$ .  $\square$

**Lemma 1.13.** If  $R$  is a commutative, simple, unit ring, then  $R$  is a field.

*Proof.* Pick non-zero  $a \in R$ , and set  $I = (a)$ . Since  $R$  is simple,  $I = R$ , hence  $1 \in I = (a)$ . In other words,  $1 = ab$  for some  $b \in R$ .  $\square$

## 1.6 Homomorphisms and isomorphisms

**Definition 1.14.** Let  $R, S$  be rings, and let  $\varphi: R \rightarrow S$ . We say that  $\varphi$  is a ring homomorphism if

1.  $\varphi(x + y) = \varphi(x) + \varphi(y)$  for all  $x, y \in R$ .
2.  $\varphi(xy) = \varphi(x)\varphi(y)$  for all  $x, y \in R$ .
3.  $\varphi(1_R) = 1_S$ .

We only insist on 3 if both  $R$  and  $S$  are unit rings.

*Remark.* The following properties follow immediately.

1.  $\varphi(0_R) = 0_S$ .
2.  $\varphi(-x) = -\varphi(x)$  for all  $x \in R$ .
3.  $\varphi(nx) = n\varphi(x)$  for all  $x \in R, n \in \mathbb{Z}$ .
4.  $\varphi(x - y) = \varphi(x) - \varphi(y)$  for all  $x, y \in R$ .

*Example.* The map  $\varphi: \mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}, k \mapsto k \bmod n$  is a homomorphism.

**Definition 1.15.** A bijective homomorphism between two rings is called an isomorphism. If an isomorphism exists between two rings, we say that they are isomorphic.

*Example.* The map  $\varphi: \mathbb{Z} \rightarrow n\mathbb{Z}, k \mapsto nk$  is an isomorphism.

*Example.* The map  $\varphi: \mathbb{C} \rightarrow \mathbb{C}, z \mapsto \bar{z}$  is an isomorphism.

*Example.* The rings  $\mathbb{Z}$  and  $\mathbb{Q}$  are not isomorphic. If there did exist an isomorphism  $\varphi: \mathbb{Q} \rightarrow \mathbb{Z}$ , then set  $a = \varphi(1/2)$ . We now demand  $a + a = \varphi(1/2 + 1/2) = 1$ ; but there is no such integer satisfying this property.

**Lemma 1.14.** *The only isomorphism  $\mathbb{Z} \rightarrow \mathbb{Z}$  is the identity map.*

**Theorem 1.15.** *The only isomorphism  $\mathbb{Q} \rightarrow \mathbb{Q}$  is the identity map.*

*Proof.* Let  $\varphi: \mathbb{Q} \rightarrow \mathbb{Q}$  be an isomorphism. We must have  $\varphi(1) = 1$ , which immediately gives  $\varphi(n) = n$  for all  $n \in \mathbb{Z}$ . Now for any rational  $p/q \in \mathbb{Q}$ , note that  $1 = \varphi(q \cdot 1/q) = q \cdot \varphi(1/q)$ , forcing  $\varphi(1/q) = 1/q$ . Thus,  $\varphi(p/q) = p/q$ , completing the proof.  $\square$

**Theorem 1.16.** *The only isomorphism  $\mathbb{R} \rightarrow \mathbb{R}$  is the identity map.*

*Proof.* Let  $\varphi: \mathbb{R} \rightarrow \mathbb{R}$  be an isomorphism. We must have  $\varphi(q) = q$  for all  $q \in \mathbb{Q}$ .

First we show that  $\varphi$  is strictly increasing. Note that when  $x > 0$ ,  $\varphi(x) = \varphi(\sqrt{x})^2 > 0$ . Thus when  $x > y$ ,  $\varphi(x - y) > 0$ , hence  $\varphi(x) > \varphi(y)$ .

