

# Chapter 1

## Relations and Functions



We begin by introducing some basic notation and terminology. Then we discuss relations and, in particular, equivalence relations, which we shall see several times throughout the book. In the final section, we talk about various sorts of functions.

### 1.1 Sets and Set Operations

A **set** is a collection of objects. We will see many sorts of sets throughout this course. Perhaps the most common will be sets of numbers. For instance, we have the set of **natural numbers**,

$$\mathbb{N} = \{1, 2, 3, \dots\},$$

the set of **integers**,

$$\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$$

and the set of **rational numbers**

$$\mathbb{Q} = \left\{ \frac{a}{b} : a, b \in \mathbb{Z}, b \neq 0 \right\}.$$

We also write  $\mathbb{R}$  for the set of **real numbers** and  $\mathbb{C}$  for the set of **complex numbers**.

But sets do not necessarily consist of numbers. Indeed, we can consider the set of all letters of the alphabet, the set of all polynomials with even integers as coefficients or the set of all lines in the plane with positive slope.

The objects in a set are called its **elements**. We write  $a \in S$  if  $a$  is an element of a set  $S$ . Thus,  $-3 \in \mathbb{Z}$  but  $-3 \notin \mathbb{N}$ . The set with no elements is called the **empty set**, and denoted  $\emptyset$ . Any other set is said to be **nonempty**.

If  $S$  and  $T$  are sets, then we say that  $S$  is a **subset** of  $T$ , and write  $S \subseteq T$ , if every element of  $S$  is also an element of  $T$ . Of course,  $S \subseteq S$ . We say that  $S$  is a **proper** subset of  $T$ , and write  $S \subsetneq T$ , if  $S \subseteq T$  but  $S \neq T$ . Thus, it is certainly true that  $\mathbb{N} \subseteq \mathbb{Z}$ , but we can be more precise and write  $\mathbb{N} \subsetneq \mathbb{Z}$ .

For any two sets  $S$  and  $T$ , their **intersection**,  $S \cap T$ , is the set of all elements that lie in  $S$  and  $T$  simultaneously.

*Example 1.1.* Let  $S = \{1, 2, 3, 4, 5\}$  and  $T = \{2, 4, 6, 8, 10\}$ . Then  $S \cap T = \{2, 4\}$ .

We can extend this notion to the intersection of an arbitrary collection of sets. If  $I$  is a nonempty set and, for each  $i \in I$ , we have a set  $T_i$ , then we write  $\bigcap_{i \in I} T_i$  for the set of elements that lie in all of the  $T_i$  simultaneously.

*Example 1.2.* For each  $q \in \mathbb{Q}$ , let  $T_q = \{r \in \mathbb{R} : r < 2^q\}$ . Then  $\bigcap_{q \in \mathbb{Q}} T_q = \{r \in \mathbb{R} : r \leq 0\}$ .

Also, for any sets  $S$  and  $T$ , their **union**,  $S \cup T$ , is the set of all elements that lie in  $S$  or  $T$  (or both).

*Example 1.3.* Using the same  $S$  and  $T$  as in Example 1.1, we have

$$S \cup T = \{1, 2, 3, 4, 5, 6, 8, 10\}.$$

Furthermore, if  $I$  is a nonempty set and we have a set  $T_i$  for each  $i \in I$ , then we write  $\bigcup_{i \in I} T_i$  for the union of all of the  $T_i$ ; that is, the set of all elements that lie in at least one of the  $T_i$ .

*Example 1.4.* If we use the same sets  $T_q$  as in Example 1.2, we have  $\bigcup_{q \in \mathbb{Q}} T_q = \mathbb{R}$ .

In addition, for any two sets  $S$  and  $T$ , the **set difference** (or **relative complement**) is the set  $S \setminus T = \{a \in S : a \notin T\}$ .

*Example 1.5.* Once again using  $S$  and  $T$  as in Example 1.1, we have  $S \setminus T = \{1, 3, 5\}$ .

We will need one more definition. The following construction is named after René Descartes.

**Definition 1.1.** Let  $S$  and  $T$  be any sets. Then the **Cartesian product**  $S \times T$  is the set of all ordered pairs  $(s, t)$ , with  $s \in S$  and  $t \in T$ .

*Example 1.6.* Let  $S = \{1, 2, 3\}$  and  $T = \{2, 3\}$ . Then

$$S \times T = \{(1, 2), (1, 3), (2, 2), (2, 3), (3, 2), (3, 3)\}.$$

There is also a Cartesian product of finitely many sets. For any sets  $T_1, T_2, \dots, T_n$ , we let  $T_1 \times T_2 \times \dots \times T_n$  be the set of all ordered  $n$ -tuples  $(t_1, t_2, \dots, t_n)$ , with  $t_i \in T_i$  for all  $i$ .

