

# Discrete Mathematics

## Contents

<b>1</b>	<b>Elementary Set Theory</b>	<b>2</b>
1.1	Relations Among Sets	3
1.2	Basic Operations of Sets	4
1.3	Index Sets	5
1.4	Some More Set Operations	6
1.5	Relations	8
	1.5.1 Equivalence Relations and Partitions	9
	1.5.2 Partial Order Relations	11
1.6	Functions	12
1.7	Function Composition	15
1.8	Isomorphisms of Sets	16
1.9	Cardinality of Sets	18

# 1 Elementary Set Theory

A **set** is (informally) an unordered collection of **elements**. More formally, any set is defined by the **membership relation**  $\in$  (read “belongs to”, “is an element of”, “is a member of”, or “is in”), where  $s \in S$  if and only if  $s$  is an element of the set  $S$ . If  $x$  is not a member of  $S$ , then we write  $x \notin S$ . We may define a set either as a list of all its members enclosed by curly braces –  $\{$  and  $\}$  – or in the form  $Y = \{x \in X \mid P(x)\}$ , where  $X$  is a previously defined set, and  $P(x)$  is a **predicate** (a function with a true/false value depending on the value of  $x$ ) – then  $Y$  is the set consisting of all members of  $X$  that satisfy the predicate  $P(x)$  (i.e., those  $x \in X$  for which  $P(x)$  is true). The latter form of defining a set is called the **set-builder** notation. For example

$$S = \{1, 'a', 2.5, +, 9, -3\}$$

defines  $S$  to be the set consisting of the six elements 1, ‘a’, 2.5, +, 9, and –3, and

$$T = \{s \in S \mid s \text{ is a number}\}$$

defines  $T$  to be the set consisting of the four elements 1, 2.5, 9, and –3. The symbol  $\mid$  is read as “such that” (and can be replaced by a  $:$  as well).

The **universal set** (usually denoted by  $U$ ) is the set consisting of all elements currently under consideration. We may write  $\{x \mid P(x)\}$  to mean  $\{x \in U \mid P(x)\}$ .

The **empty set** (or **null set**) is the set  $\emptyset$  that has no elements. That is, for every element  $a$  of the universal set,  $a \notin \emptyset$ .

*Note.* A variant of the set-builder notation replaces the element on the left side of  $\mid$  by an expression involving one or more elements, with the specifications of memberships of these elements appearing on the right side of  $\mid$ , along with other predicates, if any. For example

$$S = \{2n \mid n \in \mathbb{Z}\}$$

defines  $S$  to be the set of all elements obtained by doubling an integer – in other words,  $S$  is the set of even integers.

## 1.1 Relations Among Sets

A set  $A$  is a **subset** of a set  $B$ , denoted by  $A \subseteq B$ , if every element of  $A$  is an element of  $B$ . That is, for any element  $a$  (of the universal set),  $a \in A \implies a \in B$ . Then  $B$  is a **superset** of  $A$ , denoted by  $B \supseteq A$ . We may also say that  $B$  **contains**  $A$ , or that  $A$  is contained in  $B$ .

Two sets  $A$  and  $B$  are **equal**, written  $A = B$ , if each contains the other – i.e.,  $A \subseteq B$  and  $B \subseteq A$ . This is equivalent to the statement that  $A$  and  $B$  have exactly the same elements. Otherwise,  $A$  is not equal to  $B$  (written  $A \neq B$ ).  $A$  is a **proper subset** of  $A$  (or is properly contained in  $B$ ) if  $A \subseteq B$  and  $A \neq B$ . Then we write  $A \subsetneq B$ . Similarly,  $B$  is a proper superset of  $A$ , denoted by  $B \supsetneq A$ , if  $B \supseteq A$  and  $B \neq A$ .

*Note.* It is also common to use  $\subset$  and  $\supset$  instead of  $\subseteq$  and  $\supseteq$ , respectively. They are usually *not* alternatives to  $\subsetneq$  and  $\supsetneq$ , except when explicitly stated to be so.

The set of all subsets of a set  $A$  is called the **power set** of  $A$ , is denoted by  $2^A$  or  $\mathcal{P}(A)$ . That is,

$$2^A = \{ S \mid S \subseteq A \}.$$

**Exercise 1.1.** Let  $A$ ,  $B$ , and  $C$  be arbitrary sets.

1. Show that  $A \subseteq A$ .
2. Show that if  $A \subseteq B$  and  $B \subseteq C$ , then  $A \subseteq C$ .
3. Show that the  $\supseteq$  also satisfies these properties.
4. Show that  $\emptyset \subseteq A$ .
5. Show that if  $A$  is a set consisting of  $n$  elements, for some non-negative integer  $n$ , then  $2^A$  contains  $2^n$  elements.

