

---

---

# CHAPTER 1

---

## Preliminaries

At the turn of the 20th century, David Hilbert (1862–1943) aimed to build a sound foundation for mathematics using *axiomization*. On August 8, 1900, Hilbert gave a historical speech at the Paris Conference of the International Congress of Mathematicians. He proposed 23 problems as the goal of the mathematical research of the 20th century. He aimed to answer the following questions: Is mathematics consistent? Is mathematics complete? Is mathematics decidable? Although this great mission eventually failed, Bertrand Russell (1872–1970) and Alfred North Whitehead (1861–1947) did pioneer work on set theory and logics in their great book *Principia Mathematica*.

In this chapter, basic notions and terminologies such as sets, functions and relations are discussed without delving into great details. These are basic tools for the whole book.

## 1.1 Basic Ideas of Set Theory

We will not plunge into a formal definition of sets and its subsequent philosophical discussions. We will simply say that a **set** is a collection of “objects”, which we will call **elements**. When given a set, there will be no ambiguity on what elements are contained in it. There are usually two methods to explicitly express a set. One is to recount every element contained in it, and the other is to describe the elements’ properties using a logical and verifiable expression. For example,

$$S = \{1, 2, 3, \dots, 99\}$$

and

$$S = \{x \mid x \text{ is a positive integer and } 1 \leq x \leq 99\}$$

both describe the same set.

Below we summarize some basic notions and terminologies concerning sets.

- (1) **Elements and sets.** We write  $x \in S$  to denote that  $x$  is an element in a set  $S$ . In this case we also say that  $x$  **belongs to**  $S$ . For example, let  $S = \{1, 2, 3, a, b\}$ , then we have

$$1 \in S, \quad 2 \in S, \quad 3 \in S, \quad a \in S \quad \text{and} \quad b \in S.$$

However, 4 is not an element in  $S$  and we write  $4 \notin S$ .

A set without any element is called an **empty set** and is denoted by  $\emptyset$ .

- (2) **Subsets.** We say that a set  $A$  is a **subset** of another set  $B$  if every element in  $A$  is also an element in  $B$ . In other words,

$$x \in A \implies x \in B.$$

In this case, we write  $A \subseteq B$  and say that  $A$  is **contained in**  $B$ . For example, we have  $\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$ , where

- $\mathbb{N}$  = the set of natural numbers;
- $\mathbb{Z}$  = the set of integers;

- $\mathbb{Q}$  = the set of rational numbers;
- $\mathbb{R}$  = the set of real numbers;
- $\mathbb{C}$  = the set of complex numbers.

Also if

$$A = \{1, 3, 5, 7\} \quad \text{and} \quad B = \{1, 2, 3, 4, 5, 6, 7\},$$

then we have the relations  $A \subseteq A$ ,  $B \subseteq B$  and  $A \subseteq B$ . Note that  $B \not\subseteq A$ . Here we mean that  $B$  is not a subset of  $A$ . In other words, there is an element  $x$  in  $B$  which is not in  $A$ .

- (3) **The equality of sets.** Two sets  $A$  and  $B$  are **equal** if they contain the same elements. To show that  $A = B$  is equivalent to showing both

$$A \subseteq B \quad \text{and} \quad B \subseteq A.$$

If  $A \subseteq B$  but  $A \neq B$ , we will write that  $A \subsetneq B$  and say that  $A$  is a **proper** subset of  $B$ .

**Example 1.1.1.** Let

$$A = \{2a + 3b \mid a, b \in \mathbb{Z}\}.$$

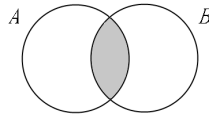
Prove that  $A = \mathbb{Z}$ , the set of integers.

*Proof.* Obviously we have  $A \subseteq \mathbb{Z}$  since  $2a + 3b$  is an integer when  $a$  and  $b$  are integers. It suffices to show that  $\mathbb{Z} \subseteq A$ . For each integer  $n$  in  $\mathbb{Z}$ , we have  $n = 2(-n) + 3n \in A$ . This shows that  $\mathbb{Z} \subseteq A$ . We make the conclusion that  $A = \mathbb{Z}$ . □

Next we introduce three important operations among sets. In the following discussion, let  $A$ ,  $B$  and  $C$  be subsets of a set  $S$ .

