


The notes for this course are designed to be interactive. I encourage you to stop and work through the exercises as they appear in the text. Each week a certain number of the exercises will be collected as homework. As an additional resource, any example, theorem, corollary, etc. in [blue](#) has an instructional video corresponding to that content. These videos are posted under Modules in ICON.

### §1.1 THE DIVISION ALGORITHM

The goal of this section is to prove the Division Algorithm. Though this is an abstract algebra course, it is important to focus on the themes of arithmetic that the study of algebra heavily depends on. We will begin our study by focusing on division.

#### Well-Ordering Axiom

We will start with the set of all integers,  $\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$  with the usual order relation of ( $<$ ) on the set  $\mathbb{Z}$ . We will also assume the Well-Ordering Axiom, which is thus stated:

 **Well-Ordering Axiom** *Every nonempty subset of the nonnegative integers contains a smallest element.*

Whenever you read a mathematical statement, you should make sure it makes sense by considering some examples.

**Example** Let  $S = \{2k + 1 \mid k \in \mathbb{Z} \text{ with } k \geq 0\}$

Let's think about this set  $S$  by listing out its elements:

$$S = \{2(0) + 1, 2(1) + 1, 2(2) + 1, 2(3) + 1, \dots\} = \{1, 3, 5, 7, \dots\}$$

## Intro to Modern Algebra Part 1a: Course Notes

---

So  $S$  is the set of positive odd numbers. Since this is a subset of the nonnegative integers, the Well-Ordering Axiom tells us this set has a least element, namely 1.

### Division Algorithm

▶ **The Division Algorithm** Let  $a, b$  be integers with  $b > 0$ . Then there exist unique integers  $q$  and  $r$  such that

$$a = bq + r \quad \text{and} \quad 0 \leq r < b$$

Before we prove the division algorithm, let's do some examples to make sure the statement is clear.

▶ **Example 1.1.1 c** Find the quotient  $q$  and remainder  $r$  when  $a$  is divided by  $b$  without using a calculator.

(c)  $a = -17; b = 4$

*Answer:* We want to find  $q$  and  $r$  so that  $-17 = 4q + r$  where  $0 \leq r < 4$ .

If we let  $q = -5$  and  $r = 3$  then we see that  $4(-5) + 3 = -20 + 3 = -17$ .

**Example 1.1.2 b** Find the quotient  $q$  and remainder  $r$  when  $a$  is divided by  $b$  without using a calculator.

(b)  $a = 302; b = 19$

*Answer:* If we do the long division, we see that  $302 \div 19$  is 15 with a remainder of 17. Thus,  $302 = 19(15) + 17$ . so  $q = 15$  and  $r = 17$ .

▶ **Example 1.1.4 a,b** Use a calculator to find the quotient  $q$  and remainder  $r$  when  $a$  is divided by  $b$  without using a calculator.

(a)  $a = 8,126,493; b = 541$

*Answer:* If we do the long division on a calculator, we see that  $8,126,493 \div 541 = 15,021.244$ . This means that the quotient  $q = 15,021$ . To determine the remainder, we multiply  $15,021 \times 541 = 8,126,361$  and subtract this from  $8,126,493$ . So  $r = 8,126,493 - 8,126,361 = 132$ .

Thus,  $8,126,493 = 541(15,021) + 132$ .

(b)  $a = -9,217,645; b = 617$

*Answer:* If we do the long division on a calculator, we see that  $-9,217,645 \div 617 = -14,939.4571$ . We want our remainder to be positive. This means that the quotient  $q = -14,940$ . Next, we multiply  $-14,940 \times 617 = -9,217,980$  and subtract this from  $-9,217,645$ . So  $r = -9,217,645 - (-9,217,980) = 335$ .

Thus,  $-9,217,645 = 617(-14,940) + 335$ .

**Exercise 1.1.1 a,b** Find the quotient  $q$  and remainder  $r$  when  $a$  is divided by  $b$  without using a calculator.

(a)  $a = 17; b = 4$

(b)  $a = 0; b = 19$

**Exercise 1.1.2 a,c** Find the quotient  $q$  and remainder  $r$  when  $a$  is divided by  $b$  without using a calculator.

(a)  $a = -51; b = 6$

(c)  $a = 2000; b = 17$

**Exercise 1.1.3** Use a calculator to find the quotient  $q$  and remainder  $r$  when  $a$  is divided by  $b$ .

(a)  $a = 517; b = 83$

(b)  $a = -612; b = 74$

(c)  $a = 7,965,532; b = 127$

### Proof of Division Algorithm

Now that we have seen some examples of how to use the division algorithm, we will prove it formally. We will do this by splitting the proof into four steps.

Step 1: Let  $S$  be the set of integers of the form  $a - bx$  where  $x$  is an integer and  $a - bx \geq 0$ . Show that  $S$  is a nonempty set by finding a value for  $x$  such that  $a - bx \geq 0$ .

*Proof of Step 1:* We first show that  $a + b|a| \geq 0$ . Since  $b$  is a positive integer by hypothesis, we must have

$$b \geq 1$$

$$b|a| \geq |a| \quad [\text{Multiply both sides of the inequality by } |a|.]$$

$$b|a| \geq -a \quad [\text{Because } |a| \geq -a \text{ by the definition of absolute value.}]$$

$$a + b|a| \geq 0$$

Now let  $x = -|a|$ . Then

$$a - bx = a - b(-|a|) = a + b|a| \geq 0.$$

So,  $a - bx$  is in  $S$  when  $x = -|a|$ . This means that  $S$  is nonempty.  $\square$

Step 2: Find  $q$  and  $r$  such that  $a = bq + r$  and  $r \geq 0$ .

## Intro to Modern Algebra Part 1a: Course Notes

---

*Proof of Step 2:* In Step 1 we showed that  $S$  is a nonempty set. So by the Well-Ordering Axiom it must have a smallest element, let's call this element  $r$ . Since  $r \in S$ , we know that  $r \geq 0$  and  $r = a - bx$  for some  $x$ , say  $x = q$ . Thus,

$$r = a - bq \text{ and } r \geq 0, \quad \text{or, equivalently,} \quad a = bq + r \text{ and } r \geq 0. \quad \square$$

Step 3: Show that  $r < b$ .

*Proof of Step 3:* Now towards a contradiction, suppose  $r \geq b$ . Then  $r - b \geq 0$ , so we have

$$0 \leq r - b = (a - bq) - b = a - b(q + 1).$$

Since  $a - b(q + 1)$  is nonnegative, it is an element of  $S$  by definition. But since  $b$  is positive, it is certainly true that  $r - b < r$ . Thus

$$a - b(q + 1) = r - b < r.$$

This last inequality states that  $a - b(q + 1)$ , an element of  $S$ , is less than  $r$ , which is the *smallest* element of  $S$ . This is a contradiction. So we cannot have  $r \geq b$ , thus  $r < b$ . □

Step 4: Show that  $r$  and  $q$  are the only numbers with these properties.

*Proof of Step 4:* To prove uniqueness, we want to suppose there are integers  $q_1$  and  $r_1$  such that  $a = bq_1 + r_1$  and  $0 \leq r_1 < b$ , and show that  $q_1 = q$  and  $r_1 = r$ . Since  $a = bq + r$  and  $a = bq_1 + r_1$  we have

$$bq + r = bq_1 + r_1.$$

So

$$b(q - q_1) = r_1 - r. \quad (*)$$

Furthermore,

$$0 \leq r < b \quad \text{and} \quad 0 \leq r_1 < b.$$

If we multiply the first inequality by  $-1$  we get

$$-b < -r \leq 0 \quad \text{and} \quad 0 \leq r < b.$$

Adding these two inequalities gives,

$$\begin{array}{ll} -b < r_1 - r < b & \\ -b < b(q - q_1) < b & \text{[By Equation (*)]} \\ -1 < q - q_1 < 1 & \text{[Divide each term by } b \text{]} \end{array}$$

But  $q - q_1$  is an integer (because  $q$  and  $q_1$  are integers) and the only integer strictly between  $-1$  and  $1$  is  $0$ . Therefore  $q - q_1 = 0$  and  $q = q_1$ . Substituting  $q - q_1 = 0$  in Equation (\*) shows that  $r_1 - r = 0$  and so  $r = r_1$ . Thus the quotient and remainder are unique. ■

▶ **Example 1.1.5** Let  $a$  be any integer and let  $b$  and  $c$  be positive integers. Suppose that when  $a$  is divided by  $b$ , the quotient is  $q$  and the remainder is  $r$ , so that

$$a = bq + r \quad \text{and} \quad 0 \leq r < b.$$

If  $ac$  is divided by  $bc$ , show that the quotient is  $q$  and the remainder is  $rc$ .

*Answer:* We want to know what happens when  $ac$  is divided by  $bc$ , so first start by multiplying both the equation and the inequality by  $c$ . Then we have

$$ac = (bc)q + rc \quad \text{and} \quad 0 \leq rc < bc.$$

The division algorithm tells us that if  $ac$  is divided by  $bc$  the quotient is  $q$  and the remainder is  $rc$  as desired.

**Exercise 1.1.6** Let  $a, b, c$  and  $q$  be as in Exercise 1.1.5 of the text. Suppose that when  $q$  is divided by  $c$ , the quotient is  $k$ . Prove that when  $a$  is

divided by  $bc$ , then the quotient is also  $k$ .

▶ **Example 1.1.7** Prove that the square of an integer is either of the form  $3k$  or of the form  $3k + 1$  for some integer  $k$ . [*Hint*: By the Division Algorithm,  $a$  must be of the form  $3q$  or  $3q + 1$  or  $3q + 2$ .]

*Proof*: Let  $a \in \mathbb{Z}$  be given. If we apply the division algorithm with  $b = 3$ , there are unique integers  $q$  and  $r$  such that

$$a = 3q + r \quad \text{and} \quad 0 \leq r < 3.$$

Since  $0 \leq r < 3$ , we have  $r = 0, 1$ , or  $2$  and so  $a$  must be of the form  $3q, 3q + 1$ , or  $3q + 2$  for some integer  $q$ . We can consider each of these cases separately.

$$\underline{a = 3q}$$

$$a^2 = (3q)^2 = 9q^2 = 3(3q^2) = 3k \text{ where } k = 3q^2 \in \mathbb{Z}.$$

$$\underline{a = 3q + 1}$$

$$a^2 = (3q + 1)^2 = 9q^2 + 6q + 1 = 3(3q^2 + 2q) + 1 = 3k + 1 \text{ where } k = 3q^2 + 2q \in \mathbb{Z}.$$

$$\underline{a = 3q + 2}$$

$$a^2 = (3q + 2)^2 = 9q^2 + 12q + 4 = 3(3q^2 + 4q + 1) = 3k + 1 \text{ where } k = 3q^2 + 4q + 1 \in \mathbb{Z}$$

It follows from the above cases that the square of an integer is either of the form  $3k$  or  $3k + 1$  for some integer  $k$ . □

**Exercise 1.1.8** Use the Division Algorithm to prove that every odd integer is either of the form  $4k + 1$  or of the form  $4k + 3$  for some integer  $k$ .

**Exercise 1.1.9** Prove that the cube of any integer  $a$  has to be exactly one of these forms:  $9k$  or  $9k + 1$  or  $9k + 8$  for some integer  $k$ . [*Hint*: Adapt the hint in Exercise 1.1.7, and cube  $a$  in each case.]

**Exercise 1.1.10** Prove the following version of the Division Algorithm, which holds for both positive and negative divisors.

*Extended Division Algorithm:* Let  $a$  and  $b$  be integers with  $b \neq 0$ . Then there exist unique integers  $q$  and  $r$  such that  $a = bq + r$  and  $0 \leq r < |b|$ .

[*Hint*: Apply Theorem 1.1 when  $a$  is divided by  $|b|$ . Then consider two cases ( $b > 0$ ) and ( $b < 0$ ).]



### §1.2 DIVISIBILITY

Last section we discussed the division algorithm. This told us that given two integers  $a$  and  $b$  with  $b > 0$  there is a unique quotient  $q$  and remainder  $r$  so that  $a = bq + r$  with  $0 \leq r < b$ . In this section we focus on when the remainder  $r$  is 0. This happens when  $b$  is a factor of  $a$ . Let's begin with a formal definition of "divides."

#### Divisibility

Let  $a$  and  $b$  be integers with  $b \neq 0$ . We say that  $b$  **divides**  $a$  (or that  $b$  is a **divisor** of  $a$ , or that  $b$  is a **factor** of  $a$ ) if  $a = bc$  for some integer  $c$ . In symbols, " $b$  divides  $a$ " is written  $b \mid a$  and " $b$  does not divide  $a$ " is written  $b \nmid a$ .

Again, whenever you are introduced to a new definition, like the new statement and theorem in the last section, you should take some time understanding how it works.