## 1.2 Basic Operations of Sets

The **union** of two sets  $A$  and  $B$  is the set  $A \cup B$  consisting of all elements that belong to  $A$  or  $B$ :

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

The **intersection** of two sets  $A$  and  $B$  is the set  $A \cap B$  consisting of all elements that belong to  $A$  and  $B$ :

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

The **complement** of a set  $A$  is the set  $\overline{A}$  of all elements (of the universal set) that do not belong to  $A$ :

$$\overline{A} = \{ x \mid x \notin A \}.$$

We may also denote the complement of  $A$  by  $A'$ ,  $A^c$ , or  $U \setminus A$ .

**Exercise 1.2.** Let  $A$ ,  $B$ , and  $C$  be arbitrary sets.

1. Show that  $A \cap B \subseteq A \subseteq A \cup B$ .
2. Show that  $\cup$  is
  - (i) **associative**:  $(A \cup B) \cup C = A \cup (B \cup C)$ ,
  - (ii) **commutative**:  $A \cup B = B \cup A$ , and
  - (iii) **idempotent**:  $A \cup A = A$ .
3. Prove that  $\cap$  is also associative, commutative, and idempotent.
4. Prove that  $\cup$  **distributes** over  $\cap$  and vice-versa:

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C).$$

5. Prove that  $\cup$  and  $\cap$  satisfy the law of **absorption**:

$$A \cup (A \cap B) = A \cap (A \cup B) = A.$$

6. Show that the following are equivalent:

- (a)  $A \subseteq B$ .
- (b)  $A \cup B = B$ .
- (c)  $A \cap B = A$ .

7. Prove that  $\cup$ ,  $\cap$  and  $-$  satisfy De Morgan's laws. That is:

$$\overline{(A \cup B)} = \overline{A} \cap \overline{B}$$

$$\overline{(A \cap B)} = \overline{A} \cup \overline{B}.$$

8. Show that  $A \cap \overline{A} = \emptyset$ .

Two sets  $A$  and  $B$  are **disjoint** if their intersection is empty – i.e.,  $A \cap B = \emptyset$ . Note that  $A$  and  $\overline{A}$  are always disjoint. Also note that  $\emptyset$  is disjoint with all sets, and is the unique set that is disjoint with itself.

Since  $\cup$  and  $\cap$  are associative, expressions of the form  $A_1 \cup A_2 \cup \dots \cup A_n$  and  $A_1 \cap A_2 \cap \dots \cap A_n$  are well-defined and unambiguous. These are called the  **$n$ -ary** (or finite) union and intersection, and denote them as  $\bigcup_{i=1}^n A_i$  and  $\bigcap_{i=1}^n A_i$ , respectively. But it is possible to define unions and intersections of collections of sets even more generally. For this, we will discuss the concept of an indexing set.

### 1.3 Index Sets

A set  $I$  is an **index set** (or **indexing set**) of a set  $S$  if we can write  $S$  as

$$S = \{s_i \mid i \in I\}.$$

That is, each element of  $s_i \in S$  corresponds to a unique element  $i \in I$ . Then  $S$  is **indexed by**  $I$ , and it is common to write  $S = \{s_i\}_{i \in I}$ .

Let  $\mathcal{A} = \{A_i\}_{i \in I}$  be a collection of sets (for some index set  $I$ ). Thus, for each  $i \in I$ ,  $A_i$  itself is a set in the collection  $\mathcal{A}$ . Then we can define

the union and intersection of the sets in  $\mathcal{A}$ , as given below.

$$\bigcup_{i \in I} A_i = \{ a \mid a \in A_i, \exists i \in I \}$$

$$\bigcap_{i \in I} A_i = \{ a \mid a \in A_i, \forall i \in I \}$$

We refer to these operations as **arbitrary** unions and intersections. In the particular case where  $I$  is a set containing finitely many elements, these reduce to the finite union and intersection defined earlier.

## 1.4 Some More Set Operations

We say that  $(a, b)$  (or  $\langle a, b \rangle$ ) is an **ordered pair** where the first element is  $a$  and the second element is  $b$ . Formally, we may define the ordered pair in terms of sets as  $(a, b) = \{a, \{a, b\}\}$ . Note that this is only one possible “encoding” of the concept of an ordered pair, and in practice, we do not think of  $(a, b)$  as the (unordered) set  $\{a, \{a, b\}\}$ .

The **Cartesian product** of two sets  $A$  and  $B$ , denoted by  $A \times B$ , is the set of all ordered pairs of elements with the first element from  $A$  and the second from  $B$ . That is,

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

The Cartesian product of  $A$  with itself is often written as  $A^2$ . Similarly, the Cartesian product  $A \times \cdots \times A$  with  $n$  terms (defined as an iterated Cartesian product of two sets at a time) is denoted by  $A^n$ .