*Example 1.7.* Let  $T_1 = \{1, 2\}$ ,  $T_2 = \{a, b\}$  and  $T_3 = \{2, 3\}$ . Then  $T_1 \times T_2 \times T_3$  is the set

$$\{(1, a, 2), (1, a, 3), (1, b, 2), (1, b, 3), (2, a, 2), (2, a, 3), (2, b, 2), (2, b, 3)\}.$$

### Exercises

- 1.1.** Let  $S = \{1, 2, 3\}$  and  $T = \{3, 4\}$ . Find  $S \cap T$ ,  $S \cup T$ ,  $S \setminus T$ ,  $T \setminus S$  and  $S \times T$ .
- 1.2.** Let  $R = \{a, b, c\}$ ,  $S = \{a, c, d\}$  and  $T = \{c, e, f\}$ . Find  $R \cap S$ ,  $R \cap (S \setminus T)$ ,  $S \cup T$ ,  $S \cap (R \cup T)$  and  $R \times S$ .
- 1.3.** Let  $R$ ,  $S$  and  $T$  be sets with  $R \subseteq S$ . Show that  $R \cup T \subseteq S \cup T$ .
- 1.4.** Let  $S = \{1, 2, \dots, n\}$ , for some positive integer  $n$ . Show that  $S$  has  $2^n$  subsets.
- 1.5.** Let  $R$ ,  $S$  and  $T$  be any sets. Show that  $R \cup (S \cap T) = (R \cup S) \cap (R \cup T)$ .
- 1.6.** For each positive integer  $n$ , let  $T_n = \{\frac{a}{n} : a \in \mathbb{Z}\}$ .
  1. What is  $\bigcup_{n=1}^{\infty} T_n$ ?
  2. What is  $\bigcap_{n=1}^{\infty} T_n$ ?

## 1.2 Relations

We are going to use relations (in particular, the equivalence relations and functions that we will see in the next two sections) quite a few times in this course.

**Definition 1.2.** Let  $S$  and  $T$  be sets. Then a **relation** from  $S$  to  $T$  is a subset  $\rho$  of  $S \times T$ . If  $s \in S$  and  $t \in T$ , then we write  $s\rho t$  if  $(s, t) \in \rho$ ; otherwise, we write  $s \not\rho t$ . In particular, a **relation** on  $S$  is a relation from  $S$  to  $S$ .

*Example 1.8.* Let  $S = \{1, 2, 3\}$  and  $T = \{1, 2, 3, 4\}$ . Define a relation  $\rho$  from  $S$  to  $T$  via  $s\rho t$  if and only if  $st^2 \leq 4$ . Then  $\rho = \{(1, 1), (1, 2), (2, 1), (3, 1)\}$ . In particular,  $3\rho 1$  but  $1 \not\rho 3$ .

We will focus on relations on a set. Let us discuss a few properties enjoyed by some relations.

**Definition 1.3.** Let  $\rho$  be a relation on  $S$ . We say that  $\rho$  is **reflexive** if  $a\rho a$  for all  $a \in S$ .

*Example 1.9.* On  $\mathbb{Z}$ , the relation  $\leq$  is reflexive, but  $<$  is not. Indeed,  $a \leq a$  for all integers  $a$ , but  $1$  is not less than  $1$ .

**Definition 1.4.** A relation  $\rho$  on a set  $S$  is **symmetric** if  $a\rho b$  implies  $b\rho a$ .

*Example 1.10.* On  $\mathbb{Z}$ , neither  $\leq$  nor  $<$  is symmetric, as  $1 < 2$  but 2 is not less than 1 (and similarly for  $\leq$ ). Define  $\rho$  via  $a\rho b$  if and only if  $|a - b| \leq 10$ . Then  $\rho$  is symmetric. Indeed, if  $a\rho b$ , then  $|a - b| \leq 10$ , and so  $|b - a| = |a - b| \leq 10$ ; thus,  $b\rho a$ .

**Definition 1.5.** Let  $\rho$  be a relation on a set  $S$ . We say that  $\rho$  is **transitive** if, whenever  $a\rho b$  and  $b\rho c$ , we also have  $a\rho c$ .

*Example 1.11.* On  $\mathbb{Z}$ , the relations  $\leq$  and  $<$  are both transitive. (If  $a \leq b$  and  $b \leq c$ , then  $a \leq c$ .) However, the relation  $\rho$  from Example 1.10 is not, since  $1\rho 8$  and  $8\rho 13$ , but  $1 \not\rho 13$ .