Now let  $x \in \mathbb{R}$ ; if  $\varphi(x) \neq x$ , we must have one of  $\varphi(x) > x$  or  $\varphi(x) < x$ . Assume the former, and find  $q \in \mathbb{Q}$  such that  $\varphi(x) > q > x$ . Now,  $q > x$  gives  $q = \varphi(q) > \varphi(x)$ , a contradiction. An analogous argument gives a contradiction when  $\varphi(x) < x$ , completing the proof.  $\square$

**Theorem 1.17.** *The only homomorphism  $\mathbb{R} \rightarrow \mathbb{R}$  is the identity map.*

*Proof.* If  $\varphi: \mathbb{R} \rightarrow \mathbb{R}$  is a homomorphism, it is easy to check that  $\varphi^{-1}(0)$  is an ideal. Since  $\mathbb{R}$  is simple, this must be  $\{0\}$  or  $\mathbb{R}$ ; the latter can be ruled out since  $\varphi(1) = 1$ . In other words,  $\varphi^{-1} = \{0\}$  so  $\varphi$  is injective. Following the previous proof,  $\varphi$  must be an isomorphism, hence the identity map.  $\square$

**Theorem 1.18.** *The only isomorphisms  $\mathbb{C} \rightarrow \mathbb{C}$  which send  $\mathbb{R} \rightarrow \mathbb{R}$  are the maps  $z \mapsto z$  and  $z \mapsto \bar{z}$ .*

*Proof.* The previous theorem guarantees that any such isomorphism  $\varphi: \mathbb{C} \rightarrow \mathbb{C}$  is completely determined by  $\varphi(i)$ . Now,  $-1 = \varphi(-1) = \varphi(i)^2$ , forcing  $\varphi(i) = \pm i$ .  $\square$

**Lemma 1.19.** *The kernel of a ring homomorphism  $\varphi: R \rightarrow S$  is an ideal of  $R$ . Its image is a subring of  $S$ .*

*Proof.* If  $x \in \ker \varphi$ , then  $\varphi(x) = 0$ , hence for any  $r \in R$  we have  $\varphi(rx) = \varphi(r)\varphi(x) = 0$ . Thus,  $rx \in \ker \varphi$ . Also, recall that  $\varphi^{-1}(0)$  is an additive subgroup of  $R$ .  $\square$

**Theorem 1.20** (First isomorphism theorem). *Let  $\varphi: R \rightarrow S$  be a surjective ring homomorphism. Then,*

$$R/\ker \varphi \cong \text{im } \varphi.$$

*Proof.* Denote  $I = \ker \varphi$ , so the elements of  $R/I$  are the cosets  $x + I$  for  $x \in R$ . This gives us the natural map

$$\phi: R/I \rightarrow S, \quad x + I \mapsto \varphi(x).$$

It can be shown that this map is well defined: if  $x + I = y + I$ , then  $x - y \in I$  so  $\varphi(x - y) = 0$ , or  $\varphi(x) = \varphi(y)$ . Now,  $\phi((x + I) + (y + I)) = \varphi(x + y) = \varphi(x) + \varphi(y) = \phi(x + I) + \phi(y + I)$ , and  $\phi((x + I)(y + I)) = \varphi(xy) = \varphi(x)\varphi(y) = \phi(x + I)\phi(y + I)$ . Additionally, if  $R$  and  $S$  are both unit rings, then  $\phi(1_R + I) = \varphi(1_R) = 1_S$ . Thus,  $\phi$  is a homomorphism. It is obvious that  $\phi$  is surjective; also observe that  $\phi^{-1}(0) = 0 + I$ , hence  $\phi$  is also injective. This proves that  $\phi$  is an isomorphism, as desired.  $\square$

**Theorem 1.21.** *Let  $I, J \subset R$  be ideals. Then,*

$$(I + J)/J \cong I/(I \cap J).$$



*Proof.* The map  $\phi: I \rightarrow (I + J)/J$ ,  $x \mapsto x + J$  can be shown to be a surjective homomorphism. Its kernel consists of the elements in  $I$  that get mapped to  $0 + J$ , so  $\ker \phi = I \cap J$ . Applying the first isomorphism theorem gives the desired result.  $\square$

**Lemma 1.22.** *Let  $I \subset R$  be an ideal, and let  $\varphi: R \rightarrow S$  be a surjective ring homomorphism, then  $\varphi(I)$  is an ideal in  $S$ .*

**Theorem 1.23** (Correspondence theorem). *Let  $I \subset R$  be an ideal. Then there exists a one-to-one correspondence between the ideals of  $R$  containing  $I$  with the ideals of  $R/I$ .*

*Proof.* Use the surjective ring homomorphism  $\phi: R \rightarrow R/I$ ,  $x \mapsto x + I$ , which maps ideals in  $R$  to ideals in  $R/I$ . Furthermore, given ideals  $J, J' \subset R$  such that  $\varphi(J) = \varphi(J')$ , note that  $x \in J$  implies  $\varphi(x) \in \varphi(J) = \varphi(J')$  so  $x \in J'$ ; this shows that  $J = J'$ , hence our map is injective. Finally, given an ideal  $K$  in  $R/I$ , its pre-image under our map is the ideal  $L = \{x \in R : x + I \in K\}$ .  $\square$