The **disjoint union** (or **coproduct**) of two sets  $A$  and  $B$ , denoted by  $A \sqcup B$ , consists of all the ordered pairs of the form  $(x, i)$  where  $i = 1$  when  $x \in A$  and  $i = 2$  when  $x \in B$ . That is,

$$A \sqcup B = \{ (a, 1) \mid a \in A \} \cup \{ (b, 2) \mid b \in B \}.$$

The disjoint union is also denoted by  $A \coprod B$ ,  $A \cup B$ , or  $A \uplus B$ .

*Note.* The second element in each ordered pair (i.e., 1 or 2) only serves to distinguish the elements that are originally from  $A$ , from those that are originally from  $B$ . Thus, for example, if  $x$  is an element common to both  $A$  and  $B$ , then  $A \sqcup B$  contains two “copies” of  $x$ , namely  $(x, 1)$  and  $(x, 2)$ . When  $A$  and  $B$  are disjoint,  $A \sqcup B$  is equivalent to  $A \cup B$  (where the meaning of “equivalent” will be formalised later).

We can also define Cartesian products and disjoint unions of a collection of sets. Let  $\mathcal{A} = \{A_i\}_{i \in I}$  be a collection of sets indexed by  $I$ . Then the Cartesian product of the collection  $\mathcal{A}$  is

$$\prod_{i \in I} = \{ (a_i)_{i \in I} \mid a_i \in A_i, i \in I \}$$

where  $(a_i)_{i \in I}$  is a sequence of elements indexed by  $I$ , with  $a_i \in A_i$  for each  $i \in I$ . The disjoint union of the collection  $\mathcal{A}$  is

$$\bigsqcup_{i \in I} = \bigcup_{i \in I} \{ (a_i, i) \mid a_i \in A_i, i \in I \} = \bigcup_{i \in I} A_i \times \{i\}.$$

*Note.* We will formally define sequences later, in Section 1.6.

The **difference** of two sets  $A$  and  $B$  is the set  $A \setminus B$  consisting all elements of  $A$  that are not elements of  $B$ . That is,

$$A \setminus B = \{a \in A \mid a \notin B\}.$$

The difference of  $A$  and  $B$  is also denoted by  $A - B$ . Note that  $A \setminus B = A \setminus (A \cap B)$ .

The **symmetric difference** of two sets  $A$  and  $B$  is the set  $A \triangle B$  consisting of all the elements that are present in exactly one of  $A$  and  $B$ . That is,

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

The symmetric difference of  $A$  and  $B$  is also denoted as  $A \ominus B$ .

**Exercise 1.3.** Let  $A$  and  $B$  be arbitrary sets.

1. Show that  $(A \cup B) \setminus B = A \setminus B$ .
2. Show that  $A \triangle B = (A \cup B) \setminus (A \cap B)$ .
3. Show that  $(2^A, \triangle)$  is an Abelian group. That is:
  - (i)  $\triangle$  is associative.
  - (ii)  $\triangle$  is commutative.
  - (iii)  $\exists E \in 2^A, \forall S \in 2^A, S \triangle E = S$ .
  - (iv)  $\forall S \in 2^A, \exists T \in 2^A, S \triangle T = E$ .

What is the order of any non-identity element of this group?

## 1.5 Relations

A **relation**  $R$  from a set  $A$  to a set  $B$ , denoted  $R: A \rightarrow B$ , is a subset of  $A \times B$ , i.e.,  $R \subseteq A \times B$ . If  $(a, b) \in R$ , then we write  $aRb$ , and if  $(a, b) \notin R$ , then we write  $a \not R b$ . The set  $A$  is the **domain** and  $B$  the **codomain** of  $R$ . Note that  $\emptyset$  is also a relation, called the **empty** or **void** relation, from  $A$  to  $B$ .

*Note.* A relation from a set  $A$  to a set  $B$  is a **binary relation**. More generally, if  $A_1, \dots, A_n$  are  $n$  sets, then a subset of  $A_1 \times \dots \times A_n$  is an  **$n$ -ary relation**.

A relation  $R: A \rightarrow B$  is said to be

1. **left-total** if for each  $a \in A$ ,  $aRb$  for some  $b \in B$ .
2. **right-total** if for each  $b \in B$ ,  $aRb$  for some  $a \in A$ .
3. **left-unique** if for each  $b \in B$ , if  $a, a' \in A$  are such that  $aRb$  and  $a'Rb$ , then  $a = a'$ .
4. **right-unique** if for each  $a \in A$ , if  $b, b' \in B$  are such that  $aRb$  and  $aRb'$ , then  $b = b'$ .