These three properties lead us directly to the next section.

### Exercises

**1.7.** Let  $S = \{1, 2, 3\}$  and  $T = \{3, 4, 5, 6, 7, 8\}$ . Define a relation  $\rho$  from  $S$  to  $T$  via  $a\rho b$  if and only if  $|a^2 - b| \leq 1$ . Find all pairs  $(a, b) \in S \times T$  such that  $a\rho b$ .

**1.8.** Define a relation  $\rho$  on  $\mathbb{Z}$  via  $a\rho b$  if and only if  $ab$  is even. Is  $\rho$  reflexive? Symmetric? Transitive?

**1.9.** Define a relation  $\rho$  on  $\mathbb{R}$  via  $a\rho b$  if and only if  $a - b \in \mathbb{Q}$ . Is  $\rho$  reflexive? Symmetric? Transitive?

**1.10.** Define a relation  $\rho$  on  $\mathbb{R}$  via  $a\rho b$  if and only if  $a - b \in \mathbb{N}$ . Is  $\rho$  reflexive? Symmetric? Transitive?

**1.11.** 1. How many relations are there on  $\{1, 2, 3\}$ ?  
2. How many of these relations are symmetric?

**1.12.** For each of the eight subsets of {reflexive, symmetric, transitive}, find a relation on  $\{1, 2, 3\}$  that has the properties in that subset, but not the properties that are not in the subset.

## 1.3 Equivalence Relations

**Definition 1.6.** An **equivalence relation** on a set  $S$  is a relation that is reflexive, symmetric and transitive.

We will use the symbol  $\sim$  to denote an equivalence relation.

*Example 1.12.* On  $\mathbb{Z}$ , let us say that  $a \sim b$  if and only if  $a + b$  is even. We claim that  $\sim$  is an equivalence relation. If  $a \in \mathbb{Z}$ , then  $a + a$  is certainly even, so  $a \sim a$ , and  $\sim$  is reflexive. If  $a \sim b$ , then  $a + b$  is even. But this also means that  $b + a$  is even, and hence  $b \sim a$ . Thus,  $\sim$  is symmetric. Finally, suppose that  $a \sim b$  and  $b \sim c$ . Then  $a + b$  and  $b + c$  are both even. This means that their sum,  $a + 2b + c$ , is even. As  $2b$  is even, we see that  $a + c$  is even, and hence  $a \sim c$ . That is,  $\sim$  is transitive.

*Example 1.13.* On the set  $S = \{a \in \mathbb{Z} : 1 \leq a \leq 20\}$ , let  $a \sim b$  if and only if  $a = 2^m b$  for some  $m \in \mathbb{Z}$ . Let us verify that this is an equivalence relation. Reflexivity: Note that  $a = 2^0 a$ , and hence  $a \sim a$ . Symmetry: If  $a \sim b$ , say  $a = 2^m b$ , then  $b = 2^{-m} a$ , and hence  $b \sim a$ . Transitivity: If  $a \sim b$  and  $b \sim c$ , say  $a = 2^m b$  and  $b = 2^n c$ , then  $a = 2^{m+n} c$ , and therefore  $a \sim c$ .

*Example 1.14.* On  $\mathbb{R}$ , let us say that  $a \sim b$  if and only if  $a - b \in \mathbb{Z}$ . Let us check that it is an equivalence relation. Reflexivity: If  $a \in \mathbb{R}$ , then  $a - a = 0 \in \mathbb{Z}$ , and hence  $a \sim a$ . Symmetry: Let  $a \sim b$ . Then  $a - b \in \mathbb{Z}$ , and hence  $b - a = -(a - b) \in \mathbb{Z}$ . Thus,  $b \sim a$ . Transitivity: Suppose that  $a \sim b$  and  $b \sim c$ . Then  $a - b, b - c \in \mathbb{Z}$ , and hence  $a - c = (a - b) + (b - c) \in \mathbb{Z}$ . That is,  $a \sim c$ .

Let us try something slightly more complicated.

*Example 1.15.* Let  $S = \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ . Define  $\sim$  on  $S$  via  $(a, b) \sim (c, d)$  if and only if  $ad = bc$ . We must verify that  $\sim$  is an equivalence relation. Reflexivity: As  $ab = ba$ , we have  $(a, b) \sim (a, b)$  for all integers  $a$  and nonzero integers  $b$ . Symmetry: Suppose that  $(a, b) \sim (c, d)$ . Then  $ad = bc$ , and this also tells us that  $(c, d) \sim (a, b)$ . Transitivity: Let  $(a, b) \sim (c, d)$  and  $(c, d) \sim (e, f)$ . Then  $ad = bc$  and  $cf = de$ . Thus,  $adf = bcf = bde$ . Since we are assuming that  $d \neq 0$ , this means that  $af = be$ . Therefore,  $(a, b) \sim (e, f)$ .