- (1) The **intersection** of  $A$  and  $B$  is defined as

$$A \cap B = \{x \in S \mid x \in A \text{ and } x \in B\}.$$

The intersection  $A \cap B$ 

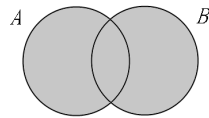
For example, if  $A = \{a, b, c, d\}$  and  $B = \{b, c, e, f\}$ , then  $A \cap B = \{b, c\}$ . Note that  $A \cap B$  contains elements from both  $A$  and  $B$ , and we have

$$(A \cap B) \subseteq A \quad \text{and} \quad (A \cap B) \subseteq B.$$

If  $A$  and  $B$  have no common elements, then  $A \cap B = \emptyset$ . In this case, we say  $A$  and  $B$  are **disjoint**.

- (2) The **union** of  $A$  and  $B$  is defined as

$$A \cup B = \{x \in S \mid x \in A \text{ or } x \in B\}.$$

The union  $A \cup B$ 

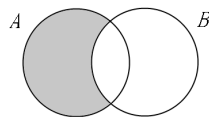
For example, if  $A = \{1, 3, 4\}$  and  $B = \{2, 4, 5, 6\}$ , then  $A \cup B = \{1, 2, 3, 4, 5, 6\}$ . Note that  $A \cup B$  contains elements from either  $A$  or  $B$ , and we have

$$A \subseteq (A \cup B) \quad \text{and} \quad B \subseteq (A \cup B).$$

In case when the two sets  $A$  and  $B$  are disjoint, we also call the union  $A \cup B$  the **disjoint union** of  $A$  and  $B$ , and we denote it by  $A \dot{\cup} B$ .

- (3) The **difference** of  $A$  and  $B$  is defined as

$$A \setminus B = \{x \in S \mid x \in A \text{ and } x \notin B\}.$$

The difference  $A \setminus B$

For example, if  $A = \{-2, -1, 3, 4\}$  and  $B = \{-1, 4, 5\}$ , then  $A \setminus B = \{-2, 3\}$ , and  $B \setminus A = \{5\}$ . Note that

$$A \setminus B \subseteq A \quad \text{and} \quad (A \setminus B) \cap B = \emptyset.$$

Obviously, the operation union (or intersection, respectively) can be generalized naturally to be performed on three or even more sets. A set of sets is often called a **class** or a **family** of sets. A family of sets is often indexed by another set  $\Lambda$  such as  $\mathbb{N}$  or  $\mathbb{Z}$ :

$$(1.1.1) \quad \mathcal{F} = \{A_i \mid i \in \Lambda\} = \{A_i\}_{i \in \Lambda}.$$

We call  $\Lambda$  the **index set** of the family  $\mathcal{F}$ .

Let  $S$  be a set. We may extend the definitions of the union and intersection of sets to a (possibly infinite) family  $\mathcal{F}$  of subsets of  $S$  as

$$\begin{aligned} \bigcup \mathcal{F} &= \{x \in S \mid x \in A \text{ for some } A \in \mathcal{F}\}; \\ \bigcap \mathcal{F} &= \{x \in S \mid x \in A \text{ for all } A \in \mathcal{F}\}. \end{aligned}$$

For the family in (1.1.1), it is customary to write

$$\bigcup \mathcal{F} = \bigcup_{i \in \Lambda} A_i \quad \text{and} \quad \bigcap \mathcal{F} = \bigcap_{i \in \Lambda} A_i.$$

### Exercises 1.1

1. Suppose that the two sets  $A$  and  $B$  satisfy

$$A \setminus B = \{-2, 1, 3\}, \quad B \setminus A = \{5, 6\} \quad \text{and} \quad A \cap B = \{0, 7\}.$$

Find  $A$ ,  $B$  and  $A \cup B$ .