A relation from  $A$  to itself is said to be a **relation on** (or **over**)  $A$  (also called a **homogeneous** relation on  $A$ ). Such relations can have a number of properties. In the following, let  $\sim$  be a relation on a set  $A$ .



1. **Reflexivity**: For all  $a \in A$ ,  $a \sim a$ .
2. **Symmetry**: For all  $a, b \in A$ , if  $a \sim b$ , then  $b \sim a$ .
3. **Anti-symmetry**: For all  $a, b \in A$ , if  $a \sim b$  and  $b \sim a$ , then  $a = b$ .
4. **Transitivity**: For all  $a, b, c \in A$ , if  $a \sim b$  and  $b \sim c$ , then  $a \sim c$ .
5. **Irreflexivity**: For all  $a \in A$ ,  $a \not\sim a$ .
6. **Asymmetry**: For all  $a \in A$ , if  $a \sim b$ , then  $b \not\sim a$ .

**Example 1.1.** The following list gives examples of familiar relations satisfying one or more of the above properties:

1. The relations  $=$  (on any set of elements where equality is defined),  $\leq$  and  $\geq$  (on any set of real numbers),  $|$  (*divides*, see Exercise 1.7),  $\subseteq$  and  $\supseteq$  (on any collection of sets),  $\cong$  and  $\sim$  (on any set of triangles), and  $\parallel$  (on any set of lines) are reflexive.
2. The relations  $=$ ,  $\neq$ ,  $\cong$ ,  $\sim$ ,  $\parallel$ ,  $\perp$  are symmetric.
3. The relations  $|$  (on any set of non-negative integers),  $\leq$ ,  $\geq$ ,  $\subseteq$ ,  $\supseteq$  are anti-symmetric.
4. The relations  $=$ ,  $\leq$ ,  $\geq$ ,  $<$ ,  $>$ ,  $|$ ,  $\subseteq$ ,  $\supseteq$ ,  $\subsetneq$ ,  $\supsetneq$ ,  $\cong$ ,  $\sim$ ,  $\parallel$  are transitive.
5. The relations  $\neq$  and  $\perp$  are irreflexive.
6. The relations  $<$ ,  $>$ ,  $\subsetneq$ ,  $\supsetneq$  are asymmetric.

#### Exercise 1.4.

1. Let  $\sim$  be the relation of the set  $A = \{a, b\}$  defined by  $a \sim a$ ,  $a \sim b$ . Is  $\sim$  transitive?
2. Show that every asymmetric relation is irreflexive.
3. Prove or disprove: Any transitive, irreflexive relation is asymmetric.
4. Prove or disprove: Any symmetric, transitive relation is reflexive.

### 1.5.1 Equivalence Relations and Partitions

A reflexive, symmetric, and transitive relation is called an **equivalence** relation. For example,  $=$ ,  $\cong$ ,  $\sim$ , and  $\parallel$  are equivalence relations. If  $\sim$  is an

equivalence relation on a set  $A$ , and  $a \in A$ , then the **equivalence class** of  $a$ , denoted as  $[a]$  or  $\bar{a}$  is the set of all elements of  $A$  that  $a$  is related to by  $\sim$ . That is,

$$[a] = \{ b \in A \mid a \sim b \}.$$

**Example 1.2.** Let  $A = \{1, 2, 3, 4, 5\}$ , and define a relation  $\sim$  on  $A$  as follows: For any  $a, b \in A$ ,  $a \sim b$  if and only if  $a - b$  is even. Then, for example, the equivalence class of 1 is  $[1] = \{1, 3, 5\}$ , and the equivalence class of 2 is  $[2] = \{2, 4, 6\}$ . Note that  $[1] = [3] = [5]$  and  $[2] = [4] = [6]$ . Also observe that  $[1]$  and  $[2]$  are disjoint, and  $[1] \cup [2] = A$ .

An equivalence relation on a set is essentially the same as a partition of the set, as you will show in ?? 1.5?? 1.6. A **partition of a set**  $S$  is a collection of non-empty and pairwise disjoint subsets of  $S$  whose union is equal to  $S$ . That is, a partition of  $S$  is a collection  $\{P_i\}_{i \in I}$  of sets  $P_i \subseteq S$ ,  $i \in I$ , such that

1.  $P_i \neq \emptyset$ , for each  $i \in I$ ,
2.  $P_i \cap P_j = \emptyset$ , for all  $i, j \in I$ ,  $i \neq j$ , and
3.  $\bigcup_{i \in I} P_i = S$ .