**Theorem 1.24** (Chinese remainder theorem). *Let  $R$  be a commutative unit ring, and  $I, J \subset R$  be ideals such that  $I + J = R$ . Then,*

$$R/IJ \cong R/I \times R/J.$$

*Proof.* Consider the map

$$\varphi: R \rightarrow R/I \times R/J, \quad x \mapsto (x + I, x + J).$$

It is clear that this is a ring homomorphism. Furthermore,  $\varphi$  is surjective: to see this, pick  $a \in I$ ,  $b \in J$  such that  $a + b = 1$ . Then

$$\varphi(ay + bx) = (a(y - x) + x + I, b(x - y) + y + J) = (x + I, y + J).$$

Now, note that  $\varphi(x) = (I, J)$  forces  $x \in I \cap J$ ; but the latter is just  $IJ$  by a previous lemma. Applying the first isomorphism theorem gives the desired result.  $\square$

## 1.7 Quotient fields

We recall the standard construction of  $\mathbb{Q}$  from  $\mathbb{Z}$ , and generalize this to the construction of the field  $Q(R)$  from an integral domain  $R$ . Consider the equivalence relation on the set  $R \times R \setminus \{0\}$  defined by

$$(a, b) \sim (c, d) \iff ad = bc.$$

This partitions  $R \times R \setminus \{0\}$  into equivalence classes; let  $Q(R)$  be the collection of these equivalence classes. Now define addition and multiplication of elements from  $Q(R)$  as

$$[a, b] + [c, d] = [ad + bc, bd], \quad [a, b] \cdot [c, d] = [ac, bd].$$

It can be verified that this is well defined. Furthermore, we have an additive identity  $[0, a]$ , a multiplicative identity  $[a, a]$ , and every non-zero element  $[a, b]$  has a multiplicative inverse  $[b, a]$ . The remaining properties can be checked to show that  $Q(R)$  is a field. We can now embed  $R$  in  $Q(R)$  via the map

$$\iota: R \rightarrow Q(R), \quad x \mapsto [ax, a].$$

It can also be shown that  $Q(R)$  is the smallest field containing  $R$ . Indeed if  $j: R \rightarrow F$  is an embedding of  $R$  in the field  $F$ , we can embed  $Q(R)$  in  $F$  using the map  $[a, b] \mapsto j(a) \cdot j(b)^{-1}$ .

*Remark.* We do not require  $R$  to have a multiplicative identity!

**Definition 1.16.** The field  $Q(R)$  constructed as above is called the field of fractions, or quotient field of the integral domain  $R$ .

**Lemma 1.25.** *The field of fractions  $Q(R)$  is the smallest field containing the integral domain  $R$ .*

**Lemma 1.26.** *Let  $R_1, R_2$  be integral domains. If  $R_1 \cong R_2$ , then  $Q(R_1) \cong Q(R_2)$ .*

## 1.8 Prime and maximal ideals

**Definition 1.17.** An ideal  $I \subseteq R$  is called a prime ideal if it is proper, and  $xy \in I$  implies that at least one of  $x, y \in I$  for all  $x, y \in R$ .

**Lemma 1.27.** *An ideal  $I \subseteq R$  is prime if and only if  $JK \subset I$  forces either  $J \subset I$  or  $K \subset I$  for all ideals  $J, K \subseteq R$ .*

*Example.* The prime ideals of  $\mathbb{Z}$  are  $\{0\}$  and  $p\mathbb{Z}$

*Example.* A commutative ring is an integral domain if and only if  $\{0\}$  is a prime ideal.

**Theorem 1.28.** *Let  $R$  be a commutative ring, and  $I$  be a proper ideal. Then,  $I$  is a prime ideal if and only if  $R/I$  is an integral domain.*

*Example.* The quotients  $\mathbb{Z}/p\mathbb{Z}$  are integral domains precisely for primes  $p$ .

**Definition 1.18.** An ideal  $I \subseteq R$  is called maximal if it is proper, and for any ideal  $J \subseteq R$  with  $I \subseteq J \subseteq R$ , either  $J = I$  or  $J = R$ .