Equivalence relations are very special.

**Definition 1.7.** Let  $\sim$  be an equivalence relation on a set  $S$ . If  $a \in S$ , then the **equivalence class** of  $a$ , denoted  $[a]$ , is the set  $\{b \in S : a \sim b\}$ .

Why are equivalence classes so interesting? We need another definition.

**Definition 1.8.** Let  $S$  be a set, and let  $T$  be a set of nonempty subsets of  $S$ . We say that  $T$  is a **partition** of  $S$  if every  $a \in S$  lies in exactly one set in  $T$ .

*Example 1.16.* Let  $S = \{1, 2, 3, 4, 5, 6, 7\}$  and  $T = \{\{1, 3, 4, 6\}, \{2, 7\}, \{5\}\}$ . Then  $T$  is a partition of  $S$ .

What is the connection between these concepts?

**Theorem 1.1.** Let  $S$  be a set, and  $\sim$  an equivalence relation on  $S$ . Then the equivalence classes with respect to  $\sim$  form a partition of  $S$ . In particular, if  $a \in S$ , then  $a \in [a]$  and, furthermore,  $a \in [b]$  if and only if  $[a] = [b]$ .

*Proof.* As  $\sim$  is reflexive,  $a \sim a$ , and hence  $a \in [a]$  for every  $a \in S$ . In particular, the equivalence classes are not empty, and every element of  $S$  is in at least one of them. Suppose that  $d \in [a] \cap [c]$ . We must show that  $[a] = [c]$ . If  $e \in [a]$ , then  $a \sim e$ . Also,  $d \in [a]$  means that  $a \sim d$ , and hence  $d \sim a$  by symmetry. Also,  $c \sim d$ . By transitivity,  $c \sim a$ , and then  $c \sim e$ . Thus,  $e \in [c]$ , and therefore  $[a] \subseteq [c]$ . By the same argument,  $[c] \subseteq [a]$ , and hence  $[a] = [c]$ . Thus, the equivalence classes

do indeed form a partition. To prove the final statement of the theorem, note that if  $a \in [a] \cap [b]$ , then  $[a] = [b]$  and, conversely, if  $[a] = [b]$ , then  $a \in [a] = [b]$ .  $\square$

So, the equivalence classes break the set down into subsets having no elements in common. It is important to note that, unless there is only one element in an equivalence class, the representative chosen for that class is not unique. That is, if  $b \in [a]$ , then we could just as easily write  $[b]$  instead of  $[a]$ . They are the same class. This complicates matters a bit when we define operations on equivalence classes, as we will find ourselves doing throughout the course. We must make sure that our operations are well-defined; that is, that they do not depend upon the particular representative of the class that we use.

Let us discuss the equivalence classes determined by the relations in our earlier examples. The plan is always the same. We know that each element of the set is in exactly one class. Thus, we will keep looking for elements of the set that are not in any classes we have constructed, and obtain new classes in this way.

*Example 1.17.* In Example 1.12, let us start with 0. We know that  $a \sim 0$  if and only if  $a$  is even. Thus,

$$[0] = \{\dots, -6, -4, -2, 0, 2, 4, 6, \dots\}.$$

(Note that we would have obtained the same class had we started, for instance, with 14. Since  $14 \in [0]$ , we have  $[0] = [14]$ .) We have not yet found 1, so we note that  $a \sim 1$  if and only if  $a + 1$  is even; that is, if and only if  $a$  is odd. Therefore,

$$[1] = \{\dots, -5, -3, -1, 1, 3, 5, \dots\}.$$

(Again, we could just as easily have used  $[-3]$ .) We have now found all elements of  $\mathbb{Z}$ . Thus, there are only two equivalence classes,  $[0]$  and  $[1]$ .

*Example 1.18.* In Example 1.13, we may as well start with 1. We have

$$[1] = \{1, 2, 4, 8, 16\}.$$

As we have not yet found 3,

$$[3] = \{3, 6, 12\}.$$

We still do not have 5, and thus we take

$$[5] = \{5, 10, 20\}.$$

Similarly, we obtain

$$\begin{aligned} [7] &= \{7, 14\}, [9] = \{9, 18\}, [11] = \{11\}, \\ [13] &= \{13\}, [15] = \{15\}, [17] = \{17\}, \text{ and } [19] = \{19\}. \end{aligned}$$

Once again, we could have used  $[8]$  in place of  $[1]$ , for instance.