The subsets  $P_i$ ,  $i \in I$ , are called the **parts** of the partition  $P$ .

**Example 1.3.** Let  $S = \{1, 2, 3, 4, 5\}$ . Then  $P = \{\{1, 3, 5\}, \{2, 4, 6\}\}$  and  $Q = \{\{1, 4\}, \{2\}, \{3, 5\}\}$  are two different partitions of  $S$ .

**Exercise 1.5.** Let  $\sim$  be an equivalence relation on a set  $A$ . Show that the following hold:

1. For all  $a \in A$ ,  $a \in [a]$ , and hence, each equivalence class is non-empty and  $A = \bigcup_{a \in A} [a]$ .
2. For all  $a, b \in A$ , if  $a \neq b$ , then  $[a] \cap [b] = \emptyset$  (i.e., any two equivalence classes are either disjoint or identical).
3. The set of all equivalence classes of  $\sim$  is a partition of  $A$ .

**Exercise 1.6.** Let  $P = \{P_i\}_{i \in I}$  be a partition of a set  $A$ . Define a relation  $\sim$  on  $A$  as follows: For any  $a, b \in A$ ,  $a \sim b$  if and only if  $a$  and  $b$  belong to the same part of the partition  $P$  (i.e.,  $a, b \in P_i$ ,  $\exists i \in I$ ). Show that the following hold:

1. The relation  $\sim$  is an equivalence relation on  $A$ .
2. The equivalence classes of  $\sim$  are exactly the parts of the partition of  $P$ .

### 1.5.2 Partial Order Relations

A reflexive, anti-symmetric, and transitive relation is called a **partial order** relation (or simply a partial order). For example,  $\leq$  and  $\geq$  on any set of real numbers,  $|$  on any set of non-negative integers, and  $\subseteq$  and  $\supseteq$  on any set of sets are partial order relations. A set  $A$  together with a partial order  $\preceq$  on it forms a **partially ordered set** or **poset**  $(A, \preceq)$ .

*Note.* The term *partial* refers to the fact that two particular elements in a partially ordered set may be **incomparable** – i.e., neither may be related to the other in the partial order. For instance, consider the subsets of  $S = \{x, y, z\}$ , which are partially ordered by the subset relation  $\subseteq$  – i.e., consider the poset  $(2^S, \subseteq)$ . Then  $A = \{x, y\}$  and  $B = \{y, z\}$  are incomparable, as neither is  $A$  a subset of  $B$ , nor is  $B$  a subset of  $A$ . On the other hand,  $A$  and  $C = \{x\}$  are **comparable** (as  $C \subseteq A$ ), and  $A$  and  $S$  itself are also comparable (as  $A \subseteq S$ ). A poset in which every pair of elements is comparable (i.e., in which there are no incomparable pairs of elements) is called a **total order**.

**Exercise 1.7.** Let  $|$  denote the **divides** relation on any set of integers. That is, for any two integers  $m$  and  $n$ , define  $m | n$  if and only if  $n = km$  for some integer  $k$ .

1. Prove that  $(\mathbb{N}, |)$  is a poset. Is  $(\mathbb{N}_0, |)$  also a poset?
2. Is  $(\mathbb{Z}, |)$  a poset?

3. Let  $n \in \mathbb{N}$ , and let  $P$  be the set of all positive divisors of  $n$ . Then show that  $(P, |)$  is a poset. What are all the natural numbers  $n$  such that  $(P, |)$  is a total order?

## 1.6 Functions

A **function** is a left-total, right-unique binary relation. In other words, a function  $f: A \rightarrow B$  is a relation from  $A$  to  $B$  such that each element of  $A$  is related to exactly one element of  $B$  under  $f$ . If  $a \in A$  is related to  $b \in B$  in  $f$ , then we say that  $f$  **maps**  $a$  to  $b$ , and write  $b = f(a)$ , or  $a \mapsto b$ . A function is also called a **mapping**. Recall that  $A$  is the domain of  $f$  and  $B$  the codomain. We may also write  $\text{dom } f$  and  $\text{cod } f$  to denote the domain and codomain of  $f$ , respectively. The **image** of  $f$ , denoted as  $\text{im } f$  or  $f(A)$ , is the set of all elements  $b$  of the codomain such that  $b = f(a)$  for some  $a \in A$ . We can write this in the following two ways:

$$\begin{aligned}\text{im } f &= \{ b \in B \mid b = f(a), \exists a \in A \} \\ \text{im } f &= \{ f(a) \mid a \in A \}.\end{aligned}$$

The **preimage** of any element of the codomain is the set of all elements of the domain that map to it. That is, for  $b \in B$ , the preimage of  $b$ , denoted  $f^{-1}(b)$ , is defined as

$$f^{-1}(b) = \{ a \in A \mid f(a) = b \}.$$

Note that the image of the function is a subset of the codomain, while the preimage of an element is the subset of the domain.