*Example.* The maximal ideals of  $\mathbb{Z}$  are  $p\mathbb{Z}$ .

**Theorem 1.29.** *Let  $R$  be a commutative unit ring, and  $I$  be a proper ideal. Then  $I$  is a maximal ideal if and only if  $R/I$  is a field.*

*Example.* Note that  $4\mathbb{Z}$  is a maximal ideal in  $2\mathbb{Z}$ , but  $2\mathbb{Z}/4\mathbb{Z}$  is not a field.

**Lemma 1.30.** *Let  $R$  be a commutative unit ring. Then every maximal ideal is prime.*

*Example.* Note that  $(X)$  is a prime ideal in  $\mathbb{Z}[X]$ , but not maximal.

**Definition 1.19.** A non-empty set  $S$  with a partial order  $\leq$  is called a partial ordered set, when we have

1.  $x \leq x$  for all  $x \in S$ .
2.  $x \leq y$  and  $y \leq x$  forces  $x = y$ .
3.  $x \leq y$  and  $y \leq z$  forces  $x \leq z$ .

**Definition 1.20.** A subset  $T$  of  $S$  is called a chain or totally ordered set if any two elements are comparable. In other words, given  $x, y \in T$ , at least one of  $x \leq y$  or  $y \leq x$ .

**Lemma 1.31** (Zorn's Lemma). *If  $S$  is a partially ordered set such that every chain  $C$  has an upper bound in  $S$ , then for every element  $x \in S$ , there exists a maximal element  $z \in S$  such that  $x \leq z$ .*

**Theorem 1.32.** *Let  $R$  be a commutative unit ring. Then  $R$  contains a maximal ideal.*

## 1.9 Divisibility

In this section, all rings are integral domains with a multiplicative identity.

**Definition 1.21.** Let  $a, b \in R$ ,  $a \neq 0$ . We say that  $a$  divides  $b$  if there exists  $c \in R$  such that  $b = ac$ . We denote this by  $a \mid b$ .

*Example.* In  $\mathbb{Z}[i]$ ,  $3 + i$  divides 10 because  $10 = (3 + i)(3 - i)$ .

**Lemma 1.33.** *If  $a, b \in R$ ,  $a \neq 0$ , then  $a \mid b$  if and only if  $(a) \supseteq (b)$ .*

**Lemma 1.34.** *Suppose that  $a \mid b$  and  $b \mid a$ . Then,  $b = ua$  for some unit  $u \in R$ .*

**Definition 1.22.** Two non-zero elements  $a, b \in R$  are called associates of each other if  $b = ua$  for some unit  $u \in R$ .

*Remark.* This defines an equivalence relation on  $R - \{0\}$ .

**Definition 1.23.** A non-zero non-unit element  $a \in R$  is said to be irreducible if  $a = bc$  forces either  $b, c$  to be a unit.

*Remark.* The only divisors of an irreducible element are its associates and units.

**Definition 1.24.** A non-zero non-unit element  $p \in R$  is said to be prime if for  $a, b \in R$ ,  $p \mid ab$  forces either  $p \mid a$ ,  $p \mid b$ .

**Lemma 1.35.** *All prime elements are irreducible.*

*Example.* Consider  $x = 1 + \sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$ ; this is irreducible, but not prime.

**Theorem 1.36.** *Let  $p \in R$  be non-zero. Then,  $p$  is a prime if and only if  $(p)$  is a prime ideal.*

**Theorem 1.37.** *Let  $x \in R$  be non-zero. Then,  $x$  is irreducible if  $(x)$  is maximal.*

*Example.* Note that  $X$  is irreducible in  $\mathbb{Z}[X]$ , but  $(X)$  is not maximal.

**Definition 1.25.** Let  $a, b \in R$  be non-zero. An element  $d \in R$  is called a greatest common divisor (gcd) of  $a$  and  $b$  if

1.  $d \mid a$  and  $d \mid b$ .
2.  $d' \mid a$  and  $d' \mid b$  forces  $d' \mid d$ .

**Definition 1.26.** Let  $a, b \in R$  be non-zero. An element  $l \in R$  is called a least common multiple (lcm) of  $a$  and  $b$  if

1.  $a \mid l$  and  $b \mid l$ .
2.  $a \mid l'$  and  $b \mid l'$  forces  $l \mid l'$ .