**Example**  $3 \mid 24$  because  $24 = 3 \cdot 8$

**Example**  $3 \nmid 17$  because there is no such integer  $c$  where  $17 = 3c$

**Example**  $-6 \mid 54$  because  $54 = (-6)(-9)$

**Example**  $b \mid 0$  holds for any nonzero  $b$  since  $0 = 0 \cdot b$

Before we proceed consider the following remarks:

**Remark 1**  $a$  and  $-a$  have the same divisors

**Remark 2** every divisor of the nonzero integer  $a$  is less than or equal to  $|a|$

**Remark 3** a nonzero integer only has finitely many divisors

Since every nonzero integer has finitely many divisors, for small integers it is straightforward to list the divisors. Consider for example, the integer 24. All of its divisors are given by

$$1, -1, 2, -2, 3, -3, 4, -4, 6, -6, 8, -8, 12, -12, 24, -24.$$

Similarly, all of the divisors of 64 are

$$1, -1, 2, -2, 4, -4, 8, -8, 16, -16, 32, -32, 64, -64.$$

The **common divisors** of 24 and 64 are the numbers that appear in both lists of factors, that is

$$1, -1, 2, -2, 4, -4, 8, -8.$$

The largest of these common factors is called the *greatest common divisor*.

### Greatest Common Divisor

Let  $a, b$  be integers, not both 0. The **greatest common divisor (gcd)** of  $a$  and  $b$  is the largest integer  $d$  that divides both  $a$  and  $b$ . In other words,  $d$  is the gcd of  $a$  and  $b$  provided that

1.  $d \mid a$  and  $d \mid b$
2. if  $c \mid a$  and  $c \mid b$ , then  $c \leq d$

The greatest common divisor of  $a$  and  $b$  is unique and is usually denoted  $(a, b)$ .

In the example before the definition, we saw that  $(24, 64) = 8$ . If we consider 14 and 3 we have  $(3, 14) = 1$ . Two integers are said to be **relatively**

**prime** if their greatest common divisor is 1.

▶ **Theorem 1.2.2 (Bezout's Identity)** Let  $a$  and  $b$  be integers, not both 0, and let  $d$  be their greatest common divisor. Then there exist (not necessarily unique) integers  $u$  and  $v$  such that  $d = au + bv$ .

Consider the example above where we saw that  $(24, 64) = 8$ . Theorem 1.2.2 tells us that we can write 8 as a linear combination of 24 and 64. Indeed,

$$8 = 24(-5) + 64(2) \quad \text{and} \quad 8 = 24(3) + 64(-1).$$

Now we will prove Theorem 1.2.2 in two steps.

### Proof of Theorem 1.2.2

Step 1: Let  $S = \{am + bn \mid m, n \in \mathbb{Z}\}$  be the set of all linear combinations of  $a$  and  $b$ . Find the smallest element of  $S$ .

*Proof of Step 1:* First note that  $a^2 + b^2 = aa + bb \in S$  and  $a^2 + b^2 \geq 0$  since we assume  $a$  and  $b$  are both not zero. Thus  $S$  contains positive elements, so by the Well-Ordering Axiom it has a least positive element. Denote this smallest element by  $t$  where  $t = au + bv$  for some  $u, v \in \mathbb{Z}$ .  $\square$

Step 2: Prove that  $t$  is the gcd of  $a$  and  $b$ , that is,  $t = d$ .

*Proof of Step 2:* Now we have to show that  $t$  satisfies 1 and 2 from the definition of greatest common divisor. First we show that  $t \mid a$  and  $t \mid b$ . By the division algorithm, there exist integers  $q$  and  $r$  such that  $a = tq + r$  with

$0 \leq r < t$ . Thus,

$$r = a - tq$$

$$r = a - (au + bv)q$$

$$r = a - aqu - bvq$$

$$r = a(1 - qu) + b(-vq).$$

Thus  $r$  is a linear combination of  $a$  and  $b$ , so  $r \in S$ . Since  $r < t$ ,  $r$  cannot be positive since  $t$  is the smallest positive element in  $S$ . Since  $r \geq 0$  this implies that  $r = 0$ . Thus

$$a = tq + r = tq + 0 = tq$$

so  $t \mid a$ . A similar argument shows that  $t \mid b$ . Thus  $t$  is a common divisor of  $a$  and  $b$ .

Now we want to show that  $t$  is unique, that is, if  $c$  is any other common divisor of  $a$  and  $b$ , then  $c \leq t$ . Since  $c \mid a$  and  $c \mid b$  we have that  $a = ck$  and  $b = cl$  for some  $k, l \in \mathbb{Z}$ . Thus we have

$$t = au + bv$$

$$= (ck)u + (cl)v$$

$$= c(ku + lv)$$

The first and last terms show that  $c \mid t$ . Since every divisor of  $t$  is less than or equal to  $|t|$  we have  $c \leq |t| \leq t$  since  $t$  is positive. It follows that  $t$  is the greatest common divisor  $d$ . ■

**Example 1.2.14 a** Find the smallest positive integer in the given set.

(a)  $\{6u + 15v \mid u, v \in \mathbb{Z}\}$

*Answer:* Note that  $(6, 15) = 3$ . Theorem 1.2.2 tells us that we can write the greatest common divisor 3 of 6 and 15 as a linear combination  $d = 6x + 15y$  where  $x, y \in \mathbb{Z}$ . Furthermore, from the proof of Theorem 1.2.2 we see that the gcd of 6 and 15 will be the smallest

positive element of the set. So 3 is an element of the set, in fact it is the smallest positive element of the set.

**Exercise 1.2.14 b** Find the smallest positive integer in the given set.

(b)  $\{12r + 17s \mid r, s \in \mathbb{Z}\}$

### Euclidean Algorithm

We introduce the Euclidean Algorithm with the following example.

**Example 1.2.15 a** The *Euclidean Algorithm* is an efficient way to find  $(a, b)$  for any positive integers  $a$  and  $b$ . It only requires you to apply the Division Algorithm several times until you reach the gcd, as illustrated here for  $(524, 148)$ .

(a) Verify that the following statements are correct.

$$\begin{array}{ll} 524 = 148 \cdot 3 + 80 & 0 \leq 80 < 148 \\ 148 = 80 \cdot 1 + 68 & 0 \leq 68 < 80 \\ 80 = 68 \cdot 1 + 12 & 0 \leq 12 < 68 \\ 68 = 12 \cdot 5 + 8 & 0 \leq 8 < 12 \\ 12 = 8 \cdot 1 + 4 & 0 \leq 4 < 8 \\ 8 = 4 \cdot 2 + 0 & \end{array}$$

Note that the divisor in each line becomes the dividend in the next line, and the remainder in each line becomes the divisor in the next line. Here the  $(524, 148) = 4$ . This is the same as the last nonzero remainder, namely 4.

(c) Use the Euclidean Algorithm to find  $(1003, 456)$ .

$$1003 = 456 \cdot 2 + 91 \qquad 0 \leq 91 < 456$$

$$456 = 91 \cdot 5 + 1 \qquad 0 \leq 1 < 91$$

$$91 = 1 \cdot 91 + 0$$

So  $(1003, 456) = 1$  since 1 is the last nonzero remainder. Recall this means that 1003 and 456 are relatively prime.

### Exercise 1.2.15 d-j

(d) Use the Euclidean Algorithm to find  $(322, 148)$

(e) Use the Euclidean Algorithm to find  $(5858, 1436)$

The equations in part (a) can be used to express the gcd 4 as a linear combination of 524 and 148 as follows. First, rearrange the first 5 equations in part (a), as shown below.

$$80 = 452 - 148 \cdot 3 \tag{1}$$

$$68 = 148 - 80 \tag{2}$$

$$12 = 80 - 68 \cdot 3 \tag{3}$$

$$8 = 68 - 12 \cdot 5 \tag{4}$$

$$4 = 12 - 8 \tag{5}$$


(f) Equation (1) expresses 80 as a linear combination of 524 and 148. Use this fact and Equation (2) to write 68 as a linear combination of 524 and 148.

(g) Use Equation (1), part (f), and Equation (3) to write 12 as a linear combination of 524 and 148.

(h) Use parts (f) and (g) to write 8 as a linear combination of 524 and 148.

- (i) Use parts (g) and (h) to write the gcd 4 as a linear combination of 524 and 148 as desired.
- (j) Use the method described in parts (f)-(i) to express the gcd in part (c) as a linear combination of 1003 and 456.

### Properties of the Greatest Common Divisor

 **Corollary 1.2.3** Let  $a$  and  $b$  be integers, not both 0, and let  $d$  be a positive integer. Then  $d$  is the greatest common divisor of  $a$  and  $b$  if and only if  $d$  satisfies these conditions:

1.  $d \mid a$  and  $d \mid b$
2. if  $c \mid a$  and  $c \mid b$ , then  $c \mid d$

### Proof of Corollary 1.2.3

We will prove this in two steps because of the if and only if.

Step 1 Prove if  $d = (a, b)$  then  $d$  satisfies conditions 1 and 2.

Suppose  $d = (a, b)$ , then  $d \mid a$  and  $d \mid b$ . So condition 1 is satisfied. Now suppose there is an integer  $c$  such that  $c \mid a$  and  $c \mid b$ . Then there exist integers  $x$  and  $y$  such that  $a = cx$  and  $b = cy$ . Also, by Theorem 1.1.2 we can write  $d$  as a linear combination of  $a$  and  $b$ , so we have

$$d = au + bv = (cx)u + (cy)v = c(xu + yv)$$

so  $d \mid c$ . Thus  $d$  satisfies condition 2. □

Step 2 Prove if  $d$  is a positive integer that satisfies conditions 1 and 2 then  $d = (a, b)$ .

## Intro to Modern Algebra Part 1a: Course Notes

---

Condition 1 is the same as the first condition in the definition of greatest common divisor introduced earlier in this section. If there is some integer  $c$  with  $c \mid a$  and  $c \mid b$  then condition 2 gives that  $c \mid d$ . Since  $c$  is a divisor of  $d$  we have that  $c \leq |d| \leq d$  since  $d$  is positive. So  $d$  satisfies the second condition in the definition of the greatest common divisor. It follows that  $(a, b) = d$ . ■

**Theorem 1.2.4** If  $a \mid bc$  and  $(a, b) = 1$ , then  $a \mid c$ .

*Proof of Theorem 1.2.4* We know that  $(a, b) = 1$ , then by Bezout's Identity we can write 1 as a linear combination of  $a$  and  $b$ , say  $1 = au + bv$  for some integers  $u$  and  $v$ . Also,  $a \mid bc$  implies  $bc = ar$  for some integer  $r$ . Using this and multiplying this equation by  $c$  we have

$$c = acu + bcv = acu + arv = a(cu + rv).$$

It follows that  $a \mid c$ . □

**Exercise 1.2.17** Suppose  $(a, b) = 1$ . If  $a \mid c$  and  $b \mid c$ , prove that  $ab \mid c$ . [Hint:  $c = bt$  (Why?), so  $a \mid bt$ . Use Theorem 1.2.4.]

▶ **Example 1.2.19** If  $a \mid (b + c)$  and  $(b, c) = 1$ , prove that  $(a, b) = 1 = (a, c)$ .

*Proof:* First we show that  $(a, b) = 1$ . Suppose  $d$  is a common divisor of  $a$  and  $b$ . Then  $d \mid a$  implies  $a = ds$  for some integer  $s$  and  $d \mid b$  implies  $b = dt$  for some integer  $t$ . Similarly, since  $a \mid b + c$  we can say that  $b + c = ak$  for some integer  $k$ . Rewriting this equation we have

$$c = ak - b = (ds)k - dt = d(sk - t)$$

so  $d \mid c$ . Thus we have  $d$  is a common divisor of  $b$  and  $c$ . Since we assume  $(b, c) = 1$  it follows that  $d = 1$ .



## Intro to Modern Algebra Part 1a: Course Notes

---

To see that  $a$  and  $c$  are relatively prime. Note that  $(b, c) = 1$  implies that  $1 = bx + cy$  for some integers  $x$  and  $y$ . Then we have

$$1 = bx + cy = (ak - c)x + cy = akx - cx + cy = a(kx) + c(-x + y).$$

If we let  $m = kx$  and  $n = -x + y$  then we have integer solutions to the equation  $1 = am + cn$ . Thus  $(a, c) = 1$ . □

**Exercise 1.2.21** Prove that  $(a, b) = (a, b + at)$  for every  $t \in \mathbb{Z}$ .

**Exercise 1.2.22** If  $(a, c) = 1$  and  $(b, c) = 1$ , prove that  $(ab, c) = 1$ .

**Example 1.2.28** Prove that a positive integer is divisible by 3 if and only if the sum of its digits is divisible by 3. [*Hint*:  $10^3 = 999 + 1$  and similarly for other powers of 10.]