*Note.* Intuitively, we think of a function as a rule that assigns, to each element of the domain, a unique element of the codomain. For instance, it is common in calculus to define a function using a formula – e.g.,  $f: \mathbb{R} \rightarrow \mathbb{R}$ ,  $f(x) = x^2 - 1$ . However, the formula or the expression itself is not the function. The function  $g: \mathbb{Z} \rightarrow \mathbb{Q}$ , defined by the formula

$g(x) = x^2 - 1$ , is different from the previously defined function  $f$ , although they are both defined using the same formula. Moreover, it may not be possible to define a function using any closed-form formula.

A function is **injective** (or **1-1**) if it is left-unique. That is,  $f: A \rightarrow B$  is injective if, for any  $a_1, a_2 \in A$ ,  $f(a_1) = f(a_2)$  implies that  $a_1 = a_2$ . An injective function is also called an **injection**. A **surjective** (or **onto**) function is one in which every element of the codomain has a non-empty preimage. That is,  $f: A \rightarrow B$  is surjective if, for each  $b \in B$ ,  $b = f(a)$  for some  $a \in A$ . Note that  $f$  is surjective if and only if  $\text{im } f = \text{cod } f$ . A surjective function is also called a **surjection**. A function that is both injective and surjective is **bijective**. A bijective function is also called a **bijection** or a **one-to-one correspondence**.

**Example 1.4.** Let  $A = \{1, 2, 3, 4, 5\}$  and  $B = \{a, b, c\}$ .

1. Define a function  $f: A \rightarrow B$ ,  $f(1) = f(2) = a$ ,  $f(3) = b$ ,  $f(4) = f(5) = c$ . Then  $f$  is a surjection ( $a$  has preimage  $\{1, 2\}$ ,  $b$  has preimage  $\{3\}$ , and  $c$  has preimage  $\{4, 5\}$ ). It is clearly not an injection, since, for example,  $f(1) = f(2)$ .
2. Define  $g: B \rightarrow A$ ,  $g(a) = 1$ ,  $g(b) = 5$ ,  $g(c) = 4$ . Then  $g$  is an injection from  $B$  to  $A$ , as  $g(a) \neq g(b)$ ,  $g(c)$  and  $g(b) \neq g(c)$ . The image of  $g$  is  $\text{im } g = \{1, 4, 5\} \neq A = \text{cod } g$ , and hence  $g$  is not a surjection.
3. Define a  $h: B \rightarrow B$ ,  $h(a) = b$ ,  $h(b) = c$ ,  $h(c) = a$ . Note that  $h$  is a bijection from  $B$  to itself.

**Example 1.5.** Define  $f: \mathbb{Z} \rightarrow \mathbb{R}$  as  $f(n) = n$ , for all  $n \in \mathbb{Z}$ . Then  $f$  is an injection, but not a surjection (e.g.,  $1.5 \in \mathbb{R}$  has no preimage under  $f$ ). Define  $g: \mathbb{R} \rightarrow \mathbb{Z}$  as  $g(x) = \lceil x \rceil$ , the ceiling of  $x$  (i.e., the smallest integer greater than or equal to  $x$  – e.g.,  $\lceil 3.2 \rceil = 4$ , and  $\lceil -1.5 \rceil = 0$ ). Then  $g$  is a surjection (for any  $n \in \mathbb{Z}$ ,  $n \in \mathbb{R}$  as well, and  $g(n) = \lceil n \rceil = n$ ), but not an injection (e.g.,  $g(1.8) = g(2) = 2$ ). Similarly, define  $h: \mathbb{R} \rightarrow \mathbb{Z}$  as  $h(x) = \lfloor x \rfloor$ , the floor of  $x$  (i.e., the greatest integer less than or equal to

$x$ ). Then  $h$  is a surjection (but not an injection) from  $\mathbb{R}$  to  $\mathbb{Z}$ , different from  $g$ .

**Example 1.6.** Define  $f: \mathbb{R} \rightarrow (0, 1)$  (the set of all real numbers strictly between 0 and 1) as

$$f(x) = \frac{1}{1 + e^x}.$$

Firstly, note that this is indeed a well-defined function from  $\mathbb{R}$  to  $(0, 1)$ , since  $e^x \geq 0$  for all  $x \in \mathbb{R}$ . Now, if  $f(x) = f(y)$ , then observe that  $e^x = e^y$ , or  $e^{x-y} = 1$ , which implies that  $x = y$ . Hence,  $f$  is injective. Next, let  $y$  be any element of the codomain,  $(0, 1)$ . Then observe that  $\frac{1}{y} > 1$ , and hence  $\frac{1}{y} - 1$  is a positive real number. Take  $x = \log\left(\frac{1}{y} - 1\right)$ , so that  $\frac{1}{1+e^x} = y$ , i.e.,  $f(x) = y$ . Thus, for every  $y \in (0, 1)$ , there exists  $x \in \mathbb{R}$  such that  $f(x) = y$ , which shows that  $f$  is surjective. Therefore,  $f$  is a bijection from  $\mathbb{R}$  to  $(0, 1)$ .