*Example.* Consider the ring  $\mathbb{Z}[\sqrt{-5}]$ , with  $a = 2(1 + \sqrt{-5})$ ,  $b = 6 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ . Then,  $a$  and  $b$  have no gcd or lcm.

**Lemma 1.38.** If the gcd of  $a$  and  $b$  does exist, then it is unique upto associates. The same applies for the lcm.

### 1.10 Factorisation domains

**Definition 1.27.** A unit integral domain  $R$  is called a factorisation domain if every non-zero, non-unit  $x \in R$  can be expressed as a unit times a product of irreducible elements, i.e.  $x = ux_1x_2 \dots x_n$  where  $u$  is a unit and each  $x_i$  is irreducible.

*Example.* The ring  $\mathbb{Z}[\sqrt{-5}]$  is a factorisation domain.

*Example.* Consider the ring of entire complex functions, i.e.

$$R = \left\{ \sum_{n=1}^{\infty} a_n z^n : a_n \in \mathbb{C}, \text{ the series converges for all } z \in \mathbb{C} \right\}.$$

Then,  $R$  is indeed a unit integral domain, and its units are those functions which vanish nowhere. Furthermore, its irreducible elements are the associates of linear polynomials  $z - a$ . Now if  $R$  were to be a factorisation domain, then every element would be an associate of a polynomial function, and thus have finitely many zeroes. However, the entire function  $\sin$  has infinitely many zeroes.

**Definition 1.28.** A unit integral domain  $R$  is called a unique factorisation domain if  $R$  is a factorisation domain and the factorisation of every element non-zero  $x \in R$  is unique upto associates.

*Example.* The ring of integers  $\mathbb{Z}$  is a unique factorisation domain.

*Example.* The ring  $\mathbb{Z}[\sqrt{-5}]$  is not a unique factorisation domain.

**Theorem 1.39.** *A unit integral domain  $R$  is a unique factorisation domain if and only if  $R$  is a factorisation domain in which every irreducible element is a prime.*

*Proof.* First suppose that  $R$  is a unique factorisation domain. Let  $x$  be an irreducible element in  $R$ , and let  $x \mid ab$ . We claim that  $x \mid a$  or  $x \mid b$ . Now,  $x \mid ab$  means that there exists  $y \in R$ ,  $xy = ab$ . We can factor  $a$  and  $b$ , and conclude that

$$xy = ab = (ua_1 \dots a_l)(vb_1 \dots b_m),$$

where  $u, v$  are units and  $a_i, b_j$  are all irreducible. Since  $R$  is a unique factorisation domain and the irreducible element  $x$  appears on the left, it must be an associate of one of the  $a_i, b_j$ . If  $x = wa_i$  for some unit  $w$ , then  $x \mid a_i$  hence  $x \mid a$ . Otherwise,  $x \mid b_j$  hence  $x \mid b$ .

Next suppose that  $R$  is a factorisation domain where every irreducible element is prime. Suppose that non-zero  $x \in R$  factorises into irreducible elements as

$$x = ux_1 \dots x_l = vy_1 \dots y_m.$$

Note that all  $x_i, y_j$  are primes. Suppose that  $l \leq m$ . Now  $x_1 \mid x$  implies that  $x_1 \mid vy_1 \dots y_m$ , hence  $x_1 \mid y_k$  for some  $y_k$ . Without loss of generality, let  $x_1 \mid y_1$ ; the irreducibility of  $y_1$  means that  $x_1 = u_1 y_1$  for some unit  $u_1$ . Thus,

$$uu_1 x_2 \dots x_l = vy_2 \dots y_m.$$

Continuing this process, we will reach  $w = vy_{l+1} \dots y_m$  for some unit  $w$ , which is a contradiction if  $l < m$ . Thus, we are forced to have  $l = m$ , and all  $x_i = u_i y_i$  for units  $u_i$ .  $\square$

**Lemma 1.40.** *Let  $R$  be a unique factorisation domain. Then, any two non-zero elements in  $R$  have a gcd and an lcm.*

## 1.11 Principal ideal domains

**Definition 1.29.** A unit integral domain  $R$  is called a principal ideal domain if every ideal of  $R$  is principal.

*Example.* The ring of integers  $\mathbb{Z}$  is a principal ideal domain.

**Theorem 1.41.** *Let  $R$  be a principal ideal domain, and let  $x \in R$  be non-zero. Then,  $x$  is irreducible if and only if  $(x)$  is maximal.*

**Corollary 1.41.1.** *Let  $R$  be a principal ideal domain. Then, every non-zero prime ideal is maximal.*

*Example.* Note that  $(0)$  is a prime ideal in  $\mathbb{Z}$ , but is not maximal.