2. Prove or disprove the following statements:

- (a)  $A \cup B = A \cup C \implies B = C$ ;  
 (b)  $A \cap B = A \cap C \implies B = C$ ;  
 (c)  $A \subseteq B, B \subseteq C \implies A \subseteq C$ ;

$$(d) A \subseteq B \implies (A \cup C) \subseteq (B \cup C) \text{ for any set } C.$$

3. Let  $A$ ,  $B$  and  $C$  be subsets of a set  $S$ . Prove the following properties on union and intersection:

$$(a) A \cup \emptyset = A \text{ and } A \cup S = S;$$

$$(b) A \cap \emptyset = \emptyset \text{ and } A \cap S = A;$$

$$(c) \text{Associativity: } (A \cup B) \cup C = A \cup (B \cup C) \text{ and } (A \cap B) \cap C = A \cap (B \cap C).$$

4. Let  $A$  be a subset and let  $\{S_i\}_{i \in \Lambda}$  be a (finite or infinite) family of subsets of a larger set  $S$ . Show that the following statements are true.

$$(a) \text{Distributivity: } A \cup (\bigcap_{i \in \Lambda} S_i) = \bigcap_{i \in \Lambda} (A \cup S_i) \text{ and } A \cap (\bigcup_{i \in \Lambda} S_i) = \bigcup_{i \in \Lambda} (A \cap S_i).$$

$$(b) \text{De Morgan laws: } A \setminus (\bigcup_{i \in \Lambda} S_i) = \bigcap_{i \in \Lambda} (A \setminus S_i) \text{ and } A \setminus (\bigcap_{i \in \Lambda} S_i) = \bigcup_{i \in \Lambda} (A \setminus S_i).$$

5. Define  $2^S$  to be the set of all subsets of  $S$ , called the **power set** of  $S$ . For two sets  $A$  and  $B$  in  $2^S$ , we define the **symmetric difference** or the **Boolean sum** of  $A$  and  $B$  to be

$$A + B = (A \setminus B) \cup (B \setminus A).$$

Prove the following assertions:

$$(a) A + (B + C) = (A + B) + C;$$

$$(b) A + \emptyset = \emptyset + A = A;$$

$$(c) A + A = \emptyset.$$

6. Let  $A = \{4m + 6n \in \mathbb{Z} \mid m, n \in \mathbb{Z}\}$  and  $B = \{6m + 8n \in \mathbb{Z} \mid m, n \in \mathbb{Z}\}$ . Show that  $A = B$ .

7. The **Cartesian product** of two sets  $A$  and  $B$  is defined as

$$A \times B = \{(a, b) \mid a \in A, b \in B\}.$$

Show that the following statements are true:

$$(a) A \times (B \cup C) = (A \times B) \cup (A \times C);$$

$$(b) (A \setminus B) \times C = (A \times C) \setminus (B \times C).$$

## 1.2 Functions

Let  $A$  and  $B$  be sets. A **function**  $f: A \rightarrow B$  consists of three parts:

- (i) the **domain**  $A$ ,
- (ii) the **codomain**  $B$ , and
- (iii) a rule assigning to each element  $x \in A$  a unique element  $f(x) \in B$ .

A function is also called a **map** or a **mapping**. Note that even when two functions appear to operate under the same rule, they are not considered to be equal if they do not have the same domain or codomain.

If  $f(a) = b$ ,  $b$  is called the **image** of  $a$  under  $f$  and  $a$  is called a **preimage** of  $b$  under  $f$ . In mathematics, when we use the word “a”, it means “at least one”, and when we use the word “the”, it means the unique one. Each element in the domain of a function  $f$  has one and only one image under  $f$ , while an element in the codomain of  $f$  may have no or one or more than one preimages. The **image** of  $f$  is defined to be

$$f(A) = \{ f(x) \in B \mid x \in A \} \subseteq B.$$

Suppose that  $f: A \rightarrow B$  and  $g: B \rightarrow C$  are two functions, the composition of  $f$  and  $g$  is a function from  $A$  to  $C$  defined by

$$\begin{aligned} g \circ f: A &\longrightarrow C \\ x &\longmapsto g(f(x)). \end{aligned}$$