**Example 1.7.** Let  $A = \{a_1, a_2, \dots, a_n\}$ , and let  $P = 2^A$ , the power set of  $A$ . Let  $X$  be the set of all binary strings of length  $n$  – i.e., the set of all sequences of the form  $x_1x_2 \cdots x_n$ , where  $x_i \in \{0, 1\}$ ,  $i = 1, \dots, n$ . Define a function  $\chi: P \rightarrow X$  as follows: For each  $S \in P$ ,  $\chi(S) = b_1b_2 \cdots b_n$  such that  $b_i = 1$  if  $a_i \in S$  and  $b_i = 0$  if  $a_i \notin S$ . Then  $\chi$  is a bijection, as shown below.

First, suppose that for  $S, T \in P$ ,  $\chi(S) = \chi(T) = b_1b_2 \cdots b_n$  (say). Then, for each  $i = 1, \dots, n$ ,  $a_i \in S$  if and only if  $b_i = 1$ , which is equivalent to  $a_i \in T$ . Thus,  $S = T$ . This shows that  $\chi$  is injective.

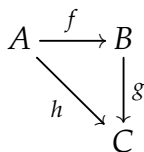
Next, let  $b_1b_2 \cdots b_n \in X$ . Define  $S \subseteq A$  as

$$S = \{a_i \in A \mid b_i = 1\}.$$

Then clearly,  $\chi(S) = b_1b_2 \cdots b_n$ . Hence,  $\chi$  is surjective.

## 1.7 Function Composition

If  $f: A \rightarrow B$  and  $g: B \rightarrow C$  are two functions, then the composition of  $f$  and  $g$  is the function  $h: A \rightarrow C$  defined by  $h(a) = g(f(a))$ , for all  $a \in A$ . We denote this function  $h$  by  $g \circ f$ , which is read as “ $g$  circle  $f$ ”, “ $g$  after  $f$ ”, or “ $g$  composed with  $f$ ”. We can also write this definition in terms of a **commutative diagram**. Consider the diagram given below.



We say that such a diagram **commutes** if the result of following any two directed paths from the same starting point to the same end point is the same. In the above diagram,  $A, f, B, g, C$  and  $A, h, C$  are two directed paths from  $A$  to  $C$  (and these are the only two directed paths with the same starting points and the same end points). Thus, the diagram commutes if and only if applying  $g$  after  $f$  equals  $h$ .

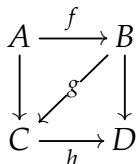
**Theorem 1.8.** *Composition of functions is an associative operation.*

*Proof.* To prove that two functions are equal, we need to show that they both map each element of the domain to the same element of the codomain. Consider three functions  $f: A \rightarrow B$ ,  $g: B \rightarrow C$ , and  $h: C \rightarrow D$ . Let  $a \in A$ . We will show that  $h \circ (g \circ f)$  and  $(h \circ g) \circ f$  map  $a$  to the same element of  $C$ .

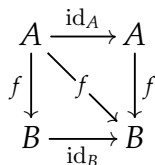
$$\begin{aligned}
 (h \circ (g \circ f))(a) &= h((g \circ f)(a)) \\
 &= h(g(f(a))) \\
 &= (h \circ g)(f(a)) \\
 &= ((h \circ g) \circ f)(a).
 \end{aligned}$$

Hence,  $h \circ (g \circ f) = (h \circ g) \circ f$ . □

**Exercise 1.8.** Show that in the diagram below, the square commutes if both the triangles commute.



The **identity function** on a set  $A$ , denoted as  $\text{id}_A$ , is the function from  $A$  to itself that maps every element of  $A$  to itself. That is,  $\text{id}_A: A \rightarrow A$  is defined as  $\text{id}_A(a) = a$ , for all  $a \in A$ . Note that  $\text{id}_A$  is a bijection from  $A$  to itself. The identity function is so named because it is the identity element (or neutral element) for the operation of function composition. That is, if  $f: A \rightarrow B$  is any function, then  $f \circ \text{id}_A = f$ , and  $\text{id}_B \circ f = f$ . Alternatively, we can say that the diagram given below commutes.