The other two examples are a bit trickier, since there are infinitely many equivalence classes. But we can attempt to describe them.

*Example 1.19.* In Example 1.14, we see that  $b \in [a]$  if and only if the difference between  $a$  and  $b$  is an integer. Thus, for instance,

$$[23.86] = \{\dots, -2.14, -1.14, -0.14, 0.86, 1.86, 2.86, \dots\}.$$

Listing the classes is an impossible task. How, then, to describe them? We note that for any real number  $a$ , there is certainly an integer  $k$  such that  $0 \leq a - k < 1$ . Now,  $a \sim (a - k)$ , and hence every element of  $\mathbb{R}$  is in a class  $[b]$ , for some  $0 \leq b < 1$ . Furthermore, if  $0 \leq b, c < 1$ , then  $0 \leq |b - c| < 1$  and therefore  $b - c$  can only be an integer if  $b = c$ . That is, if  $0 \leq b, c < 1$  and  $b \neq c$ , then  $[b] \neq [c]$ . Thus, the equivalence classes are precisely

$$\{[b] : b \in \mathbb{R}, 0 \leq b < 1\}.$$

*Example 1.20.* What about Example 1.15? We note that  $(c, d) \in [(a, b)]$  if and only if  $ad = bc$ . Another way to say this is that  $\frac{a}{b} = \frac{c}{d}$ . Thus,  $[(a, b)]$  consists of all ordered pairs  $(c, d)$ , with  $c, d \in \mathbb{Z}$  and  $d \neq 0$ , such that  $\frac{a}{b} = \frac{c}{d}$ . This is, in fact, exactly how the rational numbers are constructed! We need to ensure that  $\frac{2}{3}$  and  $\frac{4}{6}$  are treated as the same fraction, and these equivalence classes make that happen. We obtain one equivalence class for each fraction  $\frac{a}{b}$ . For instance,

$$[(2, 3)] = \{\dots, (-6, -9), (-4, -6), (-2, -3), (2, 3), (4, 6), (6, 9), \dots\}.$$

### Exercises

**1.13.** Define a relation  $\sim$  on  $\mathbb{N}$  via  $a \sim b$  if and only if  $a - b = 3k$ , for some  $k \in \mathbb{Z}$ . Is  $\sim$  an equivalence relation? If so, what are the equivalence classes?

**1.14.** Define a relation  $\sim$  on  $\{1, 2, 3, 4, 5, 6, 7\}$  via  $a \sim b$  if and only if  $a$  and  $b$  are both even or both odd. Is  $\sim$  an equivalence relation? If so, what are the equivalence classes?

**1.15.** Define a relation  $\sim$  on  $\mathbb{Z}$  via  $a \sim b$  if and only if  $|a| = |b|$ . Is  $\sim$  an equivalence relation? If so, what are the equivalence classes?

**1.16.** Define a relation  $\sim$  on  $\mathbb{Z}$  via  $a \sim b$  if and only if  $ab > 0$ . Is  $\sim$  an equivalence relation? If so, what are the equivalence classes?

**1.17.** Let  $S$  be the set of all subsets of  $\mathbb{Z}$ . Define a relation  $\sim$  on  $S$  via  $T \sim U$  if and only if  $T \subseteq U$ . Is  $\sim$  an equivalence relation? If so, what are the equivalence classes?

**1.18.** Let  $S$  be the set of all subsets of  $\mathbb{Z}$ . Define a relation  $\sim$  on  $S$  via  $T \sim U$  if and only if  $T \setminus U$  and  $U \setminus T$  are both finite. Show that  $\sim$  is an equivalence relation and describe  $[\{1, 2, 3\}]$  and  $[\{\dots, -4, -2, 0, 2, 4, \dots\}]$ .

**1.19.** On the plane  $\mathbb{R}^2$ , define a relation  $\sim$  via  $(a, b) \sim (c, d)$  if and only if  $3a - b = 3c - d$ . Show that  $\sim$  is an equivalence relation, and describe  $[(4, 2)]$ .

**1.20.** Let  $S$  be a nonempty set. Show that for any partition of  $S$ , there is an equivalence relation on  $S$  having the sets in the partition as its equivalence classes.

**1.21.** Find an equivalence relation on  $\mathbb{N}$  having exactly two equivalence classes, one of which contains exactly three elements.

**1.22.** Suppose there is a relation  $\rho$  on a set  $S$ , such that  $\rho$  is both reflexive and transitive. Define  $\sim$  on  $S$  via  $a \sim b$  if and only if  $a\rho b$  and  $b\rho a$ . Show that  $\sim$  is an equivalence relation.