*Proof*: Let  $x$  be a positive integer. Note that we can write  $x$  as its decimal expansion  $x = a_0a_1 \dots a_n$ . This implies that

$$\begin{aligned} x &= a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 + \dots + a_n \cdot 10^n \\ &= a_0 + a_1(9 + 1) + a_2(99 + 1) + \dots + a_n(\underbrace{9 \dots 9}_{n \text{ times}} + 1) \\ &= a_0 + 9a_1 + a_1 + 99a_2 + a_2 + \dots + \underbrace{9 \dots 9}_{n \text{ times}} a_n + a_n \\ &= \underbrace{(a_0 + a_1 + \dots + a_n)}_s + (9a_1 + 99a_2 + \dots + \underbrace{9 \dots 9}_{n \text{ times}} a_n) \end{aligned}$$

Note that the first group of terms  $s$  represents the sum of the digits of  $x$ . If  $x$  is divisible by 3 then because the right group of terms is divisible by 3 (each term is divisible by 9 and thus 3), then  $s$  must be divisible by 3. Conversely, if the sum of the digits of  $x$  is divisible by 3, we see from above that each group of terms in the decimal expansion of  $x$  is divisible by 3 so  $x$  must also be divisible by 3. □

**Exercise 1.2.29** Prove that a positive integer is divisible by 9 if and only if the sum of its digits is divisible by 9. [See Exercise 28.]

## §1.3 PRIMES AND UNIQUE FACTORIZATION


### Primality

Now we begin our discussion on prime numbers. Prime numbers are very important because they serve as the multiplicative building blocks of the integers. In this section we will show that every integer that is nonzero other than  $\pm 1$  can be written uniquely as the product of primes.

An integer  $p$  is said to be **prime** if  $p \neq 0, \pm 1$  and the only divisors of  $p$  are  $\pm 1$  and  $\pm p$ .

**Remark 4:**  $p$  is prime if and only if  $-p$  is prime


**Remark 5:** if  $p$  and  $q$  are prime and  $p \mid q$ , then  $p = \pm q$

 **Theorem 1.3.5** Let  $p$  be an integer with  $p \neq 0, \pm 1$ . Then  $p$  is prime if and only if  $p$  has this property:


whenever  $p \mid bc$ , then  $p \mid b$  or  $p \mid c$ .

*Proof of Theorem 1.3.5:* First assume  $p$  is prime and that  $p \mid bc$ . Let  $d = (p, b)$ . Then  $d$  must be a positive divisor of the prime  $p$ . Thus the only possibilities are  $(p, b) = 1$  and  $(p, b) = \pm p$  (whichever is positive.) If  $(p, b) = \pm p$ , then  $p \mid b$ . If  $(p, b) = 1$ , since  $p \mid bc$ , we must have  $p \mid c$  by Theorem 1.2.4. Thus in either case,  $p \mid b$  or  $p \mid c$ . Now assume that if  $p \mid bc$  then  $p \mid b$  or  $p \mid c$ . Please see **Exercise 1.3.7** to complete the proof.  $\square$

**Exercise 1.3.7** If  $a, b, c$  are integers and  $p$  is a prime that divides both  $a$  and  $a + bc$ , prove that  $p \mid b$  or  $p \mid c$ .

 **Corollary 1.3.6** If  $p$  is prime and  $p \mid a_1 a_2 \cdots a_n$ , then  $p$  divides at least one of the  $a_i$ .

*Proof of Corollary 1.3.6:* Let  $p$  be prime such that  $p \mid a_1 a_2 \cdots a_n$  and consider the product  $(a_1 a_2 \cdots a_n) = a_1(a_2 a_3 \cdots a_n)$ . Then by Theorem 1.3.5  $p \mid a_1$  or  $p \mid a_2 a_3 \cdots a_n$ . If  $p \mid a_1$  then we are done. Otherwise if  $p \mid a_2(a_3 a_4 \cdots a_n)$  we have that  $p \mid a_2$  or  $p \mid a_3 a_4 \cdots a_n$ . We can continue in this way until we find some  $a_i$  such that  $p \mid a_i$ . This will take at most  $n$  steps. □

 **Example 1.3.15** If  $p$  is prime and  $p \mid a^n$ , is it true that  $p^n \mid a^n$ ? Justify your answer.


*Answer:* Note that  $a^n = \underbrace{a \cdots a}_{n \text{ times}}$ . So if  $p \mid a^n$  by Corollary 1.3.6 we must have  $p \mid a$ . Thus  $a = pk$  for some integer  $k$ . Then  $a^n = (pk)^n = p^n k^n$ . It follows that  $p^n \mid a^n$ .

**Exercise 1.3.7** If  $a, b, c$  are integers and  $p$  is a prime that divides both  $a$  and  $a + bc$ , prove that  $p \mid b$  or  $p \mid c$ .

**Exercise 1.3.17** If  $p$  is prime and  $(a, b) = p$ , then  $(a^2, b^2) = ?$

**Exercise 1.3.18** Prove or disprove each of the following statements:

- (a) If  $p$  is prime and  $p \mid (a^2 + b^2)$  and  $p \mid (c^2 + d^2)$ , then  $p \mid (a^2 - c^2)$ .
- (b) If  $p$  is prime and  $p \mid (a^2 + b^2)$  and  $p \mid (c^2 + d^2)$ , then  $p \mid (a^2 + c^2)$ .
- (c) If  $p$  is prime and  $p \mid a$  and  $p \mid (a^2 + b^2)$ , then  $p \mid b$ .

 **Theorem 1.3.7** Every integer  $n$  except  $0, \pm 1$  is a product of primes.

*Proof of Theorem 1.3.7* First assume that  $n > 1$ . Let  $S$  be the set of all integers greater than 1 that are not a product of primes. We want to show that  $S$  is an empty set. Towards a contradiction, suppose that  $S$  is a nonempty set. By the Well-Ordering Axiom,  $S$  must have a smallest element, call it  $m$ . Since  $m$  is not prime, it must have some positive divisors, say  $m = ab$  for  $a, b \in \mathbb{Z}$ . Note that  $1 < a < m$  and  $1 < b < m$ . Since  $m$  is the smallest element of  $S$  that implies that  $a$  and  $b$  are not in  $S$ .

Recall that  $S$  is the set of all integers greater than 1 that are not a product of primes, so  $a, b \notin S$  implies that both  $a$  and  $b$  must be the product of primes, so


$$a = p_1 p_2 \cdots p_r \text{ and } b = q_1 q_2 \cdots q_s$$

where  $r \geq 1$  and  $s \geq 1$  and each  $p_i$  and  $q_j$  is prime. But then

$$m = ab = p_1 p_2 \cdots p_r q_1 q_2 \cdots q_s$$

is a product of prime numbers, a contradiction. So we cannot have  $S$  be nonempty.  $S$  empty implies that every integer  $n > 1$  is a product of primes. This argument also holds for  $-n$ . □

## Fundamental Theorem of Arithmetic

 **The Fundamental Theorem of Arithmetic** Every integer  $n$  except  $0, \pm 1$  is a product of primes. This prime factorization is unique in the following sense: If

$$n = p_1 p_2 \cdots p_r \text{ and } n = q_1 q_2 \cdots q_s$$

with each  $p_i, q_j$  prime, then  $r = s$  (that is, the number of factors is the same) and after reordering and relabeling the  $q$ 's,

$$p_1 = \pm q_1, \quad p_2 = \pm q_2, \quad p_3 = \pm q_3, \dots, p_r = \pm q_r$$

*Proof of Fundamental Theorem of Arithmetic:* We saw in Theorem 1.3.7 that every integer  $n$  except  $0, \pm 1$  can be factored into the product of primes. So any given integer  $n$  has at least one factorization into primes, say  $n = p_1 p_2 \cdots p_r$ . Suppose there exists another factorization of  $n$  into the product of primes where  $n = q_1 q_2 \cdots q_s$ . We want to show that  $r = s$  and after a relabeling the  $p_i = \pm q_j$ .

Since we have two factorizations of  $n$  into the product of primes we can set them equal to one another. So

$$p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s,$$

and  $p_1(p_2 \cdots p_r) = q_1 q_2 \cdots q_s$  implies that  $p_1 \mid q_1 q_2 \cdots q_s$ , by Corollary 1.3.6. We can assume that  $p_1 \mid q_1$ . Thus  $p_1 = \pm q_1$ .

Substituting we now have  $\pm q_1 p_2 p_3 \cdots p_r = q_1 q_2 q_3 \cdots q_s$ . If we divide both sides by  $q_1$  we have

$$p_2(\pm p_3 p_4 \cdots p_r) = q_2 q_3 q_4 \cdots q_s.$$

Thus,  $p_2 \mid q_2 q_3 \cdots q_s$ . By Corollary 1.3.6,  $p_2$  must divide one of the  $q_j$ , assume  $p_2 \mid q_2$ . Then  $p_2 = \pm q_2$  and

$$\pm q_2 p_3 p_4 \cdots p_r = q_2 q_3 q_4 \cdots q_s.$$

If we divide both sides by  $q_2$  we have that

$$p_3(\pm p_4 \cdots p_r) = q_3 q_4 \cdots q_s.$$

We can continue in this manner eliminating one prime on each side at every step. If  $r = s$  then this process will lead to the conclusion that  $p_1 = \pm q_1$ ,  $p_2 = \pm q_2, \dots, p_r = \pm q_r$ .

Towards a contradiction assume that  $r > s$ . Then after  $s$  steps we will eliminate all the  $q_j$  and will have an equation of the form

$$\pm p_{s+1} p_{s+2} \cdots p_r = 1.$$

This implies that  $p_r \mid 1$ . Since the only divisors of 1 are  $\pm 1$ , this implies that  $p_r = \pm 1$ . But  $p_r$  is prime, so this is not possible. We arrive at a similar contradiction if we assume that  $r < s$ . Thus  $r = s$  as desired.  $\square$

**Corollary 1.3.9** Every integer  $n > 1$  can be written in one and only one way in the form  $n = p_1 p_2 p_3 \cdots p_r$ , where the  $p_i$  are positive primes such that  $p_1 \leq p_2 \leq p_3 \leq \cdots \leq p_r$ .

**Example 1.3.1 a** Express 5040 as a product of primes.

*Answer*

$$\begin{aligned} 5040 &= 56 \cdot 9 \\ &= 8 \cdot 7 \cdot 3 \cdot 3 \\ &= 2 \cdot 2 \cdot 2 \cdot 7 \cdot 3 \cdot 3 \end{aligned}$$

**Exercise 1.3.1 b,c** Express each number as a product of primes.

(b) -2345

(c) 45,670

**Exercise 1.3.4** Primes  $p$  and  $q$  are said to be *twin primes* if  $q = p + 2$ . For example, 3 and 5 are twin primes; so are 11 and 13. Find all pairs of positive twin primes less than 200.

### Primality Testing

We are often concerned with determining whether a given number is prime. The following theorem gives us a way to do this for relatively small numbers.

▶ **Theorem 1.3.10** Let  $n > 1$ . If  $n$  has no positive prime factor less than or equal to  $\sqrt{n}$ , then  $n$  is prime.

*Proof of Theorem 1.3.10:* Towards a contradiction, suppose that  $n$  is not prime. Then  $n$  is composite which implies that  $n$  has at least two positive prime factors, say  $p_1$  and  $p_2$ , so that  $n = p_1 p_2 k$  for some  $k \in \mathbb{Z}$ . We assume that  $n$  has no positive prime factors less than or equal to  $\sqrt{n}$ , so we must have that  $p_1 > \sqrt{n}$  and  $p_2 > \sqrt{n}$ . Thus,

$$n = p_1 p_2 k \geq p_1 p_2 > \sqrt{n} \sqrt{n} = n.$$

We cannot have  $n$  strictly greater than itself. Since assuming that  $n$  is not prime leads to a contradiction, we conclude that  $n$  is prime.  $\square$

▶ **Example 1.3.3 a** Is 701 prime?

*Answer:* Theorem 1.3.10 tells us that 701 is prime if none of the prime numbers less than or equal to  $\sqrt{701} = 26.476$  divide 701. So we need to check if 2, 3, 5, 7, 11, 13, 17, 19, and 23 divide 701. None of these divide 701, so **701 is prime**.

**Exercise 1.3.3 b,c,d** Which of the following numbers are prime?



(b) 1009

(c) 1949

(d) 1951

## §2.1 CONGRUENCE AND CONGRUENCE CLASSES

### Congruence

▶ Let  $a, b, n$  be integers with  $n > 0$ . Then  **$a$  is congruent to  $b$  modulo  $n$** , written  $a \equiv b \pmod{n}$ , if  $n \mid a - b$ .