**Lemma 1.42.** *Let  $R$  be a principal ideal domain. Then, every irreducible element is prime.*

**Theorem 1.43.** *Every principal ideal domain is a unique factorisation domain.*

**Corollary 1.43.1.** *Let  $R$  be a principal ideal domain. Then, any two non-zero elements in  $R$  have a gcd and an lcm.*

*Example.* The ring  $\mathbb{Z}[X]$  is a unique factorisation domain, but not a principal ideal domain.

## 1.12 Euclidean domains

**Definition 1.30.** An integral domain  $R$  is called a Euclidean domain if there is a map  $d: R - \{0\} \rightarrow \mathbb{Z}_{\geq 0}$  such that

1.  $d(a) \leq d(ab)$  for all non-zero  $a, b \in R$ .
2. For all  $a \in R$  and non-zero  $b \in R$ , there exist  $q, r \in R$  such that  $a = bq + r$  with either  $r = 0$  or  $d(r) < d(b)$ .

The map  $d$  is called the algorithm map and the second property is called the division algorithm.

*Example.* The ring of integers  $\mathbb{Z}$  is a Euclidean domain, with  $d(n) = |n|$ .

*Example.* The ring of Gaussian integers  $\mathbb{Z}[i]$  is a Euclidean domain, with  $d(a + ib) = a^2 + b^2$ .

*Example.* Every field is a Euclidean domain, with  $d(x) = 1$ .

**Lemma 1.44.** *Every ideal in a Euclidean domain is principal.*

*Proof.* Let  $R$  be a Euclidean domain, and let  $I \subseteq R$  be an ideal. If  $I = 0$ , we trivially have  $I = (0)$ . Thus, let  $I \neq 0$ , and choose non-zero  $a \in I$  such that  $d(a)$  is minimal. We claim that  $I = (a)$ . Indeed, let  $b \in I$ , and exhibit  $q, r \in R$  such that  $b = aq + r$ . This shows that  $r = b - aq \in I$ . Note that  $d(r) < d(a)$  contradicts the minimality of  $d(a)$ , hence we must have  $r = 0$ , and  $b = aq \in (a)$ . Thus,  $I = (a)$  as desired.  $\square$

**Lemma 1.45.** *Every Euclidean domain is a unit ring.*

*Proof.* The previous lemma shows that if  $R$  is a Euclidean domain, then  $R = (a)$  for some  $a \in R$ . Since  $a \in R$ , we must have  $a = a_0 a$  for some  $a_0 \in R$ . We claim that  $a_0$  is the identity in  $R$ . Indeed, for  $x \in R = (a)$ , we must have  $x = ra$  for some  $r \in R$ , hence  $x = ra_0 a = a_0(ra) = a_0 x$ .  $\square$

**Theorem 1.46.** *Every Euclidean domain is a principal ideal domain.*

*Example.* The ring  $\mathbb{Z}[(1 + \sqrt{19})/2]$  is a principal ideal domain, but not a Euclidean domain.

**Corollary 1.46.1.** *Every Euclidean domain is a unique factorisation domain.*

**Corollary 1.46.2.** *Let  $R$  be a Euclidean domain. Then, any two non-zero elements in  $R$  have a gcd and an lcm.*

**Lemma 1.47.** *Let  $R$  be a Euclidean domain, and let  $a, b \in R$ . If  $a$  is a proper divisor of  $b$ , then  $d(a) < d(b)$ .*

### 1.13 Polynomial rings

**Theorem 1.48** (Eisenstein's criterion). *Let  $R$  be a unique factorisation domain, and*

$$f(x) = \sum_{i=0}^n a_i x^i \in R[X].$$

*Suppose that there is a prime  $p \in R$  such that  $a \mid a_i$  for  $0 \leq i < n$ ,  $p \nmid a_n$ , and  $p^2 \nmid a_0$ . Then,  $f(x)$  is irreducible.*

**Corollary 1.48.1.** *Let  $p$  be a prime and let  $n > 1$ . Then,  $x^n - p \in \mathbb{Z}[X]$  is irreducible.*

**Lemma 1.49** (Gauss lemma). *Let  $R$  be a unique factorisation domain, and let  $F$  be the field of fractions of  $R$ . Let  $f(x) \in R[X]$  be irreducible in  $\mathbb{R}[X]$ . Then,  $f(x)$  is irreducible in  $F[X]$ .*