## 1.4 Functions

Let us give two equivalent definitions of a function. Formally, if  $S$  and  $T$  are sets, then a function from  $S$  to  $T$  is a relation  $\rho$  from  $S$  to  $T$  such that, for each  $s \in S$ , there is exactly one  $t \in T$  such that  $s\rho t$ . In practice, nobody really thinks of functions in this way. The working definition follows.

**Definition 1.9.** Let  $S$  and  $T$  be any sets. Then a **function**  $\alpha : S \rightarrow T$  is a rule assigning, to each  $s \in S$ , an element  $\alpha(s)$  of  $T$ .

Readers who have studied calculus will no doubt be familiar with functions from  $\mathbb{R}$  to  $\mathbb{R}$ .

*Example 1.21.* We can define a function  $\alpha : \mathbb{R} \rightarrow \mathbb{R}$  via  $\alpha(a) = 5a^3 - 4a^2 + 7a + 3$  for all  $a \in \mathbb{R}$ .

But we do not need to go from  $\mathbb{R}$  to  $\mathbb{R}$ .

*Example 1.22.* We can define a function  $\alpha : \mathbb{Z} \rightarrow \mathbb{Q}$  via  $\alpha(a) = (-2)^a$  for all  $a \in \mathbb{Z}$ .

In fact, the sets involved do not have to be sets of numbers.

*Example 1.23.* Let  $S$  be the set of all English words and  $T$  the set of letters in the alphabet. We can define  $\alpha : S \rightarrow T$  by letting  $\alpha(w)$  be the first letter of the word  $w$ , for every  $w \in S$ .

A few properties enjoyed by certain functions are important.

**Definition 1.10.** A function  $\alpha : S \rightarrow T$  is **one-to-one** (or **injective**) if  $\alpha(s_1) = \alpha(s_2)$  implies  $s_1 = s_2$ , for all  $s_1, s_2 \in S$ .

Putting this another way, a one-to-one function sends different elements to different places.

*Example 1.24.* Define functions  $\alpha$  and  $\beta$  from  $\mathbb{R}$  to  $\mathbb{R}$  via  $\alpha(a) = a^2$  and  $\beta(a) = a^3$ , for all  $a \in \mathbb{R}$ . Then  $\alpha$  is not one-to-one, since  $\alpha(1) = \alpha(-1)$ , but  $\beta$  is one-to-one, since if  $a^3 = b^3$ , then taking the cube root of both sides, we have  $a = b$ , for any  $a, b \in \mathbb{R}$ .

**Definition 1.11.** A function  $\alpha : S \rightarrow T$  is **onto** (or **surjective**) if, for every  $t \in T$ , there exists at least one  $s \in S$  such that  $\alpha(s) = t$ .

*Example 1.25.* Define  $\alpha$  and  $\beta$  as in Example 1.24. Then  $\alpha$  is not onto, since there is no  $a \in \mathbb{R}$  such that  $\alpha(a) = -1$ . However, if  $b \in \mathbb{R}$ , then  $\beta(\sqrt[3]{b}) = b$ ; thus,  $\beta$  is onto.

We should not get the idea that one-to-one and onto always occur together.

*Example 1.26.* Define  $\alpha : \mathbb{R} \rightarrow \mathbb{R}$  via  $\alpha(a) = 2^a$ . Then  $\alpha$  is one-to-one, for if  $2^a = 2^b$ , then taking the base 2 logarithm of both sides, we see that  $a = b$ . On the other hand, there is no  $a \in \mathbb{R}$  such that  $2^a = -1$ , so  $\alpha$  is not onto.

However, it is nice when we can combine the two properties.

**Definition 1.12.** A function  $\alpha : S \rightarrow T$  is **bijective** if it is one-to-one and onto.

An equivalent way of expressing this property is that for each  $t \in T$ , there is exactly one  $s \in S$  such that  $\alpha(s) = t$ . There must be such an  $s$ , since  $\alpha$  is onto, but if  $\alpha(s_1) = \alpha(s_2) = t$ , for some  $s_1, s_2 \in S$ , then since  $\alpha$  is one-to-one,  $s_1 = s_2$ . For this reason, a bijective function is also known as a **one-to-one correspondence**.

*Example 1.27.* Combining Examples 1.24 and 1.25, we see that  $\alpha : \mathbb{R} \rightarrow \mathbb{R}$  given by  $\alpha(a) = a^3$  is bijective.

Let us discuss how to combine functions.

**Definition 1.13.** Let  $R, S$  and  $T$  be sets, and let  $\alpha : R \rightarrow S$  and  $\beta : S \rightarrow T$  be functions. Then the **composition**,  $\beta \circ \alpha$ , or simply  $\beta\alpha$ , is the function from  $R$  to  $T$  given by  $(\beta\alpha)(r) = \beta(\alpha(r))$  for all  $r \in R$ .