▶ **Example**  $17 \equiv 5 \pmod{6}$  because  $6 \mid (17 - 5) = 12$

▶ **Example**  $7 \equiv -3 \pmod{5}$  because  $5 \mid (7 - (-3)) = 10$

**Exercise** Prove that  $a \equiv b \pmod{n}$  if and only if  $a = b + nk$  for some  $k \in \mathbb{Z}$ .

**Exercise 2.1.1 a,b** Show that  $a^{p-1} \equiv 1 \pmod{p}$  for the given  $p$  and  $a$ :

(a)  $a = 2, p = 5$

(b)  $a = 4, p = 7$

**Exercise 2.1.3** Every published book has a ten-digit ISBN-10 number (on the back cover or the copyright page) that is usually of the form  $x_1 - x_2x_3x_4 - x_5x_6x_7x_8x_9 - x_{10}$  (where each  $x_i$  is a single digit). Sometimes the last digit of an ISBN number is the letter X. In such cases, treat X as if it were the number 10. The first 9 digits identify the book. The last digit  $x_{10}$  is a *check digit*; it is chosen so that

$$10x_1 + 9x_2 + 8x_3 + 7x_4 + 6x_5 + 5x_6 + 4x_7 + 3x_8 + 2x_9 + x_{10} \equiv 0 \pmod{11}$$

If an error is made when scanning or keying an ISBN number into a computer, the left side of the congruence will not be congruent to 0 modulo 11, and the number will be rejected as invalid. Which of the following are apparently valid ISBN numbers?

(a) 3-540-90518-9

(b) 0-031-10559-5

(c) 0-385-49596

### Congruence as an Equivalence Relation

One goal of this section is to show that congruence is an equivalence relation. In fact, if you look at the congruence sign, it looks a lot like an equals sign. There are several properties of equality that are important.

**reflexive:**  $a = a$  for every integer  $a$

**symmetric:** if  $a = b$  then  $b = a$

**transitive:** if  $a = b$  and  $b = c$ , then  $a = c$

Whenever a relation, that is the way we relate two elements together, satisfies the three conditions above, it is called an equivalence relation. Thus equality is an equivalence relation. It turns out that congruence is also an equivalence relation. It is reflexive, symmetric, and reflexive.



**Theorem 2.1.1 Congruence as an Equivalence Relation** Let  $n$  be a positive integer. For all  $a, b, c \in \mathbb{Z}$ ,

1.  $a \equiv a \pmod{n}$ ;
2. if  $a \equiv b \pmod{n}$ , then  $b \equiv a \pmod{n}$ ;
3. if  $a \equiv b \pmod{n}$  and  $b \equiv c \pmod{n}$ , then  $a \equiv c \pmod{n}$ .

*Proof of Theorem 2.1.1:* We need to show that congruence is reflexive, symmetric, and transitive.

reflexive: We want to show that  $a \equiv a \pmod{n}$ , which is the same as showing that  $n \mid a - a$ . But  $a - a = 0$  and every integer divides 0. So  $a \equiv a \pmod{n}$ .

## Intro to Modern Algebra Part 1a: Course Notes

---

symmetric: Now suppose that  $a \equiv b \pmod{n}$ . We want show that this implies  $b \equiv a \pmod{n}$ . Since  $a \equiv b \pmod{n}$  then  $n \mid a - b$  so  $a - b = nk$  for some  $k \in \mathbb{Z}$ . Then,

$$b - a = -(a - b) = -(nk) = n(-k).$$

So  $n \mid b - a$ , thus  $b \equiv a \pmod{n}$ .

transitive: Now suppose that  $a \equiv b \pmod{n}$  and  $b \equiv c \pmod{n}$ . We want to show that  $n \mid a - c$ . Then  $a \equiv b \pmod{n}$  implies  $a - b = nk$  for some  $k \in \mathbb{Z}$  and  $b \equiv c \pmod{n}$  implies  $b - c = nl$  for some  $l \in \mathbb{Z}$ . Then

$$a - c = a - b + b - c = nk + nl = n(k + l).$$

So  $n \mid a - c$ , thus  $a \equiv c \pmod{n}$ . □

### Congruence Classes

Now we will discuss important properties of congruence classes.

**Theorem 2.1.2** If  $a \equiv b \pmod{n}$  and  $c \equiv d \pmod{n}$ , then

1.  $a + c \equiv b + d \pmod{n}$
2.  $ac \equiv bd \pmod{n}$

*Proof of Theorem 2.1.2:* First we show that condition 1 holds. This means we need to show that  $n \mid (a + c) - (b + d)$ , that is, there exists some integer  $m$  so that  $(a + c) - (b + d) = nm$ . Since  $a \equiv b \pmod{n}$  we have that  $n \mid (a - b)$  so  $a - b = nk$  for some  $k \in \mathbb{Z}$ . Similarly, since  $c \equiv d \pmod{n}$  we have  $n \mid (c - d)$  so  $c - d = nl$  for some  $l \in \mathbb{Z}$ . Now we have:

$$\begin{aligned}(a + c) - (b + d) &= a + c - b - d \\ &= (a - b) + (c - d) \\ &= nk + nl \\ &= n(k + l)\end{aligned}$$

If we let  $k+l = m$  then we see that  $n \mid (a+c)-(b+d)$  so  $a+c \equiv b+d \pmod n$  as desired.

Next we want to show that condition 2 holds. Thus, we must show that  $n \mid (ac - bd)$ . Note that

$$\begin{aligned}ac - bd &= ac + 0 - bd \\ &= ac - bc + bc - bd \\ &= c(a - b) + b(c - d) \\ &= c(nk) + b(nt) \\ &= cnk + bnt \\ &= n(ck + bt)\end{aligned}$$

It follows that  $n \mid (ac - bd)$  so  $ac \equiv bd \pmod n$ . □

**Exercise 2.1.2** Answer the following:

- (a) If  $k \equiv 1 \pmod 4$ , then what is  $6k + 5$  congruent to modulo 4?
  
- (b) If  $r \equiv 3 \pmod{10}$  and  $s \equiv -7 \pmod{10}$ , then what is  $2r + 3s$  congruent to modulo 10?

▶ Let  $a$  and  $n$  be integers with  $n > 0$ . The **congruence class of  $a$  modulo  $n$**  (denoted  $[a]$ ) is the set of all those integers that are congruent to  $a$  modulo  $n$ , that is,

$$[a] = \{b \mid b \in \mathbb{Z} \text{ and } b \equiv a \pmod{n}\}.$$

This is sometimes denoted  $[a]_n$ .

▶ **Example** In congruence modulo 5,  $[9] = \{9 + 5k \mid k \in \mathbb{Z}\}$

▶ **Example** In congruence modulo 11,  $[9] = \{9 + 11k \mid k \in \mathbb{Z}\}$


Note that above we could have used the notation of  $[9]_5$  and  $[9]_{11}$ .

▶ **Theorem 2.1.3**  $a \equiv c \pmod{n}$  if and only if  $[a] = [c]$ .

*Proof of Theorem 2.1.3:* First we will prove that if  $a \equiv c \pmod{n}$  then  $[a] = [c]$ . To show  $[a] = [c]$  we will show that  $[a]$  is a subset of  $[c]$ ,  $[a] \subseteq [c]$ , and then that  $[c]$  is a subset of  $[a]$ ,  $[c] \subseteq [a]$ . Let  $b \in [a]$ . Then  $b \equiv a \pmod{n}$  and since  $a \equiv c \pmod{n}$  by transitivity  $b \equiv c \pmod{n}$ . Then  $b \in [c]$  and  $[a] \subseteq [c]$ .


Now let  $b \in [c]$ . Then  $b \equiv c \pmod{n}$  and we have  $a \equiv c \pmod{n}$  implies  $c \equiv a \pmod{n}$  implies  $b \equiv a \pmod{n}$  by symmetry and transitivity respectively. So  $b \in [a]$  and it follows that  $[c] \subseteq [a]$ . We can conclude that  $[a] = [c]$ .

Now suppose that  $[a] = [c]$ . Since  $a \equiv a \pmod{n}$  by reflexivity, we have  $a \in [a]$ , and thus  $a \in [c]$ . By definition, this implies that  $a \equiv c \pmod{n}$ .  $\square$

 **Corollary 2.1.4** Two congruence classes modulo  $n$  are either disjoint or identical.

*Proof of Corollary 2.1.4* Suppose  $[a]$  and  $[c]$  are disjoint. This means that  $[a] \neq [c]$ . Suppose the two congruence classes share an element, that is  $[a] \cap [c]$  is nonempty. This means there is an integer  $b$  so that  $b \in [a]$  and  $b \in [c]$ , so  $b \equiv a \pmod{n}$  and  $b \equiv c \pmod{n}$ . Since congruence is an equivalence relation, from Theorem 2.1.1 we have that  $a \equiv c \pmod{n}$ . Thus  $[a] = [c]$ .  $\square$

**Exercise 2.1.12** If  $p \geq 5$  and  $p$  is prime, prove that  $[p] = [1]$  or  $[p] = [5]$  in  $\mathbb{Z}/6\mathbb{Z}$

 **Example 2.1.6** If  $a \equiv b \pmod{n}$  and  $k \mid n$ , is it true that  $a \equiv b \pmod{k}$ ? Justify your answer.

**Exercise 2.1.8** Prove that every odd integer is congruent to 1 modulo 4 or 3 modulo 4.

**Exercise 2.1.9** Prove that

(a)  $(n - a)^2 \equiv a^2 \pmod{n}$

(b)  $(2n - a)^2 \equiv a^2 \pmod{4n}$

The set of all congruence classes modulo  $n$  is denoted  $\mathbb{Z}/n\mathbb{Z}$  which is read “ $\mathbb{Z} \bmod n$ .” This is often denoted  $\mathbb{Z}_n$  as well. The book uses this notation.

Note that the elements in  $\mathbb{Z}/n\mathbb{Z}$  are congruence classes, NOT single integers. For example,  $[5] \in \mathbb{Z}/n\mathbb{Z}$  but  $5 \notin \mathbb{Z}/n\mathbb{Z}$ . Also note that,

**The set  $\mathbb{Z}/n\mathbb{Z}$  has exactly  $n$  elements.**

**Example** The set  $\mathbb{Z}/3\mathbb{Z}$  has three elements,  $[0]$ ,  $[1]$ , and  $[2]$ .

**Exercise** Two students were having a debate about the set  $\mathbb{Z}/6\mathbb{Z}$ . Both agreed that  $\mathbb{Z}/6\mathbb{Z}$  had six elements. The first student said that the elements were  $\{[1], [2], [3], [4], [5], [6]\}$  while the second said that the elements were  $\{[0], [1], [2], [3], [4], [5]\}$ . Which student is correct?

**Exercise 2.1.16:** If  $[a] = [1]$  in  $\mathbb{Z}/n\mathbb{Z}$ , prove that  $(a, n) = 1$ . Show by example that the converse may be false.



## §2.2 MODULAR ARITHMETIC

### Modular Arithmetic

In the last section we introduced congruence and discussed some of its properties. Now we focus on how to perform operations like addition and multiplication with congruence classes. We start with the following definition.

▶ **Addition** and **multiplication** in  $\mathbb{Z}/n\mathbb{Z}$  are defined by

$$[a] \oplus [b] = [a + b] \quad \text{and} \quad [a] \odot [c] = [ac].$$

▶ **Example** Compute  $[3] \odot [7]$  in  $\mathbb{Z}/8\mathbb{Z}$

*Answer:* From the above definition we have  $[3] \odot [7] = [3 \cdot 7] = [21] = [5]$ .

▶ **Example** Compute  $[123] \oplus [157]$  in  $\mathbb{Z}/122\mathbb{Z}$ .

*Answer:* Note that  $[123] = [1]$  in  $\mathbb{Z}/122\mathbb{Z}$  and  $[157] = [35]$  in  $\mathbb{Z}/122\mathbb{Z}$ . So  $[123] + [157] = [1] + [35] = [36]$ .

▶ **Example** Determine the addition and multiplication tables for  $\mathbb{Z}/3\mathbb{Z}$

*Answer:* The addition and multiplication tables for  $\mathbb{Z}/3\mathbb{Z}$  are given below:

$\oplus$	[0]	[1]	[2]
[0]	[0]	[1]	[2]
[1]	[1]	[2]	[0]
[2]	[2]	[0]	[1]

$\odot$	[0]	[1]	[2]
[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]
[2]	[0]	[2]	[1]

**Exercise 2.2.1** Write out the addition and multiplication tables for the following:

- (a)  $\mathbb{Z}/2\mathbb{Z}$
- (b)  $\mathbb{Z}/4\mathbb{Z}$
- (c)  $\mathbb{Z}/7\mathbb{Z}$
- (d)  $\mathbb{Z}/12\mathbb{Z}$

The same **exponent notation** used in ordinary arithmetic is used in  $\mathbb{Z}/n\mathbb{Z}$ . If  $[a] \in \mathbb{Z}/n\mathbb{Z}$ , and  $k$  is a positive integer, then  $[a]^k$  denotes the product

$$\underbrace{[a] \odot [a] \odot \cdots \odot [a]}_{k \text{ factors}}$$

**Example** Find  $[3]^2$  and  $[3]^4$  in  $\mathbb{Z}/5\mathbb{Z}$

*Answer:*

$$[3]^2 = [3] \odot [3] = [9] = [4] \quad \text{and} \quad [3]^4 = [3] \odot [3] \odot [3] \odot [3] = [81] = [1]$$

## Properties of Modular Arithmetic

▶ **Theorem 2.2.7** For any congruence classes  $[a], [b]$ , and  $[c] \in \mathbb{Z}/n\mathbb{Z}$ , we have the following properties.