For example if  $f: \mathbb{R} \rightarrow \mathbb{R}$  and  $g: \mathbb{R} \rightarrow \mathbb{R}$  are given by

$$f(x) = 2x + 1 \quad \text{and} \quad g(x) = x^2,$$

then

$$(g \circ f)(x) = g(2x + 1) = (2x + 1)^2 = 4x^2 + 4x + 1,$$

and similarly,

$$(f \circ g)(x) = f(g(x)) = 2x^2 + 1.$$

From this example we can see that  $g \circ f$  and  $f \circ g$  are not equal in general. However, composition of functions is indeed associative. Suppose further given a function  $h: C \rightarrow D$ . Then for all  $x \in A$ , we have

$$(h \circ (g \circ f))(x) = h((g \circ f)(x)) = h(g(f(x)))$$

and

$$((h \circ g) \circ f)(x) = (h \circ g)(f(x)) = h(g(f(x))).$$

This shows that

$$(1.2.1) \quad h \circ (g \circ f) = (h \circ g) \circ f.$$

A function  $f: A \rightarrow B$  is **one-to-one** or **injective** if it satisfies the condition

$$x_1 \neq x_2 \implies f(x_1) \neq f(x_2)$$

or the equivalent condition

$$f(x_1) = f(x_2) \implies x_1 = x_2.$$

**Proposition 1.2.1.** *The composition of two injective functions is injective.*

*Proof.* Suppose that the functions  $f: A \rightarrow B$  and  $g: B \rightarrow C$  are one-to-one. Let  $(g \circ f)(x_1) = (g \circ f)(x_2)$ . We want to prove that  $x_1 = x_2$ . By definition, we have

$$g(f(x_1)) = g(f(x_2)).$$

As  $g$  is one-to-one, it follows that  $f(x_1) = f(x_2)$ . Again, since  $f$  is also one-to-one, it implies that  $x_1 = x_2$ . Thus,  $g \circ f$  is one-to-one.  $\square$

A function  $f: A \rightarrow B$  is **onto** or **surjective** if  $f(A) = B$ . This means that for any  $b \in B$ , there exists  $a \in A$  such that  $f(a) = b$ .

**Proposition 1.2.2.** *The composition of two surjective functions is surjective.*

*Proof.* Suppose that  $f: A \rightarrow B$  and  $g: B \rightarrow C$  are onto. Then

$$f(A) = B \quad \text{and} \quad g(B) = C.$$

It follows that

$$g \circ f(A) = g(f(A)) = g(B) = C.$$

This proves that  $g \circ f$  is onto.  $\square$

A function  $f: A \rightarrow B$  is called a **one-to-one correspondence** or a **bijective** function if  $f$  is both one-to-one and onto. Now Propositions 1.2.1 and 1.2.2 together give us the following result.

**Corollary 1.2.3.** *The composition of two bijective functions is bijective.*

There is a special property regarding bijectivity unique to finite sets.

**Proposition 1.2.4.** *Let  $S$  be a finite set and let  $f: S \rightarrow S$  be a function.*

- (a) *If  $f$  is onto then  $f$  is one-to-one and hence bijective.*
- (b) *If  $f$  is one-to-one then  $f$  is onto and hence bijective.*

This proposition is basically a restatement of

**Pigeonhole Principle.** *Let  $m > n$  be two positive integers. If one is to put  $m$  pigeons into  $n$  pigeonholes, then there is at least one hole containing two or more pigeons. In other words, let  $A$  be a set of  $m$  elements and  $B$  be a set of  $n$  elements. Then there are no injective functions from  $A$  to  $B$ .*

We leave proving Proposition 1.2.4 as an exercise.

At last we give a different classification of bijective maps.

Let  $A$  and  $B$  be sets. We define the **identity function** from  $A$  to  $A$ , denoted  $\mathbf{1}_A$ , to be the function sending  $a \in A$  to  $a$  itself. Let  $f: A \rightarrow B$  be a function. Then for all  $x \in A$ ,

$$\begin{aligned}(f \circ \mathbf{1}_A)(x) &= f(\mathbf{1}_A(x)) = f(x), \\ (\mathbf{1}_B \circ f)(x) &= \mathbf{1}_B(f(x)) = f(x).\end{aligned}$$

It follows that

$$(1.2.2) \quad f \circ \mathbf{1}_A = f = \mathbf{1}_B \circ f.$$

If  $f: A \rightarrow B$  is a function, then we say  $g: B \rightarrow A$  is an **inverse function** of  $f$  if  $g \circ f = \mathbf{1}_A$  and  $f \circ g = \mathbf{1}_B$ . It is an easy exercise to show that the inverse function is unique if it exists. Hence, we can denote the inverse function of  $f$  by  $f^{-1}$ .