Note that when we write  $\beta\alpha$ , we are applying  $\alpha$  first, then  $\beta$ . The order is important! Indeed, depending upon the sets involved, it is possible that applying  $\beta$  first, then  $\alpha$ , would not make sense. But even if it did make sense, the result would not necessarily be the same.

*Example 1.28.* Define functions  $\alpha$  and  $\beta$  from  $\mathbb{R}$  to  $\mathbb{R}$  via  $\alpha(a) = a^3 + 1$  and  $\beta(a) = a^2$ , for all  $a \in \mathbb{R}$ . Then  $(\beta\alpha)(a) = \beta(a^3 + 1) = a^6 + 2a^3 + 1$ , whereas  $(\alpha\beta)(a) = \alpha(a^2) = a^6 + 1$ , for all  $a \in \mathbb{R}$ . That is,  $\beta\alpha$  and  $\alpha\beta$  are different functions.

We can list a few important properties of the composition of functions.

**Theorem 1.2.** Let  $\alpha : R \rightarrow S$ ,  $\beta : S \rightarrow T$  and  $\gamma : T \rightarrow U$  be functions. Then

1.  $(\gamma\beta)\alpha = \gamma(\beta\alpha)$ ;
2. if  $\alpha$  and  $\beta$  are one-to-one, then so is  $\beta\alpha$ ;

3. if  $\alpha$  and  $\beta$  are onto, then so is  $\beta\alpha$ ; and  
 4. if  $\alpha$  and  $\beta$  are bijective, then so is  $\beta\alpha$ .

*Proof.* (1) Take any  $r \in R$ . Then  $((\gamma\beta)\alpha)(r) = (\gamma\beta)(\alpha(r)) = \gamma(\beta(\alpha(r)))$ . Similarly,  $(\gamma(\beta\alpha))(r) = \gamma((\beta\alpha)(r)) = \gamma(\beta(\alpha(r)))$ .

(2) Suppose that  $(\beta\alpha)(r_1) = (\beta\alpha)(r_2)$  for some  $r_1, r_2 \in R$ . Then  $\beta(\alpha(r_1)) = \beta(\alpha(r_2))$ . Since  $\beta$  is one-to-one,  $\alpha(r_1) = \alpha(r_2)$ . Since  $\alpha$  is one-to-one,  $r_1 = r_2$ .

(3) Take any  $t \in T$ . Since  $\beta$  is onto, there exists an  $s \in S$  such that  $\beta(s) = t$ . But  $\alpha$  is also onto, so there exists an  $r \in R$  such that  $\alpha(r) = s$ . Thus,  $(\beta\alpha)(r) = \beta(\alpha(r)) = \beta(s) = t$ .

(4) Combine (2) and (3). □

The following additional property of bijective functions can be useful.

**Theorem 1.3.** *Let  $\alpha : S \rightarrow T$  be a bijective function. Then there exists a bijective function  $\beta : T \rightarrow S$  such that  $(\beta\alpha)(s) = s$  for all  $s \in S$  and  $(\alpha\beta)(t) = t$  for all  $t \in T$ .*

*Proof.* Since  $\alpha$  is bijective, for any  $t \in T$ , there is a unique  $s \in S$  such that  $\alpha(s) = t$ . Define  $\beta : T \rightarrow S$  via  $\beta(t) = s$ . By definition, we have  $(\beta\alpha)(s) = \beta(\alpha(s)) = s$ , for all  $s \in S$ . Also, if  $t \in T$ , then choosing  $s$  such that  $\alpha(s) = t$ , we have  $\beta(t) = s$ , and therefore  $(\alpha\beta)(t) = \alpha(\beta(t)) = \alpha(s) = t$ , as required. It remains to show that  $\beta$  is bijective. But if  $\beta(t_1) = \beta(t_2)$ , then

$$t_1 = (\alpha\beta)(t_1) = \alpha(\beta(t_1)) = \alpha(\beta(t_2)) = (\alpha\beta)(t_2) = t_2,$$

so  $\beta$  is one-to-one. Furthermore, if  $s \in S$ , then  $\beta(\alpha(s)) = (\beta\alpha)(s) = s$ , and hence  $\beta$  is onto. □

*Example 1.29.* Let  $\alpha : \mathbb{R} \rightarrow \mathbb{R}$  be given by  $\alpha(a) = a^3$  for all  $a$ . Example 1.27 showed us that  $\alpha$  is bijective. It is easily checked that if we let  $\beta : \mathbb{R} \rightarrow \mathbb{R}$  be given by  $\beta(a) = \sqrt[3]{a}$  for all  $a$ , then  $(\alpha\beta)(a) = (\beta\alpha)(a) = a$  for all  $a$ .