1. If  $[a] \in \mathbb{Z}/n\mathbb{Z}$  and  $[b] \in \mathbb{Z}/n\mathbb{Z}$ , then  $[a] \oplus [b] \in \mathbb{Z}/n\mathbb{Z}$ .
2.  $[a] \oplus ([b] \oplus [c]) = ([a] \oplus [b]) \oplus [c]$ .
3.  $[a] \oplus [b] = [b] \oplus [a]$ .
4.  $[a] \oplus [0] = [a] = [0] \oplus [a]$ .
5. For each  $[a] \in \mathbb{Z}/n\mathbb{Z}$ , the equation  $[a] \oplus X = [0]$  has a solution in  $\mathbb{Z}/n\mathbb{Z}$ .
6. If  $[a] \in \mathbb{Z}/n\mathbb{Z}$  and  $[b] \in \mathbb{Z}/n\mathbb{Z}$ , then  $[a] \odot [b] \in \mathbb{Z}/n\mathbb{Z}$ .
7.  $[a] \odot ([b] \odot [c]) = ([a] \odot [b]) \odot [c]$ .
8.  $[a] \odot ([b] \oplus [c]) = [a] \odot [b] \oplus [a] \odot [c]$  and  $([a] \oplus [b]) \odot [c] = [a] \odot [c] \oplus [b] \odot [c]$ .
9.  $[a] \odot [b] = [b] \odot [a]$ .
10.  $[a] \odot [1] = [a] = [1] \odot [a]$ .

**Exercise 2.2.10** Prove parts 3,7,8, and 9 of Theorem 2.2.7.

Note that when the context is clear, we will use  $+$  and  $\cdot$  to mean  $\oplus$  and  $\odot$  respectively. Similarly, we will sometimes use  $1$  to mean  $[1]$  when there is little room for confusion.

## Solving Equations with Congruence Classes

Since  $\mathbb{Z}/n\mathbb{Z}$  has exactly  $n$  elements, when we can solve equations in with congruence classes we can substitute each of these  $n$  elements to see which ones are solutions. Consider the following example:

▶ **Example:** Find all solutions of  $x^3 + 2x + 3 = 0$  in  $\mathbb{Z}/5\mathbb{Z}$

*Answer:*

$$\underline{x = 0}$$

$$(0)^3 + 2(0) + 3 = 0 + 0 + 3 = 3$$

$$\underline{x = 1}$$

$$(1)^3 + 2(1) + 3 = 1 + 2 + 3 = 6 = 1$$

$$\underline{x = 2}$$

$$(2)^3 + 2(2) + 3 = 8 + 4 + 3 = 15 = 0$$

$$\underline{x = 3}$$

$$(3)^3 + 2(3) + 3 = 27 + 6 + 3 = 36 = 1$$

$$\underline{x = 4}$$

$$(4)^3 + 2(4) + 3 = 64 + 8 + 3 = 75 = 0$$

So [2] and [4] are solutions to  $x^3 + 2x + 3$  in  $\mathbb{Z}/5\mathbb{Z}$ .

**Exercise 2.2.3:** Solve the equation  $x^2 = [1]$  in  $\mathbb{Z}/8\mathbb{Z}$ .


**Exercise 2.2.4:** Solve the equation  $x^4 = [1]$  in  $\mathbb{Z}/5\mathbb{Z}$ .

**Exercise 2.2.7:** Solve the equation  $x^3 \oplus x^2 \oplus x \oplus [1] = [0]$  in  $\mathbb{Z}/8\mathbb{Z}$ .

**Exercise 2.2.8:** Solve the equation  $x^3 + x^2 = [2]$  in  $\mathbb{Z}/10\mathbb{Z}$ .

§2.3 THE STRUCTURE OF  $\mathbb{Z}/p\mathbb{Z}$  ( $p$  PRIME) AND  $\mathbb{Z}/n\mathbb{Z}$ Structure of  $\mathbb{Z}/p\mathbb{Z}$  when  $p$  is Prime

It has been established that  $\mathbb{Z}$  has nice properties that are shared with many of the sets  $\mathbb{Z}/n\mathbb{Z}$ . However, not all nice properties are shared. For example, in the integers, the if we take the product of two nonzero integers, the result is always nonzero. In  $\mathbb{Z}/6\mathbb{Z}$  however,  $2 \cdot 3 = 0$  even though 2 and 3 are both nonzero. Yet in  $\mathbb{Z}/7\mathbb{Z}$  the product of two nonzero integers is always nonzero. In this section, we will explore the properties of  $\mathbb{Z}/p\mathbb{Z}$  where  $p$  is prime. We begin with the following theorem.

 **Theorem 2.3.8** If  $p > 1$  is an integer, then the following conditions are equivalent.

1.  $p$  is prime
2. For any  $a \neq 0$  in  $\mathbb{Z}/p\mathbb{Z}$ , the equation  $ax = 1$  has a solution in  $\mathbb{Z}/p\mathbb{Z}$
3. Whenever  $bc = 0$  in  $\mathbb{Z}/n\mathbb{Z}$ , then  $b = 0$  or  $c = 0$ .

*Proof of Theorem 2.3.8* First we show that if  $p$  is prime, the equation  $ax = 1$  has a solution in  $\mathbb{Z}/p\mathbb{Z}$  for any nonzero  $a$ . Since  $a$  is nonzero, we can say that  $a \not\equiv 0 \pmod{p}$ . Thus  $p$  does not divide  $a$ . Consider  $(a, p)$ . Since  $p$  does not divide  $a$  the greatest common divisor of  $p$  and  $a$  must be 1. By Bezout's Identity, we can write 1 as a linear combination of  $a$  and  $p$ . So we have  $1 = au + pv$  for some integers  $u$  and  $v$ . Then  $au - 1 = -pv = p(-v)$ , thus  $au \equiv 1 \pmod{p}$ . This implies that  $[au] = [1]$  in  $\mathbb{Z}/p\mathbb{Z}$ . So  $[a][u] = [au] = 1$ , thus  $x = [u]$  is a solution of  $[a]x = [1]$ .

Now suppose that  $bc = 0$  in  $\mathbb{Z}/p\mathbb{Z}$ . if  $b$  is zero there is nothing to prove. If  $b \neq 0$ , then by assumption, the equation  $bx = 1$  has a solution for some  $x \in \mathbb{Z}/p\mathbb{Z}$ . Then we have

$$0 = x \cdot 0 = x(bc) = (xb)c = (bx)c = 1 \cdot c = c.$$

So either  $b = 0$  or  $c = 0$  as desired.

Suppose that  $b, c$  are any integers such that  $p \mid bc$ . Then  $bc \equiv 0 \pmod{p}$ , so we have that

$$[b][c] = [bc] = [0] \text{ in } \mathbb{Z}/p\mathbb{Z}.$$

Thus by assumption  $[b] = [0]$  or  $[c] = [0]$ . This implies that  $b \equiv 0 \pmod{p}$  or  $c \equiv 0 \pmod{p}$ , so  $p \mid b$  or  $p \mid c$ . It follows that  $p$  is prime.  $\square$

**Exercise** Verify Theorem 2.3.2 for  $p = 5$ . Try again for  $p = 4$ . What do you observe?

Note that when  $n$  is not prime,  $ax = 1$  does not need to have a solution in  $\mathbb{Z}/n\mathbb{Z}$ . For example,  $2x = 1$  does not have a solution in  $\mathbb{Z}/4\mathbb{Z}$ .


**Theorem 2.3.9** Let  $a$  and  $n$  be integers with  $n > 1$ . Then the equation

$$[a]x = [1] \text{ has a solution in } \mathbb{Z}/n\mathbb{Z} \text{ if and only if } (a, n) = 1 \text{ in } \mathbb{Z}.$$

**Multiplicative Cancellation Law** Let  $p$  be a prime and  $a, b, c \in \mathbb{Z}/p\mathbb{Z}$  with  $a \neq [0]_p$ . Then  $ab = ac$  if and only if  $b = c$ .

**Exercise** Verify that the cancellation law holds in  $\mathbb{Z}/5\mathbb{Z}$  but does not hold in  $\mathbb{Z}/4\mathbb{Z}$ .

### Units

 An element  $a$  in  $\mathbb{Z}/n\mathbb{Z}$  is called a **unit** if the equation  $ax = 1$  has a solution. Equivalently,  $a$  is a unit if there is an element  $b$  in  $\mathbb{Z}/n\mathbb{Z}$  such that  $ab = 1$ . Here  $b$  is the **inverse** of  $a$ .

▶ **Theorem 2.3.10** Let  $a$  and  $n$  be integers with  $n > 1$ . Then

$[a]$  is a unit in  $\mathbb{Z}/n\mathbb{Z}$  if and only if  $(a, n) = 1$  in  $\mathbb{Z}$ .

▶ **Example 2.3.1 a** Find all of the units in  $\mathbb{Z}/7\mathbb{Z}$

*Answer:* Theorem 2.3.10 says that  $[a]$  is a unit in  $\mathbb{Z}/7\mathbb{Z}$  if  $(a, 7) = 1$ . So we look for all of the numbers  $a \in \{0, 1, 2, 3, 4, 5, 6\}$  that are relatively prime to 7. Each nonzero number in this set is relatively prime to 7, so  $[1], [2], [3], [4], [5], [6]$  are all units in  $\mathbb{Z}/7\mathbb{Z}$ .

**Exercise 2.3.1 b,c,d** Find all of the units in the following sets.


(a)  $\mathbb{Z}/8\mathbb{Z}$

(b)  $\mathbb{Z}/9\mathbb{Z}$

(c)  $\mathbb{Z}/10\mathbb{Z}$

### Zero Divisors

▶ A nonzero element  $a$  of  $\mathbb{Z}/n\mathbb{Z}$  is called a **zero divisor** if the equation  $ax = 0$  has a *nonzero* solution (that is, if there is a nonzero element  $c$  in  $\mathbb{Z}/n\mathbb{Z}$  such that  $ac = 0$ .)

 **Example 2.3.2 b** Find all of the zero divisors in  $\mathbb{Z}/8\mathbb{Z}$

*Answer:* Consider the following multiplication table for  $\mathbb{Z}/8\mathbb{Z}$ :

·	0	1	2	3	4	5	6	7
0	0	<b>0</b>	<b>0</b>	<b>0</b>	<b>0</b>	<b>0</b>	<b>0</b>	<b>0</b>
1	<b>0</b>	1	2	3	4	5	6	7
2	<b>0</b>	2	4	6	<b>0</b>	2	4	6
3	<b>0</b>	3	6	1	4	7	2	5
4	<b>0</b>	4	<b>0</b>	4	<b>0</b>	4	<b>0</b>	4
5	<b>0</b>	5	2	7	4	1	6	3
6	<b>0</b>	6	4	2	<b>0</b>	6	4	2
7	<b>0</b>	7	6	5	4	3	2	1

We see that the zero divisors of  $\mathbb{Z}/8\mathbb{Z}$  are 0, 2, 4, 6.

**Exercise 2.3.2 a,c,d** Find all the zero divisors in the following sets:

(a)  $\mathbb{Z}/7\mathbb{Z}$

(c)  $\mathbb{Z}/9\mathbb{Z}$

(d)  $\mathbb{Z}/10\mathbb{Z}$

**Exercise 2.3.3** Based on Exercise 2.3.1 and 2.3.2, make a conjecture about units and zero divisors in  $\mathbb{Z}/n\mathbb{Z}$ .

**Exercise 2.3.9 a,b** Answer the following.

(a) If  $a$  is a unit in  $\mathbb{Z}/n\mathbb{Z}$ , prove that  $a$  is not a zero divisor.

(b) If  $a$  is a zero divisor in  $\mathbb{Z}/n\mathbb{Z}$ , prove that  $a$  is not a unit. [*Hint:* Think contrapositive in part (a).]