**Theorem 1.2.5.** *The function  $f: A \rightarrow B$  is bijective if and only if  $f$  has an inverse function.*

*Proof.* To show the “if” part, let  $g$  be the inverse function of  $f$ . Suppose  $f(a) = f(a')$ . Then  $a = g(f(a)) = g(f(a')) = a'$ . This shows that  $f$  is one-to-one. On the other hand, let  $b \in B$ . Then  $b = f(g(b))$  is in the image of  $f$ . Hence  $f$  is also onto.

To show the “only if” part, assume that  $f$  is bijective. Define the function  $g: B \rightarrow A$  as follows. For each  $b \in B$ , there is exactly one  $a \in A$  such that  $f(a) = b$ . Define  $g(b) = a$ . Then  $g$  is easily seen to be the inverse of  $f$ .  $\square$

Sometimes when one wants to show a function is bijective, it is easier to construct its inverse function than actually show that the function is one-to-one and onto.

### Exercises 1.2

1. Let  $f: A \rightarrow B$  and  $g: B \rightarrow C$  be two functions.
  - (a) If  $g \circ f$  is one-to-one, show that  $f$  is one-to-one.
  - (b) Give an example of  $f$  and  $g$  such that  $g \circ f$  is one-to-one but  $g$  is not.
  - (c) If  $g \circ f$  is onto, show that  $g$  is onto.
  - (d) Give an example of  $f$  and  $g$  such that  $g \circ f$  is onto but  $f$  is not.
2. Show that the inverse of a function is unique if it exists.
3. Suppose that  $f$  and  $g$  are bijective functions from  $S$  into itself satisfying  $g \circ f(x) = x$  for all  $x \in S$ . Show that  $f \circ g(x) = x$  for all  $x \in S$ .
4. Use Pigeonhole Principle to prove Proposition 1.2.4.
5. Suppose given a function  $f: S \rightarrow T$  and let  $A \subseteq S$  and  $B \subseteq T$ . We define the **image** of  $A$  under  $f$  to be

$$\text{Im } f = f(A) = \{ b \in T \mid b = f(a) \text{ for some } a \in A \},$$

and the **preimage** of  $B$  under  $f$  to be

$$f^{-1}(B) = \{a \in S \mid f(a) \in B\}.$$

In particular,  $f^{-1}(\{b\})$  is also written as  $f^{-1}(b)$ . Prove the following assertions:

- (a)  $A \subseteq A' \Rightarrow f(A) \subseteq f(A')$  and  $B \subseteq B' \Rightarrow f^{-1}(B) \subseteq f^{-1}(B')$ .
- (b)  $A \subseteq f^{-1}(f(A))$  and  $f(f^{-1}(B)) \subseteq B$ .
- (c)  $f^{-1}(B \cup B') = f^{-1}(B) \cup f^{-1}(B')$  and  $f^{-1}(B \cap B') = f^{-1}(B) \cap f^{-1}(B')$ .
- (d)  $f(A \cup A') = f(A) \cup f(A')$  and  $f(A \cap A') \subseteq f(A) \cap f(A')$ .

## 1.3 Equivalence Relations and Partitions

A **relation**  $R$  on a set  $A$  is a subset of  $A \times A$ . If  $R$  is a relation, it is customary to write  $aRb$  when  $(a, b) \in R$ .