**Theorem 1.50** (Gauss theorem). *Let  $R$  be a unique factorisation domain. Then,  $R[X]$  is also a unique factorisation domain.*



## 2 Modules

### 2.1 Basic definitions

**Definition 2.1.** Let  $R$  be a ring. A left  $R$ -module is an abelian group  $(M, +)$  together with a map  $R \times M \rightarrow M$  given by  $(a, x) \mapsto ax$  such that for all  $a, b \in R$ ,  $m, n \in M$ , the following hold.

1.  $a(m + n) = am + an$ .
2.  $(a + b)m = am + bm$ .
3.  $a(bm) = (ab)m$ .
4.  $1m = m$ .

*Remark.* When  $R$  is commutative, we simply call this structure an  $R$ -module.

*Example.* Any abelian group is a  $\mathbb{Z}$ -module.

*Example.* Any vector space  $V$  over a field  $F$  is an  $F$ -module.

*Example.* Any ring  $R$  is an  $R$ -module over itself. Indeed, given an ideal  $I \subseteq R$ , we see that  $I$  is an  $R$ -module.

*Example.* Let  $M$  be an  $S$ -module. If  $\varphi: R \rightarrow S$  is a ring homomorphism, we can treat  $M$  as an  $R$ -module, with scalar multiplication  $(a, m) \mapsto \varphi(a)m$  for  $a \in R$ ,  $m \in M$ .

In particular,  $S$  is an  $R$ -module, with  $(r, s) \mapsto \varphi(r)s$  for  $r \in R$ ,  $s \in S$ .

Using this idea, suppose that  $I \subseteq R$  is an ideal, and  $\pi: R \rightarrow R/I$  is the canonical homomorphism. Then  $R/I$  is an  $R$ -module, with  $(r, s + I) \mapsto rs + I$  for  $r, s \in R$ .

**Definition 2.2.** Let  $M$  be a module. A subset  $N \subseteq M$  is called a submodule of  $M$  if  $N$  is a subgroup of  $(M, +)$ , and  $rx \in N$  for all  $r \in R$ ,  $x \in N$ .

*Example.* Any subspace of a vector space is a submodule.

*Example.* All polynomials of degree at most  $n$  is a submodule of the  $R$  module  $R[x]$ .

*Example.* The submodules of a commutative ring  $R$  are precisely the ideals of  $R$ .

**Definition 2.3.** Let  $R$  be a ring, and let  $M, N$  be  $R$ -modules. A map  $\varphi: M \rightarrow N$  is called a homomorphism if for all  $r \in R$ ,  $m, m' \in M$ , the following hold.

1.  $\varphi(m + m') = \varphi(m) + \varphi(m')$ .
2.  $\varphi(rm) = r\varphi(m)$ .

The set of all  $R$ -module homomorphisms  $\varphi: M \rightarrow N$  is denoted  $\text{Hom}_R(M, N)$ .

*Example.* Any linear transformation between vector spaces over a field  $F$  is a homomorphism of  $F$ -modules.

**Definition 2.4.** A bijective homomorphism is called an isomorphism.

**Definition 2.5.** A homomorphism  $\varphi: M \rightarrow M$  is called an endomorphism. The set of all  $R$ -module endomorphisms  $\varphi: M \rightarrow M$  is denoted  $\text{End}_R(M, M) = \text{Hom}_R(M, M)$ .

**Definition 2.6.** A bijective endomorphism is called an automorphism.

**Lemma 2.1.** Let  $\varphi: M \rightarrow N$  be a homomorphism of  $R$ -modules. Then, the following hold.

1. The set  $\ker \varphi$  is a submodule of  $M$ .
2. The set  $\text{im } \varphi$  is a submodule of  $N$ .
3. The map  $\varphi$  is injective if and only if  $\ker \varphi = \{0\}$ .

**Theorem 2.2.** Let  $M$  be an  $R$ -module, and  $N \subseteq M$  be a submodule. Then, the quotient group  $M/N$  is an  $R$ -module, with  $r[m] \mapsto [rm]$  for  $r \in R, m \in M$ .

**Theorem 2.3.** If  $\varphi \in \text{Hom}_R(M, M')$ , then  $M/\ker \varphi \cong \text{im } \varphi$ .