### §3.1 RINGS

▶ A **ring** is a nonempty set  $R$  equipped with two operations (usually written as addition and multiplication) that satisfy the following axioms. For all  $a, b, c \in R$ :

1. [*closure for addition*] If  $a \in R$  and  $b \in R$ , then  $a + b \in R$
2. [*associative addition*]  $a + (b + c) = (a + b) + c$ .
3. [*commutative addition*]  $a + b = b + a$ .
4. [*additive identity*] There is an element  $0_R$  in  $R$  such that

$$a + 0_R = a = 0_R + a \text{ for every } a \in R.$$

5. For each  $a \in R$ , the equation  $a + x = 0_R$  has a solution in  $R$ .
6. [*closure for multiplication*] If  $a \in R$  and  $b \in R$ , then  $ab \in R$ .
7. [*associative multiplication*]  $a(bc) = (ab)c$ .
8. [*distributive laws*]  $a(b + c) = ab + ac$  and  $(a + b)c = ac + bc$

▶ A **commutative ring** is a ring  $R$  that satisfies the following:

$$ab = ba \text{ for all } a, b \in R.$$

▶ A **ring with identity** is a ring  $R$  that contains an element  $1_R$  satisfying the following:

$$a1_R = a = 1_Ra \text{ for all } a \in R.$$

▶ **Example** The integers  $\mathbb{Z}$  with the usual addition and multiplication are a commutative ring with identity.

▶ **Example** The set of even integers  $2\mathbb{Z} = \{2k \mid k \in \mathbb{Z}\}$  is a commutative ring without identity.

**Example** The set of all functions from  $\mathbb{R}$  to  $\mathbb{R}$  is a commutative ring with identity.

**Example** The set of all  $n \times n$  matrices with entries in  $\mathbb{R}$  is a noncommutative ring with identity.

**Exercise 3.1.1** The following subsets of  $\mathbb{Z}$  (with ordinary addition and multiplication) satisfy all but one of the axioms for a ring. In each case, which axiom fails?

- (a) The set  $S$  of all odd integers and 0.
- (b) The set of nonnegative integers.

**Example** Let  $R = \{0, 1\}$  and  $a, b \in R$ . Define addition and multiplication on  $R$  by:

$\begin{array}{c cc} + & 0 & 1 \\ \hline 0 & 0 & 1 \\ 1 & 1 & a \end{array}$	$\begin{array}{c cc} + & 0 & 1 \\ \hline 0 & 0 & 0 \\ 1 & 0 & b \end{array}$
--	--

For which values of  $a$  and  $b$  is  $(R, +, \cdot)$  a ring?

*Answer:* Since 1 needs to have an additive inverse,  $R$  will not be a ring if  $a = 1$ . Suppose now that  $a = 0$ . If  $b = 1$ , then  $(R, +, \cdot)$  is  $\mathbb{Z}/2\mathbb{Z}, (\oplus, \odot)$  with the regular addition and multiplication so  $R$  is a ring. If  $b = 0$ , then  $xy = 0$  for all  $x, y \in R$ , and axioms 4-8 hold. Axioms 1-4 hold because the addition is the same as in  $\mathbb{Z}/2\mathbb{Z}$ . So  $R$  is a ring.

In both cases  $R$  is commutative. If  $b = 1$ , then 1 is an identity. If  $b = 0$ ,

$R$  does not have an identity.

**Example** Let  $R = \{0, 1\}$ . Define an addition and multiplication on  $R$  by:

$$\begin{array}{c|cc} \boxplus & 0 & 1 \\ \hline 0 & 1 & 0 \\ 1 & 0 & 1 \end{array}$$

$$\begin{array}{c|cc} \boxdot & 0 & 1 \\ \hline 0 & 0 & 1 \\ 1 & 1 & 1 \end{array}$$

Is  $(R, \boxplus, \boxdot)$  a ring?

*Answer:* Note that 1 is an additive identity, so  $0_R = 1$ . Also 0 is a multiplicative identity, so  $1_R = 0$ . Using the symbols  $0_R$  and  $1_R$  we can write the addition and multiplication table as follows:

$$\begin{array}{c|cc} \boxplus & 0_R & 1_R \\ \hline 0_R & 0_R & 1_R \\ 1_R & 1_R & 0_R \end{array}$$

$$\begin{array}{c|cc} \boxdot & 0_R & 1_R \\ \hline 0_R & 0_R & 0_R \\ 1_R & 0_R & 1_R \end{array}$$

So most entries in the table are determined by the fact that  $0_R$  and  $1_R$  are the additive and multiplicative identity, respectively. Also

$$1_R \boxplus 1_R = 0 \boxplus 0 = 1 = 0_R \text{ and } 0_R \boxdot 0_R = 1 \boxdot 1 = 1 = 0_R.$$

Observe that the new tables are the same as for  $\mathbb{Z}/2\mathbb{Z}$ . So  $(R, \boxplus, \boxdot)$  is a ring.

**Exercise 3.1.18** Define a new multiplication in  $\mathbb{Z}$  by the rule  $ab = 1$  for all  $a, b \in \mathbb{Z}$ . With ordinary addition and this new multiplication, is  $\mathbb{Z}$  a ring?

### Integral Domains

An **integral domain** is a commutative ring  $R$  with identity  $1_R \neq 0_R$  that satisfies the following:

Whenever  $a, b \in R$  and  $ab = 0_R$ , then  $a = 0_R$  or  $b = 0_R$ .

**Example** The integers  $\mathbb{Z}$  are an integral domain.

**Example**  $\mathbb{Z}/p\mathbb{Z}$  is an integral domain if  $p$  is prime

**Example**  $\mathbb{Z}/6\mathbb{Z}$  is not an integral domain because  $3 \cdot 2 = 0$  where 3 and 2 are both nonzero.

**Example 3.1.22** Define a new addition  $\oplus$  and multiplication  $\odot$  on  $\mathbb{Z}$  by

$$a \oplus b = a + b - 1 \quad \text{and} \quad a \odot b = a + b - ab,$$

where the operations on the right-hand side of the equal signs are ordinary addition, subtraction, and multiplication. Prove that, with the new operations  $\oplus$  and  $\odot$ ,  $\mathbb{Z}$  is an integral domain.

*Proof:* We must show that with these new operations  $\mathbb{Z}$  satisfies the 8 criteria for being a ring. Then we show that it is an integral domain. Let  $a, b, c \in \mathbb{Z}$ .

1. Since  $a, b \in \mathbb{Z}$ , we have  $a \oplus b = a + b - 1 \in \mathbb{Z}$  so there is closure under the addition.

2. Note that,

$$\begin{aligned}a \oplus (b \oplus c) &= a \oplus (b + c - 1) \\&= a + (b + c - 1) - 1 \\&= (a + b - 1) + c - 1 \\&= (a + b - 1) \oplus c \\&= (a \oplus b) \oplus c\end{aligned}$$

so the addition is associative.

3. We have that

$$a \oplus b = a + b - 1 = b + a - 1 = b \oplus a$$

so commutativity of addition holds.

4. If we set  $0_R = 1$  we have that

$$a \oplus 0_R = a \oplus 1 - 1 = a$$

so 1 is the additive identity.

5. Consider the equation

$$1 = 0_R = a \oplus x = a + x - 1.$$

If we solve this equation for  $x$  we have  $x = 2 - a \in \mathbb{Z}$ , so this property holds.

6. Note that  $a \odot b = a + b - ab \in \mathbb{Z}$  since  $a, b \in \mathbb{Z}$  so there is closure for the multiplication.

7. We have

$$\begin{aligned}a \odot (b \odot c) &= a \odot (b + c - bc) \\&= a + (b + c - bc) - a(b + c - bc) \\&= a + b + c - ab - bc - ac + abc\end{aligned}$$

and

$$\begin{aligned}
 (a \odot b) \odot c &= (a + b - ab) \odot c \\
 &= (a + b - ab) + c - (a + b - ab)c \\
 &= a + b + c - ab - ac - bc + abc.
 \end{aligned}$$

So we see that  $a \odot (b \odot c) = (a \odot b) \odot c$  and thus we have associativity of the multiplication.

8. For the distributive property, note that

$$\begin{aligned}
 a \odot (b \oplus c) &= a \odot (b + c - 1) \\
 &= a + b + c - 1 - a(b + c - 1) \\
 &= 2a + b + c - ab - ac - 1 \\
 &= (a + b - ab) + (a + c - ac) - 1 \\
 &= (a \odot b) + (a \odot c) - 1 \\
 &= (a \odot b) \oplus (a \odot c)
 \end{aligned}$$

and

$$\begin{aligned}
 (a \oplus b) \odot c &= (a + b - 1) \odot c \\
 &= a + b - 1 + c - (a + b - 1)c \\
 &= a + b + 2c - ac - bc - 1 \\
 &= (a + c - ac) + (b + c - bc) - 1 \\
 &= (a \odot c) + (b \odot c) - 1 \\
 &= (a \odot c) \oplus (b \odot c)
 \end{aligned}$$

so the distributive properties hold.

It follows that  $(\mathbb{Z}, \oplus, \odot)$  is a ring. Now we want to show that it is an integral domain. Since

$$a \odot b = a + b - ab = b + a - ba = b \odot a$$

it is a commutative ring. Let  $I_R = 0$ . Then

$$a \odot I_R = a \odot 0 = a + 0 - a \cdot 0 = a$$

and

$$I_R \odot a = 0 \odot a = 0 + a - 0 \cdot a = a$$

so  $I_R = 0$  is the multiplicative identity. Thus  $(\mathbb{Z}, \oplus, \odot)$  is a commutative ring with identity.


To show it is an integral domain, assume  $a \odot b = 0_R$ . Then  $a + b - ab = 1$ . But  $a + b - ab = 1$  implies  $0 = ab - a - b + 1 = (a - 1)(b - 1)$ . So  $(a - 1) = 0$  or  $(b - 1) = 0$ . So  $a = 1 = 0_R$  or  $b = 1 = 0_R$ . It follows that the ring is an integral domain.  $\square$

**Exercise 3.1.24** Define a new addition and multiplication on  $\mathbb{Z}$  by

$$a \oplus b = a + b - 1 \quad \text{and} \quad a \odot b = ab - (a + b) + 2.$$

Prove that with these new operations  $\mathbb{Z}$  is an integral domain.


### Fields

 A **field** is a commutative ring  $R$  with identity  $1_R \neq 0_R$  that satisfies the following:

For each  $a \neq 0_R$  in  $R$ , the equation  $ax = 1_R$  has a solution in  $R$ .

 **Example** The rational numbers  $\mathbb{Q}$  are a field.

 **Example** The complex numbers  $\mathbb{C}$  are a field.

 **Example** The real numbers  $\mathbb{R}$  are a field.

## Intro to Modern Algebra Part 1a: Course Notes

---

**Exercise 3.1.2** Let  $R = \{0, e, b, c\}$  with addition and multiplication defined by the tables below. Assume associativity and distributivity and show that  $R$  is a ring with identity. Is  $R$  commutative? Is  $R$  a field?

+	0	e	b	c
0	0	e	b	c
e	e	0	c	b
b	b	c	0	e
c	c	b	e	0

·	0	e	b	c
0	0	0	0	0
e	0	e	b	c
b	0	b	b	0
c	0	c	0	c

**Exercise 3.1.3** Let  $F = \{0, e, a, b\}$  with operations given by the following tables. Assume associativity and distributivity and show that  $F$  is a field.

+	0	e	a	b
0	0	e	a	b
e	e	0	b	a
a	a	b	0	e
b	b	a	e	0

·	0	e	a	b
0	0	0	0	0
e	0	e	a	b
a	0	a	b	e
b	0	b	e	a

**Exercise 3.1.4** Find matrices  $A$  and  $C$  in  $M(\mathbb{R})$  such that  $AC = \mathbf{0}$ , but  $CA \neq \mathbf{0}$ , where  $\mathbf{0}$  is the zero matrix. [*Hint*: Example 6.]

**Exercise 3.1.29** The addition table and part of the multiplication table for a three-element ring are given below. Use the distributive laws to complete the multiplication table.

+	r	s	t
r	r	s	t
s	s	t	r
t	t	r	s

·	r	s	t
r	r	r	r
s	r	t	
t	r		



## Direct Products of Rings

▶ **Theorem 3.1.1** Let  $R$  and  $S$  be rings. Define addition and multiplication on the Cartesian product  $R \times S$  by

$$(r, s) + (r', s') = (r + r', s + s') \quad \text{and} \quad (r, s)(r', s') = (rr', ss').$$

Then:

1.  $R \times S$  is a ring;
2.  $0_{R \times S} = (0_R, 0_S)$ ;
3.  $-(r, s) = (-r, -s)$  for all  $r \in R, s \in S$ ;
4. if  $R$  and  $S$  are both commutative, then so is  $R \times S$ ;
5. if both  $R$  and  $S$  have an identity, then  $R \times S$  has an identity and  $1_{R \times S} = (1_R, 1_S)$ .

▶ **Example 3.1.15 b** Write out the addition and multiplication tables for  $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ .

$+$	$(0,0)$	$(1,1)$	$(1,0)$	$(0,1)$	$\cdot$	$(0,0)$	$(1,1)$	$(1,0)$	$(0,1)$
$(0,0)$	$(0,0)$	$(1,1)$	$(1,0)$	$(0,1)$	$(0,0)$	$(0,0)$	$(0,0)$	$(0,0)$	$(0,0)$
$(1,1)$	$(1,1)$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$	$(0,0)$	$(1,1)$	$(1,0)$	$(0,1)$
$(1,0)$	$(1,0)$	$(0,1)$	$(0,0)$	$(1,1)$	$(1,0)$	$(0,0)$	$(1,0)$	$(1,0)$	$(0,0)$
$(0,1)$	$(0,1)$	$(1,0)$	$(1,1)$	$(0,0)$	$(0,1)$	$(0,0)$	$(0,1)$	$(0,0)$	$(0,1)$


**Exercise 3.1.9 a** Let  $R$  be a ring and consider the subset  $R^*$  of  $R \times R$  defined by  $R^* = \{(r, r) \mid r \in R\}$ . If  $R = \mathbb{Z}/6\mathbb{Z}$ , list the elements of  $R^*$ .

**Exercise 3.1.15 a,c** Write out the addition and multiplication tables for:

(a)  $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$

(c)  $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$

## Subrings

 **Theorem 3.2** Suppose that  $R$  is a ring and that  $S$  is a subset of  $R$  such that

1.  $S$  is closed under addition (if  $a, b \in S$ , then  $a + b \in S$ );
2.  $S$  is closed under multiplication (if  $a, b \in S$ , then  $ab \in S$ );
3.  $0_R \in S$ ;
4. If  $a \in S$ , then the solution of the equation  $a + x = 0_R$  is in  $S$ .

Then  $S$  is a **subring** of  $R$ .

**Example** The subset  $S = \{0, 3\}$  of  $\mathbb{Z}/6\mathbb{Z}$  is closed under addition and multiplication ( $0+0 = 0$ ;  $0+3 = 3$ ;  $3+3 = 0$ ; similarly  $0 \cdot 0 = 0 = 0 \cdot 3$ ;  $3 \cdot 3 = 3$ ). By definition of  $S$  we have  $0 \in S$ . Finally the equation  $0 + x = 0$  has solution  $x = 0 \in S$ , and the equation  $3 + x = 0$  has solution  $x = 3 \in S$ . Therefore,  $S$  is a subring of  $\mathbb{Z}/6\mathbb{Z}$  by Theorem 3.1.2.

**Example**  $\mathbb{Z}$  is a subring of  $\mathbb{Q}$

**Example 3.1.5 a** Is the following subset a subring of  $M(\mathbb{R})$ ? All matrices of the form  $\begin{pmatrix} 0 & r \\ 0 & 0 \end{pmatrix}$  with  $r \in \mathbb{Q}$ .

*Answer:* Yes this is a subring without identity since every product is the zero matrix.

### Subfields

If  $S$  is a subring of  $R$  and  $S$  is itself a field then we say  $S$  is **subfield** of  $R$ .

**Example**  $\mathbb{Q}$  is a subfield of  $\mathbb{R}$

**Example**  $\mathbb{R}$  is a subfield of  $\mathbb{Q}$

## §3.2 BASIC PROPERTIES OF RINGS

## Arithmetic in Rings

▶ **Theorem 3.2.3** For any element  $a$  in a ring  $R$ , the equation  $a+x = 0_R$  has a unique solution.

*Answer:* From the 5th ring axiom, we know that the equation  $a+x = 0_R$  has at least one solution, call it  $u$ . Now we show that solution is unique. Suppose  $v$  is another solution to  $a+x = 0_R$ . Then we have  $a+u = 0_R$  and  $a+v = 0_R$ . Thus,

$$v = 0_R + v = (a + u) + v = (u + a) + v = u + (a + v) = u + 0_R = u.$$

It follows that  $u$  is unique. □

In the equation from Theorem 3.2.3, the element  $x$  is the additive inverse of  $a$  in  $R$ . If we let  $x = -a$ , we say that  $-a$  is the unique element of  $R$  such that

$$a + (-a) = 0_R = (-a) + a.$$

▶ **Example** In  $\mathbb{Z}/6\mathbb{Z}$ , the solution of the equation  $2 + x = 0$  is 4, so in  $\mathbb{Z}/6\mathbb{Z}$   $-2 = 4$ .

▶ **Remark** In a ring  $b-a$  means  $b+(-a)$ .

▶ **Theorem 3.2.4** If  $a + b = a + c$  in a ring  $R$ , then  $b = c$ .

*Proof of Theorem 3.2.4:* If I add  $-a$  to both sides  $a + b = a + c$  and then

using associativity and negatives show that

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

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

$$0_R + b = 0_R + c$$

$$b = c. \quad \square$$

**Theorem 3.2.5** For any elements  $a$  and  $b$  of a ring  $R$ ,

1.  $a \cdot 0_R = 0_R = 0_R \cdot a$ . In particular,  $0_R \cdot 0_R = 0_R$ .
2.  $a(-b) = -ab$  and  $(-a)b = -ab$ .
3.  $-(a) = a$ .
4.  $-(a + b) = (-a) + (-b)$ .
5.  $-(a - b) = -a + b$ .
6.  $(-a)(-b) = ab$ . If  $R$  has an identity, then
7.  $(-1_R)a = -a$ .

*Proof:* We need to show that each of the above properties in Theorem 3.2.5 hold.

1. Since  $0_R + 0_R = 0_R$ , by the distributive law we have

$$a \cdot 0_R + a \cdot 0_R = a(0_R + 0_R) = a \cdot 0_R = a \cdot 0_R + 0_R.$$

Thus  $a \cdot 0_R = 0_R$ . Similarly, we have that  $0_R \cdot a = 0_R$ .

2. Note that  $-ab$  is the unique solution of the equation  $ab + x = 0_R$ , so if any other  $x$  satisfies this equation it must be equivalent to  $-ab$ . But  $x = a(-b)$  is a solution since

$$ab + a(-b) = a[b + (-b)] = a[0_R] = 0_R.$$

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

**3.** By definition,  $-(-a)$  is the unique solution of  $(-a) + x = 0_R$ . But  $a$  is a solution of this equation since  $(-a) + a = 0_R$ . Hence  $-(-a) = a$  by uniqueness.

**4.** Note that  $-(a + b)$  is the unique solution of  $(a + b) + x = 0_R$ , but  $(-a) + (-b)$  is also a solution. Then by commutativity of addition we have

$$\begin{aligned}(a + b) + [(?a) + (-b)] &= a + (-a) + b + (-b) \\ &= 0_R + 0_R \\ &= 0_R.\end{aligned}$$

Therefore,  $-(a + b) = (-a) + (-b)$  by uniqueness.

**5.** Note that

$$-(a - b) = -(a + (-b)) = (-a) + (-(-b)) = -a + b$$

by definition of subtraction.

**6.** By (2) and (3) we have

$$\begin{aligned}(-a)(-b) &= -(a(-b)) \\ &= -(-ab) \\ &= ab.\end{aligned}$$

**7.** By (2) we have

$$(-1_R)a = -(1_Ra) = -(a) = -a. \quad \square$$

**Exercise 3.2.1** Let  $R$  be a ring and  $a, b \in R$ .

(a)  $(a + b)(a - b) = ?$

(b)  $(a + b)^3 = ?$

(c) What are the answers in parts (a) and (b) if  $R$  is commutative?

**Exercise 3.2.3 b** An element  $e$  of a ring  $R$  is said to be **idempotent** if  $e^2 = e$ .

(a) Find all the idempotents in  $\mathbb{Z}/12\mathbb{Z}$

**Exercise 3.2.5** Answer the following:

(a) Show that a ring has only one zero element. [*Hint*: If there were more than one, how many solutions would the equation  $0_R + x = 0_R$  have?]

(b) Show that a ring  $R$  with identity has only one identity element.


(c) Can a unit in a ring  $R$  with identity have more than one inverse? Why?

**Exercise 3.2.31** A **Boolean ring** is a ring  $R$  with identity in which  $x^2 = x$  for every  $x \in R$ . For examples, see Exercises 19 and 44 in Section 3.1. If  $R$  is a Boolean ring, prove that:

(a)  $a + a = 0_R$  for every  $a \in R$ , which means that  $a = -a$ . [*Hint*: Expand  $(a + a)^2$ .]

(b)  $R$  is commutative. [*Hint*: Expand  $(a + b)^2$ .]

### Units and Zero Divisors

 An element  $a$  in a ring  $R$  with identity is called a **unit** if there exists  $u \in R$  such that  $au = 1_R = ua$ . In this case the element  $u$  is called the **multiplicative inverse** of  $a$  and is denoted  $a^{-1}$ .

**Exercise 3.2.2** Find the inverse of matrices  $A$ ,  $B$ , and  $C$  in Example 7 on page 64 of the text.

▶ An element  $a$  in a ring  $R$  is a **zero divisor** provided that

1.  $a \neq 0_R$ .
2. There exists a nonzero element  $c \in R$  such that  $ac = 0_R$  or  $ca = 0_R$ .

**Example** Every integral domain  $R$  satisfies Axiom 11: If  $ab = 0_R$ , then  $a = 0_R$  or  $b = 0_R$ . In other words, the product of two nonzero elements cannot be 0. Therefore,

**An integral domain contains no zero divisors.**

### Integral Domains and Fields

▶ **Theorem 3.2.7 Cancellation Properties** Cancellation is valid in any integral domain  $R$ : If  $a \neq 0_R$  and  $ab = ac$  in  $R$ , then  $b = c$ .


*Answer:* Suppose  $ab = ac$ . Then  $ab - bc = 0_R$ , so that  $a(b - c) = 0_R$ . Since  $a \neq 0_R$ , we must have  $b - c = 0_R$  (if not, then  $a$  is a zero divisor, contradicting Axiom 11.) Therefore,  $b = c$ .  $\square$

**Exercise 3.2.29** Let  $R$  be a commutative ring with identity. Prove that  $R$  is an integral domain if and only if cancellation holds in  $R$  (that is,  $a \neq 0_R$  and  $ab = ac$  in  $R$  imply  $b = c$ .)

**Exercise 3.2.21** Let  $R$  be a ring and let  $a$  be a nonzero element of  $R$  that is not a zero divisor. Prove that cancellation holds for  $a$ ; that is, prove that

- (a) If  $ab = ac$  in  $R$ , then  $b = c$ .
- (b) If  $ba = ca$  in  $R$ , then  $b = c$ .



 **Theorem 3.2.8** Every field  $F$  is an integral domain.

*Proof:* Let  $F$  be a field. Then  $F$  is a commutative ring with identity. Suppose  $ab = 0_F$ . If  $b = 0_F$  there is nothing to prove. If  $b \neq 0_F$ , then  $b$  is a unit (since every nonzero element of  $F$  is a unit.) Thus we have

$$a = a \cdot 1_F = abb^{-1} = 0_F b^{-1} = 0_F.$$

So in each case either  $a = 0_F$  or  $b = 0_F$ . It follows that  $F$  is an integral domain.  $\square$

**Example** Show that the converse of Theorem 3.2.8 is false. That is, give an example of an integral domain that is not a field.

 **Theorem 3.2.9** Every finite integral domain  $R$  is a field.

*Proof:* Let  $R$  be a finite integral domain where  $a_1, a_2, \dots, a_n$  are the distinct elements of  $R$ . Suppose  $a_t \neq 0_R$ . Consider the products  $a_t a_1, a_t a_2, a_t a_3, \dots, a_t a_n$ . If  $a_i \neq a_j$  then it follows that  $a_t a_i \neq a_t a_j$ . Thus,  $a_t a_1, a_t a_2, \dots, a_t a_n$  are  $n$  distinct elements of  $R$ . However,  $R$  has exactly  $n$  elements, so these represent the elements of  $R$ , perhaps in a different order. In particular, for some  $j$ ,  $a_t a_j = 1_R$ . Thus the equation  $a_t x = 1_R$  has a solution. Since  $a_t$  was arbitrary,  $R$  is a field.  $\square$

## §3.3 ISOMORPHISMS AND MAPPINGS

## Isomorphic Rings

Consider the subset  $S = \{0, 2, 4, 6, 8\}$  of  $\mathbb{Z}/10\mathbb{Z}$ . If we use the addition and multiplication of  $\mathbb{Z}/10\mathbb{Z}$  we see that  $S$  is a commutative ring. This is apparent from the following tables.

+	0	6	2	8	4
0	0	6	2	8	4
6	6	2	8	4	0
2	2	8	4	0	6
8	8	4	0	6	2
4	4	0	6	2	8

·	0	6	2	8	4
0	0	0	0	0	0
6	0	6	2	8	4
2	0	2	4	6	8
8	0	8	6	4	2
4	0	4	8	2	6

Now write out the addition and multiplication tables for  $\mathbb{Z}/5\mathbb{Z}$ . Label  $[0]$  as 0,  $[1]$  as 6,  $[2]$  as 2,  $[3]$  as 8, and  $[4]$  as 4. In general. What do you notice about the tables compared to the given tables for our set  $S$  above?