The notion of “relations” is rather general. For example, let  $A = \{1, 3, 5, 6\}$ . The relation  $<$  on  $A$  is the set

$$\{(1, 3), (1, 5), (1, 6), (3, 5), (3, 6), (5, 6)\}.$$

Of course, the more customary expression for “ $(1, 3) \in <$ ” is “ $1 < 3$ ”. Similarly, the relation  $\leq$  on  $A$  is the set

$$\{(1, 1), (1, 3), (1, 5), (1, 6), (3, 3), (3, 5), (3, 6), (5, 5), (5, 6), (6, 6)\}.$$

For another example, let  $S = \{0, 1\}$ . The relation  $\supseteq$  on  $2^S$  is the set

$$\left\{ (\emptyset, \emptyset), (\{0\}, \emptyset), (\{1\}, \emptyset), (\{0, 1\}, \emptyset), (\{0\}, \{0\}), \right. \\ \left. (\{0, 1\}, \{0\}), (\{1\}, \{1\}), (\{0, 1\}, \{1\}), (\{0, 1\}, \{0, 1\}) \right\}.$$

One can make up all kinds of relations on a set. For example,  $=$ ,  $\leq$ ,  $\geq$ ,  $>$  and  $<$  are relations on real numbers  $\mathbb{R}$ . Even “no relation” is a relation if one takes the relation to be the empty set.

**Definition 1.3.1.** An **equivalence relation**  $E$  on a set  $A$  is a relation on  $A$  such that the following conditions are satisfied for all  $a, b, c \in A$ :

- (i) (reflexivity)  $aEa$ ;
- (ii) (symmetry)  $aEb \implies bEa$ ;
- (iii) (transitivity)  $aEb$  and  $bEc \implies aEc$ .

The equality  $=$  on numbers is an equivalence relation while  $\leq$ ,  $\geq$ ,  $>$  and  $<$  are not equivalence relations. For example, the relation  $\leq$  satisfies reflexivity and transitivity but not symmetry. The statement  $2 \leq 3$  is true but the statement  $3 \leq 2$  is false. In fact, an equivalence relation is a generalization of equality. The symbols  $\sim$ ,  $\approx$ ,  $\equiv$ ,  $\simeq$  or  $\cong$  are often used to denote an equivalence relation.

**Example 1.3.2.** Let  $a, b \in \mathbb{Z}$ . Define  $a \equiv b \Leftrightarrow 2 \mid a + b$ . Then  $\equiv$  is an equivalence relation on  $\mathbb{Z}$ . Let  $a$ ,  $b$  and  $c$  be arbitrary integers. Since  $2 \mid a + a = 2a$ , we have  $a \equiv a$ . If  $a \equiv b$ , then  $2 \mid a + b = b + a$  and we have  $b \equiv a$ . If  $a \equiv b$  and  $b \equiv c$ , then  $2 \mid a + b$  and  $2 \mid b + c$ . This implies that  $2 \mid (a + b) + (b + c) = a + c + 2b$ . It follows that  $2 \mid a + c$  and  $a \equiv c$ . We conclude that  $\equiv$  is an equivalence relation.

**Definition 1.3.3.** Let  $E$  be an equivalence relation on  $S$ . Let  $a \in S$ . Define

$$[a] = \{b \in S \mid bEa\}.$$

The set  $[a]$  is called the **equivalence class** of  $a$  (with respect to  $E$ ) and  $a$  is called a **representative** of this class. We often use  $S/E$  to denote the set of the equivalence classes with respect to  $E$ .

Observe that with respect to  $\equiv$  in Example 1.3.2, there are exactly two equivalence classes in  $\mathbb{Z}$ : the set of even integers and the set of odd integers.

An equivalence relation naturally partitions a set.

**Definition 1.3.4.** A **partition** of a set  $S$  is a collection of *disjoint nonempty* subsets of  $S$  whose union is  $S$ . More precisely, a collection of subsets  $\{A_i\}_{i \in \Lambda}$  of  $S$  is a partition if the following three conditions are satisfied:

- (i)  $A_i \neq \emptyset$  for all  $i \in \Lambda$ ;
- (ii)  $A_i \cap A_j = \emptyset$  for  $i \neq j$  in  $\Lambda$ ;
- (iii)  $S = \bigcup_{i \in \Lambda} A_i$ .

For example, let  $S = \{1, 2, 3, 4, 5, 6\}$ . Then  $\{\{1, 3, 5\}, \{2, 4\}, \{6\}\}$  is a partition of  $S$  while  $\{\{1, 3, 5\}, \{2, 4\}, \{6, 3\}\}$  is not.