We close the chapter by defining two special types of functions.

**Definition 1.14.** A **permutation** of a set  $S$  is a bijective function from  $S$  to  $S$ .

*Example 1.30.* By Example 1.27, the function  $\alpha : \mathbb{R} \rightarrow \mathbb{R}$  given by  $\alpha(a) = a^3$  is a permutation of  $\mathbb{R}$ .

*Example 1.31.* Let  $S = \{1, 2, 3, 4\}$ . Define  $\alpha : S \rightarrow S$  via  $\alpha(1) = 3$ ,  $\alpha(2) = 2$ ,  $\alpha(3) = 4$  and  $\alpha(4) = 1$ . Then  $\alpha$  is a permutation of  $S$ .

As this last example illustrates, a permutation is simply a rearrangement of the elements of  $S$ .

**Definition 1.15.** Let  $S$  be a set. Then a **binary operation** on  $S$  is a function from  $S \times S$  to  $S$ .

*Example 1.32.* We can define a binary operation  $*$  on  $\mathbb{R}$  via  $a * b = 2a^2b - 3b^4 + 5$ , for all  $a, b \in \mathbb{R}$ . (Putting this in terms of functions, we could write  $\alpha((a, b)) = 2a^2b - 3b^4 + 5$  for all  $a, b \in \mathbb{R}$ .)

Note that in order to obtain a binary operation, we must stay within our original set. For instance, we would not get a binary operation on  $\mathbb{N}$  if we tried to let  $a * b = \frac{a}{b}$ , for the simple reason that  $1 * 2 = \frac{1}{2} \notin \mathbb{N}$ .

### Exercises

**1.23.** Define  $\alpha : \{1, 2, 3, 4\} \rightarrow \{1, 2, 3, 4, 5, 6, 7\}$  via  $\alpha(a) = 2a - 1$ . Is this function one-to-one? Is it onto?

**1.24.** Define  $\alpha : \mathbb{R} \rightarrow \mathbb{R}$  via  $\alpha(a) = \sqrt[3]{a+1} - 2$ . Is this function one-to-one? Is it onto?

**1.25.** Let  $S$  be the set of real numbers and  $T$  the set of positive real numbers. Define  $\alpha : S \rightarrow T$  via  $\alpha(a) = 2^{3a-5}$ . Show that  $\alpha$  is a bijection and find  $\beta : T \rightarrow S$  such that  $(\beta\alpha)(a) = a$  for all  $a \in S$ .

**1.26.** Define  $\alpha : \mathbb{R} \rightarrow \mathbb{R}$  via

$$\alpha(a) = \begin{cases} 4a - 3, & a \leq 1 \\ a^2, & a > 1. \end{cases}$$

Show that  $\alpha$  is bijective and find  $\beta : \mathbb{R} \rightarrow \mathbb{R}$  such that  $(\beta\alpha)(a) = a$  for all  $a \in \mathbb{R}$ .

**1.27.** Which of the following are binary operations on  $\mathbb{N}$ ?

1.  $a * b = ab$
2.  $a * b = a - b$
3.  $a * b = 3$  for all  $a$  and  $b$

**1.28.** Let  $S$  be a finite set, and suppose that  $\alpha : S \rightarrow S$  is a one-to-one function. Show that  $\alpha$  is a permutation of  $S$ . Construct an explicit counterexample to show that this need not be true if  $S$  is infinite.

**1.29.** Let  $\alpha : R \rightarrow S$  and  $\beta : S \rightarrow T$  be functions, and suppose that  $\beta\alpha$  is onto. Must  $\alpha$  be onto? Must  $\beta$ ?

**1.30.** Let  $\alpha : R \rightarrow S$  and  $\beta : S \rightarrow T$  be functions, and suppose that  $\beta\alpha$  is one-to-one. Must  $\alpha$  be one-to-one? Must  $\beta$ ?

**1.31.** Let  $S$  be a set with  $m$  elements and  $T$  a set with  $n$  elements, for some positive integers  $m$  and  $n$ .

1. How many functions are there from  $S$  to  $T$ ?
2. How many of these functions are one-to-one?

**1.32.** Let  $S$  and  $T$  be sets and  $\alpha : S \rightarrow T$  a function. Show that there exist a set  $R$  and functions  $\beta : S \rightarrow R$  and  $\gamma : R \rightarrow T$  such that  $\beta$  is onto,  $\gamma$  is one-to-one and  $\alpha = \gamma\beta$ .