In general, *isomorphic rings* are rings that have the same structure, in the sense that the addition and multiplication tables of one are the same as the other, just with the elements relabeled. This idea is intuitive for small finite systems, but we need a definition to define isomorphisms that is easily applicable and that also works for large rings. We can do this with mappings. When we relabel elements, we are pairing every element of one ring  $R$  with a unique element in a new ring  $S$ . Thus, there is a function  $f : R \rightarrow S$  that assigns each  $r$  to its new label,  $f(r) \in S$ .

If we consider the preceding example, we have that  $f : \mathbb{Z}/5\mathbb{Z} \rightarrow S$  is given by

$$f(\bar{0}) = 0 \quad f(\bar{1}) = 6 \quad f(\bar{2}) = 2 \quad f(\bar{3}) = 8 \quad f(\bar{4}) = 4.$$

There are additional properties necessary so that  $f$  can change the addition and multiplication tables of  $\mathbb{Z}/5\mathbb{Z}$  into  $S$ . We generalize these conditions

with the following definition.

▷ A ring  $R$  is **isomorphic** to a ring  $S$ , written  $R \cong S$ , if there is a function  $f : R \rightarrow S$  such that:

1.  $f$  is injective (if  $f(r) = f(r')$  in  $S$  then  $r = r'$  in  $R$ )
2.  $f$  is surjective (for each  $s \in S$ , there is some  $r$  so that  $f(r) = s$ )
3.  $f(a + b) = f(a) + f(b)$  and  $f(ab) = f(a)f(b)$  for all  $a, b \in R$ .

In this case the function  $f$  is called an **isomorphism**.

▷ **Example** Consider the field of  $K$  of all  $2 \times 2$  matrices of the form  $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$  where  $a$  and  $b$  are real numbers. Let  $f : K \rightarrow \mathbb{C}$  by the rule

$$f \begin{pmatrix} a & b \\ -b & a \end{pmatrix} = a + bi.$$

We want to show that  $f$  defines an isomorphism.

$f$  is injective

Suppose  $f \begin{pmatrix} a & b \\ -b & a \end{pmatrix} = f \begin{pmatrix} r & s \\ -s & r \end{pmatrix}$ . So by definition this implies that  $a + bi = r + si$  in  $\mathbb{C}$ . By the rules of equality in  $\mathbb{C}$ , we must have  $a = r$  and  $b = s$ . Thus in  $K$  we have

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} = \begin{pmatrix} r & s \\ -s & r \end{pmatrix}$$

so  $f$  is injective.

$f$  is surjective

The function  $f$  is surjective because any complex number  $a + bi$  is the

image under  $f$  of the matrix  $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$  in  $K$ .

$$\underline{f(A + B) = f(A) + f(B)}$$

$$\begin{aligned} f\left[\begin{pmatrix} a & b \\ -b & a \end{pmatrix} + \begin{pmatrix} c & d \\ -d & c \end{pmatrix}\right] &= \begin{pmatrix} a + c & b + d \\ -b - d & a + c \end{pmatrix} \\ &= (a + c) + (b + d)i \\ &= (a + bi) + (c + di) \\ &= f\begin{pmatrix} a & b \\ -b & a \end{pmatrix} + f\begin{pmatrix} c & d \\ -d & c \end{pmatrix} \end{aligned}$$

$$\underline{f(AB) = f(A)f(B)}$$

$$\begin{aligned} f\left[\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \begin{pmatrix} c & d \\ -d & c \end{pmatrix}\right] &= f\begin{pmatrix} ac - bd & ad + bc \\ -ad - bc & ac - bd \end{pmatrix} \\ &= (ac - bd) + (ad + bc)i \\ &= (a + bi)(c + di) \\ &= f\begin{pmatrix} a & b \\ -b & a \end{pmatrix} f\begin{pmatrix} c & d \\ -d & c \end{pmatrix} \end{aligned}$$

It follows that  $f$  is an isomorphism.

$f : A \rightarrow B$  is a **bijjective mapping** if  $f$  is injective and  $f$  is surjective

**Example** Let  $R$  be any ring and  $\iota : R \rightarrow R$  is the identity map given by  $\iota(r) = r$ . This is called the inclusion map. Then we have

$$\iota(a + b) = a + b = \iota(a) + \iota(b)$$

and

$$\iota(ab) = ab = \iota(a)\iota(b).$$

Since  $\iota$  is bijection, it is an isomorphism.

**Exercise 3.3.1** Let  $f : \mathbb{Z}/6\mathbb{Z} \rightarrow \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$  be the bijection given by  $0 \rightarrow (0, 0)$ ;  $1 \rightarrow (1, 1)$ ;  $2 \rightarrow (0, 2)$ ;  $3 \rightarrow (1, 0)$ ;  $4 \rightarrow (0, 1)$ ;  $5 \rightarrow (1, 2)$ .

Use the addition and multiplication tables of  $\mathbb{Z}/6\mathbb{Z}$  and  $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$  to show that  $f$  is an isomorphism.

**Exercise 3.3.2** Use tables to show that  $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$  is isomorphic to the ring  $R$  of Exercise 2 in Section 3.1.

**Exercise 3.3.4** Let  $S$  be the subring  $\{0, 2, 4, 6, 8\}$  of  $\mathbb{Z}/10\mathbb{Z}$  and let  $\mathbb{Z}/5\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$ . Show that the following bijection from  $\mathbb{Z}/5\mathbb{Z}$  to  $S$  is *not* an isomorphism:

$$\bar{0} \rightarrow 0 \quad \bar{1} \rightarrow 2 \quad \bar{2} \rightarrow 4 \quad \bar{3} \rightarrow 6 \quad \bar{4} \rightarrow 8.$$

**Exercise 3.3.17** Show that the complex conjugation function  $f : \mathbb{C} \rightarrow \mathbb{C}$  given by  $f(a + bi) = a - bi$  is a bijection.

**Exercise 3.3.19** Show that  $S = \{0, 4, 8, 12, 16, 20, 24\}$  is a subring of  $\mathbb{Z}/28\mathbb{Z}$ . Then prove that the map  $f : \mathbb{Z}/7\mathbb{Z} \rightarrow S$  given by  $f([x]_7) = [8x]_{28}$  is an isomorphism.

**Exercise 3.3.5** Prove that the field  $\mathbb{R}$  of real numbers is isomorphic to the ring of all  $2 \times 2$  matrices of the form  $\begin{pmatrix} 0 & 0 \\ 0 & a \end{pmatrix}$ , with  $a \in \mathbb{R}$ . [*Hint*: Consider the function  $f$  given by  $f(a) = \begin{pmatrix} 0 & 0 \\ 0 & a \end{pmatrix}$ , with  $a \in \mathbb{R}$ .]

**Exercise 3.3.9** If  $f : \mathbb{Z} \rightarrow \mathbb{Z}$  is an isomorphism, prove that  $f$  is the identity map. [*Hint*: What are  $f(1), f(1 + 1), \dots, ?$ ]

### Ring Homomorphisms

▶ Let  $R$  and  $S$  be rings. A function  $f : R \rightarrow S$  is said to be a **homomorphism** if

$$f(a + b) = f(a) + f(b) \text{ and } f(ab) = f(a)f(b) \text{ for all } a, b \in R.$$

**Example** We define the zero map between two rings  $R$  and  $S$  given by  $z : R \rightarrow S$  given by  $z(r) = 0$  for every  $r \in R$  is a homomorphism because for any  $a, b \in R$

$$z(a + b) = 0 = 0 + 0 = z(a) + z(b)$$

and

$$z(ab) = 0 = 0 \cdot 0 = z(a)z(b).$$

When  $R$  and  $S$  both contain nonzero elements, then the zero map is neither injective nor surjective.

▶ **Example 11** Consider  $\mathbb{Z}/8\mathbb{Z}$ . The units are  $\{1, 3, 5, 7\}$ . Since being a unit is preserved under isomorphism, any ring isomorphic to  $\mathbb{Z}/8\mathbb{Z}$  will also have four units. Thus,  $\mathbb{Z}/8\mathbb{Z}$  is not isomorphic to any ring with less than 4 units. In particular,  $\mathbb{Z}/8\mathbb{Z}$  is not isomorphic to  $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$  because there are only two units in  $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ .

▶ **Theorem 3.3.10** Let  $f : R \rightarrow S$  be a homomorphism of rings. Then

1.  $f(0_R) = 0_S$
2.  $f(-a) = -f(a)$  for every  $a \in R$

## Intro to Modern Algebra Part 1a: Course Notes

3.  $f(a - b) = f(a) - f(b)$  for all  $a, b \in R$ .

If  $R$  is a ring with identity and  $f$  is surjective, then

1.  $S$  is a ring with identity  $f(1_R)$ .

2. Whenever  $u$  is a unit in  $R$ , then  $f(u)$  is a unit in  $S$  and  $f(u)^{-1} = f(u^{-1})$ .

▶ **Corollary 3.3.11** If  $f : R \rightarrow S$  is a homomorphism of rings, then the image of  $f$  is a subring of  $S$  where the image of  $f$  is given by

$$\text{Im}f = \{s \in S \mid s = f(r) \text{ for some } r \in R\} = \{f(r) \mid r \in R\}.$$

▶ **Example 3.3.11 a** State at least one reason why  $f : \mathbb{R} \rightarrow \mathbb{R}$  with  $f(x) = \sqrt{x}$  is not a homomorphism.

*Answer:* Let  $a, b \in \mathbb{R}$ , then  $f(a) + f(b) = \sqrt{a} + \sqrt{b}$  and  $f(a + b) = \sqrt{a + b}$ . So we see that  $f(a + b) \neq f(a) + f(b)$ .

**Exercise 3.3.11 b,c,d** State at least one reason why the given function is *not* a homomorphism.

(b)  $g : E \rightarrow E$  where  $E$  is the ring of even integers and  $f(x) = 3x$ .

(c)  $h : \mathbb{R} \rightarrow \mathbb{R}$  and  $f(x) = 2^x$

(d)  $k : \mathbb{Q} \rightarrow \mathbb{Q}$  where  $k(0) = 0$  and  $k\left(\frac{a}{b}\right) = \frac{b}{a}$  if  $a \neq 0$ .

**Exercise 3.3.12** Which of the following functions are homomorphisms?

(a)  $f : \mathbb{Z} \rightarrow \mathbb{Z}$  defined by  $f(x) = -x$ .

(b)  $f : \mathbb{Z}/2\mathbb{Z} \rightarrow \mathbb{Z}/2\mathbb{Z}$  defined by  $f(x) = -x$

(c)  $g : \mathbb{Q} \rightarrow \mathbb{Q}$  defined by  $g(x) = \frac{1}{x^2 + 1}$

(d)  $h : \mathbb{R} \rightarrow M\mathbb{R}$  defined by  $h(a) = \begin{pmatrix} a & 0 \\ a & 0 \end{pmatrix}$ .

(e)  $f : \mathbb{Z}/12\mathbb{Z} \rightarrow \mathbb{Z}/4\mathbb{Z}$ , defined by  $f([x]_{12}) = [x]_4$ , where  $[u]_n$  denotes the class of the integer  $u$  in  $\mathbb{Z}/n\mathbb{Z}$

**Example 3.3.15** Let  $f : R \rightarrow S$  be a homomorphism of rings. If  $r$  is a zero divisor in  $R$ , is  $f(r)$  a zero divisor in  $S$ ?

**Exercise 3.3.10** If  $R$  is a ring with identity and  $f : R \rightarrow S$  is a homomorphism from  $R$  to a ring  $S$ , prove that  $f(1_R)$  is an idempotent in  $S$ . [Idempotents were defined in Exercise 3.2.3.]

### Preserving Properties under Mappings

Suppose that  $f : R \rightarrow S$  is an isomorphism and the elements  $a, b, c, \dots$  of  $R$  have a particular property. If the elements of  $f(a), f(b), f(c), \dots$  of  $S$  have the same property then the property is **preserved by isomorphism**. For example, the property of being a zero element or being the identity element is preserved by isomorphism. One important idea with properties we know are invariant, is that we can use them to show that two rings are not isomorphic.

**Example 13** Suppose  $R$  is a commutative ring and  $f : R \rightarrow S$  is an isomorphism. Then for any  $a, b \in R$  we have  $ab = ba$  in  $R$ . Thus in  $S$ ,

$$f(a)f(b) = f(ab) = f(ba) = f(b)f(a).$$

**Example 3.3.34 a** If  $f : R \rightarrow S$  is an isomorphism of rings, is  $a \in R$  a zero divisor preserved by the isomorphism?



**Exercise 3.3.34 b,c** If  $f : R \rightarrow S$  is an isomorphism of ring, which of the following properties are preserved by this isomorphism? Justify your answers.

(b)  $a \in R$  is idempotent

(c)  $R$  is an integral domain

**Exercise 3.3.35 f** Show that  $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$  and  $\mathbb{Z}/16\mathbb{Z}$  are not isomorphic.