If a family of subsets forms a partition of a bigger set  $S$ , every element of  $S$  belongs to exactly one member of this family. If one takes two subsets  $A$  and  $B$  from a partition of  $S$ , then either  $A = B$  or  $A \cap B = \emptyset$ .

**Proposition 1.3.5.** *Let  $E$  be an equivalence relation of  $S$ . Then the equivalence classes with respect to  $E$  form a partition of  $S$ .*

*Proof.* Take any  $a \in S$ . Then  $a \in [a]$ . It follows that  $[a] \neq \emptyset$  and the union of all the equivalence classes is  $S$ . It remains to show that if we take any  $a, b \in S$ , then either  $[a] = [b]$  or  $[a] \cap [b] = \emptyset$ . Suppose  $[a] \cap [b] \neq \emptyset$ . Find  $c \in [a] \cap [b]$ . Then  $cEa$  and  $cEb$ . If  $d \in [a]$ , then  $dEa$ . By symmetry of  $E$ , we have  $aEc$ . By transitivity of  $E$ , we have  $dEb$  and thus  $d \in [b]$ . We have shown that  $[a] \subseteq [b]$ . Similarly, we can show that  $[b] \subseteq [a]$ . Hence  $[a] = [b]$ .  $\square$

Thus we may use equivalence relations to form new sets.

### Exercises 1.3

1. Let  $f: S \rightarrow T$  be a function. Then  $f$  defines a relation  $\sim_f$  on  $S$  by letting

$$a \sim_f b \iff f(a) = f(b), \quad \text{for } a, b \in S.$$

Show that  $\sim_f$  is an equivalence relation.

2. Let  $\mathbb{Z}_+$  be the set of all positive integers. Define a relation  $\equiv$  on  $\mathbb{Z}_+$  by letting  $a \equiv b$  if and only if  $a + b$  is even. Is  $\equiv$  an equivalence relation? If yes, describe all the equivalence classes of  $\equiv$ .
3. Define a relation on  $\mathbb{Z}$  by letting  $aRb$  if and only if  $ab \geq 0$ . Is  $R$  an equivalence relation on  $\mathbb{Z}$ ? If yes, describe its equivalence classes.
4. Let  $\pi$  be a partition on  $S$ . Define a relation  $\sim_\pi$  on  $S$  by letting  $a \sim_\pi b$  if and only if  $a$  and  $b$  belong to the same set in  $\pi$ . Show that  $\sim_\pi$  is an equivalence relation of  $S$ .

## 1.4 A Note on Natural Numbers

Most students probably believe that they are extremely familiar with the set of natural numbers  $\mathbb{N}$ . However, it is quite tedious to go through the formal construction of the natural numbers and establish the subsequent facts and properties regarding them. And many students starting the study of abstract algebra will be puzzled why on earth would anyone need to go through all this trouble. Hence, we will skip this part of work, and hopefully one day the reader would acquire enough mathematical maturity to feel the need to fill the gap herself or himself.

The interesting thing is that even mathematicians have different opinions regarding the notation  $\mathbb{N}$ . Some take it as the set of all positive integers  $\{1, 2, 3, \dots\}$ , while some take it as the set  $\{0, 1, 2, 3, \dots\}$ . To set theorists, it is more natural to use the latter. However, it does not really matter in most situations, as long as one knows where one stands. In this book, we will assume

$$\mathbb{N} = \{1, 2, 3, 4, 5, \dots\}$$

is the set of positive integers. Hence, the notations  $\mathbb{N}$  and  $\mathbb{Z}_+$  stand for the same set.

In this section, we would like to review some of the most important properties of the natural numbers without giving the proofs. Interested readers are encouraged to read books on set theory for more details. These properties will be used in many proofs in this book. If not for the discussions in this section, many students would probably never realize that they are using them.

**Theorem 1.4.1** (The Well-Ordering Principle). *Every nonempty subset of  $\mathbb{N}$  contains a least number.*

**Theorem 1.4.2** (The First Principle of Mathematical Induction). *Let  $S$  be a subset of  $\mathbb{N}$  which contains 1. Suppose  $S$  is such that  $n \in S$  implies  $n + 1 \in S$ . Then  $S = \mathbb{N}$ .*

We present here another commonly used form of mathematical induction.