**Exercise 1.9.** Let  $A$  be a set.

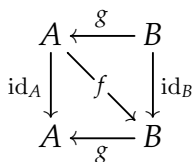
1. Show that  $\text{id}_A \circ \text{id}_A = \text{id}_A$ .
2. Show that if  $i: A \rightarrow A$  is any function satisfying the same property as the identity function, i.e., for every set  $B$  and every function  $f: A \rightarrow B$ ,  $f \circ i = f$ , and for every set  $C$  and every function  $g: C \rightarrow A$ ,  $i \circ g = g$ , then  $i = \text{id}_A$ .

## 1.8 Isomorphisms of Sets

If  $f: A \rightarrow B$  is a function, then a function  $g: B \rightarrow A$  is an **inverse** of  $f$  if  $g \circ f = \text{id}_A$  and  $f \circ g = \text{id}_B$ . Equivalently,  $g$  is an inverse of  $f$  if the



diagram given below commutes.



**Exercise 1.10.** Prove that any function has at most one inverse.

Hint: Assume that a function  $f: A \rightarrow B$  has two inverses  $g$  and  $h$ , and evaluate  $g \circ f \circ h$  in two different ways.

A function  $f: A \rightarrow B$  is an **isomorphism** (of sets) if it has an inverse. Then the unique inverse (see Exercise 1.10) of  $f$  is denoted by  $f^{-1}$ . Note that  $f^{-1}$  is an isomorphism from  $B$  to  $A$ . For any two sets  $A$  and  $B$ , we say that  $A$  is **isomorphic to**  $B$  if there is an isomorphism from  $A$  to  $B$ . We write this as  $A \cong B$ .

**Exercise 1.11.**

1. Show that the identity function on a set is an isomorphism from the set to itself.
2. Prove that if  $f$  and  $g$  are isomorphisms, from  $A$  to  $B$  and from  $B$  to  $C$ , respectively, then  $g \circ f$  is an isomorphism from  $A$  to  $C$ .
3. Show that  $\cong$  is an equivalence relation on any collection of sets.

Now, we will prove that an isomorphism of sets is exactly the same thing as a bijection.

**Theorem 1.9.** A function  $f: A \rightarrow B$  is an isomorphism if and only if it is a bijection.

*Proof.* First, suppose that  $f$  is a bijection. We need to show that  $f$  is an isomorphism from  $A$  to  $B$  – i.e., that it has an inverse. We construct the inverse as follows. Define  $g: B \rightarrow A$  as  $g(b) = a$ , where  $a \in A$  is such that  $f(a) = b$ , for each  $b \in B$ .

To see that  $g$  is well-defined, observe that as  $f$  is bijective, for every  $b \in B$ , there exists an  $a \in A$  such that  $f(a) = b$ , and as  $f$  is injective, this element  $a$  is unique (i.e., if  $f(a') = b = f(a)$ , then  $a' = a$ ).

To see that  $g$  is the inverse of  $f$ , first consider any  $a \in A$ . If  $f(a) = b$ , then  $g(b) = a$ , by definition of  $g$ . That is,  $g(f(a)) = a$ , which shows that  $g \circ f = \text{id}_A$ . Next, consider any  $b \in B$ . Then, by definition of  $g$ ,  $g(b) = a \in A$  such that  $f(a) = b$ . That is,  $f(g(b)) = b$ , which shows that  $f \circ g = \text{id}_B$ . Thus,  $g$  is the inverse of  $f$ , and therefore  $f$  is an isomorphism.

Conversely, suppose that  $f: A \rightarrow B$  is an isomorphism. We will show that  $f$  is a bijection. For any  $b \in B$ , if we take  $a = f^{-1}(b)$ , then  $f(a) = b$ , which shows that  $f$  is surjective. To see that  $f$  is injective, suppose that  $a_1, a_2 \in A$  and  $f(a_1) = f(a_2)$ . Then  $a_1 = f^{-1}(f(a_1)) = f^{-1}(f(a_2)) = a_2$ . Hence,  $f$  is a bijection.  $\square$

## 1.9 Cardinality of Sets

The **cardinality** of a set is the number of elements in it. As sets can have infinitely many elements, we will define cardinality more rigorously using the concept of set isomorphisms.

**Definition 1.10.** Two sets  $A$  and  $B$  have the same **cardinality** if  $A \cong B$ . If  $A \cong \{1, \dots, n\}$ , then  $A$  is **finite** of cardinality  $n$ . If  $A \cong \mathbb{N}$ , then  $A$  is **countably infinite**. In either case,  $A$  is **countable**. Otherwise,  $A$  is **uncountable** or **uncountably infinite**.