**Theorem 1.4.3** (The Second Principle of Mathematical Induction). *Let*

$S$  be a subset of  $\mathbb{N}$  which contains 1. Suppose  $S$  is such that  $x \in S$  for all  $1 \leq x \leq n$  implies  $n + 1 \in S$ . Then  $S = \mathbb{N}$ .

We will assume that readers are familiar with addition and multiplication as well as the order in  $\mathbb{N}$ . Finally, we add a few words on *cardinality*.

**Definition 1.4.4.** We say that two sets  $A, B$  have the same **cardinality**, if there is a bijective map from  $A$  onto  $B$ . We use  $|A|$  to denote the cardinality of  $A$ . When  $A$  is a finite set,  $|A|$  is simply the number of the elements in  $A$ .

It is not always easy to construct a bijective map between two sets of the same cardinality. Thus we will need to know more.

**Definition 1.4.5.** If there is an injective map from  $A$  to  $B$ , then we say  $B$  **dominates**  $A$ , and we will write  $A \preceq B$ .

**Theorem 1.4.6** (Schröder-Bernstein Theorem). *If  $A \preceq B$  and  $B \preceq A$  then  $|A| = |B|$ .*

Hence, to show two sets  $A$  and  $B$  are of the same cardinality, one can do so by constructing an injective map from  $A$  to  $B$  and an injective map from  $B$  to  $A$ .

**Definition 1.4.7.** We say that an infinite set  $S$  is **countable** if  $|S| = |\mathbb{N}|$ , that is, there is a bijective map from  $\mathbb{N}$  to  $S$ . Otherwise, we say  $S$  is **uncountable**.

It is well-known that the set of rational numbers is countable, while the set of real numbers is uncountable.

---

### Exercises 1.4

1. Let  $S$  be a set which satisfies the well-ordering principle and let  $A$  be a subset of  $S$ . Show that  $A$  also satisfies the well-ordering principle.
2. (Long division in  $\mathbb{N} \cup \{0\}$ ) Show that for any  $a, b \in \mathbb{N} \cup \{0\}$  where  $b \neq 0$ , there exist  $q \in \mathbb{N} \cup \{0\}$  and  $0 \leq r < b$  such that  $a = bq + r$ . (Hint: Use the Well-Ordering Principle.)

3. Let  $S = \{5m + 8n \in \mathbb{N} \mid m, n \in \mathbb{N}\}$ . Find the largest natural number which is not contained in  $S$ .
4. Let  $\{A_i\}_{i \in \mathbb{N}}$  be a family of countable subsets of a set  $S$ . Show that  $\bigcup_{i \in \mathbb{N}} A_i$  is countable.

### Review Exercises for Chapter 1

1. Let  $f, g$  and  $h$  be three functions from a set into itself.
  - (a) Suppose that  $f$  is one-to-one and  $f \circ g = f \circ h$ . Show that  $g = h$ .
  - (b) Suppose that  $f$  is onto and  $g \circ f = h \circ f$ . Show that  $g = h$ .
2. Suppose that  $f$  and  $g$  are both functions from  $S$  into itself satisfying  $g \circ f(x) = x$  for all  $x \in S$ . Show that  $f \circ g(x) = x$  for all  $x \in S$  if  $S$  is finite. Is this assertion true in general?
3. Let  $f$  be a bijective function from  $S = \{a, b, c\}$  onto itself. Prove that

$$f^6(x) = x$$

for all  $x \in S$ . Here  $f^n = f \circ f \circ \cdots \circ f$  ( $n$  times).

4. Let  $z = a + bi$  be a complex number where  $a, b \in \mathbb{R}$ . Remember that the **absolute value** of  $z$  is  $|z| = \sqrt{a^2 + b^2}$ . Define a relation on  $\mathbb{C}$  by letting  $z \sim w$  if  $|z| = |w|$ . Show that  $\sim$  is an equivalence relation.
5. Let  $S$  be the set of all infinite sequences of  $\mathbb{N}$ , that is,

$$S = \{(a_i)_{i=1}^{\infty} \mid a_i \in \mathbb{N}\}.$$

Is  $S$  countable?