

1

Introduction

1.1 Sets

Sets form the foundation for mathematics. We shall define a set to be a well-defined collection of objects. This definition is similar to the one given by Georg Cantor, one of the pioneers in the early development of set theory. The inadequacy of this definition became apparent when paradoxes or contradictions were discovered by the Italian logician Burali-Forti in 1879 and later by Bertrand Russell with the famous Russell paradox. It became obvious that sets had to be defined more carefully. Axiomatic systems have been developed for set theory to correct the problems discussed above and hopefully to avoid further contradictions and paradoxes. These systems include the Zermelo–Fraenkel–von Neumann system, the Gödel–Hilbert–Bernays system and the Russell–Whitehead system. In these systems the items that were allowed to be sets were restricted. Axioms were created to define sets. Any object which could not be created from these axioms was not allowed to be a set. These systems have been shown to be equivalent in the sense that if one system is consistent, then they all are. However, Gödel has shown that if the systems are consistent, it is impossible to prove that they are.

Definition 1.1 *An object in a set is called an **element** of the set or is said to **belong** to the set. If an object x is an element of a set A , this is denoted by $x \in A$. If an object x is not a member of a set A , this is denoted by $x \notin A$.*

Objects in a set are called elements. Finite sets may be described by listing their elements. For example the set of positive integers less than or equal to seven may be described by the notation $\{1, 2, 3, 4, 5, 6, 7\}$ where the braces are used to indicate that we are describing a set. Thus symbols in an alphabet can be listed using this notation. We can also list the set of positive integers less than or equal to 10 000, by using the notation $\{1, 2, 3, 4, \dots, 10\,000\}$ and the set of

positive integers by $\{1, 2, 3, 4, \dots\}$, where three dots denote the continuation of a pattern. By definition, $1 \in \{1, 2, 3, 4, 5\}$ but $8 \notin \{1, 2, 3, 4, 5\}$. An element of a set may also be a set. Therefore $A = \{1, 2, \{3, 4, 5\}, 3, 4\}$ is a set that contains elements 1, 2, $\{3, 4, 5\}$, 3, and 4. Note that $5 \notin A$, but $\{3, 4, 5\} \in A$.

In many cases, listing the elements of a set can be tedious if not impossible. For example, consider listing the set of all primes. We thus have a second form of notation called **set builder notation**. Using this notation, the set of all objects having property P will be described by $\{x : x \text{ has property } P\}$. For example the set of all former Prime Ministers of Britain would be described by $\{x : x \text{ has been a Prime Minister of Britain}\}$. The set of all positive even integers less than or equal to 100, could be described by $\{x : x \text{ is a positive even integer less than or equal to } 100\}$.

Definition 1.2 A set A is called a **subset** of a set B if every element of the set A is an element of the set B . If A is a subset of B , this is denoted by $A \subseteq B$. If A is not a subset of B , this is denoted by $A \not\subseteq B$.

Therefore $\{a, b, c\} \subseteq \{a, b, c, d, e\}$ but $\{a, b, f\} \not\subseteq \{a, b, c, d, e\}$. By definition, any set is a subset of itself.

Definition 1.3 A set A is **equal** to a set B if $A \subseteq B$ and $B \subseteq A$.

Therefore two sets are equal if they contain the same elements. Notice that there is no order in a set. A set is simply defined by the elements that it contains. Also an element either belongs to a set or does not. It would be redundant to list an element more than once when defining a set.

Definition 1.4 The **intersection** of two sets A and B , denoted by $A \cap B$, is the set consisting of all elements contained in both A and B .

Let $A = \{x : x \text{ plays tennis}\}$ and $B = \{x : x \text{ plays golf}\}$, then $A \cap B = \{x : x \text{ plays tennis and golf}\}$. If $A = \{x : x \text{ is a positive integer divisible by } 3\}$ and $B = \{x : x \text{ is a positive integer divisible by } 2\}$, then $A \cap B = \{x : x \text{ is a positive integer divisible by } 6\}$.

Definition 1.5 The **union** of two sets A and B , denoted by $A \cup B$, is the set consisting of all elements contained in either A or B .

Let $A = \{x : x \text{ plays tennis}\}$ and $B = \{x : x \text{ plays golf}\}$, then $A \cup B = \{x : x \text{ plays tennis or golf}\}$.

If $A = \{x : x \text{ is a positive integer divisible by } 3\}$ and $B = \{x : x \text{ is a positive integer divisible by } 2\}$, then $A \cup B = \{x : x \text{ is a positive integer divisible by either } 2 \text{ or } 3\}$.

Definition 1.6 The *set difference*, denoted by $B - A$, is the set of all elements in the set B that are not in the set A .

For example, the set $\{1, 2, 3, 4, 5\} - \{2, 4, 6, 8, 10\} = \{1, 3, 5\}$.

Example 1.1 Let $A = \{x : x \text{ plays tennis}\}$ and $B = \{x : x \text{ plays golf}\}$, the set $A - B = \{x : x \text{ plays tennis but does not play golf}\}$.

Definition 1.7 The *symmetric difference*, denoted by $A \Delta B$, is the set $(A - B) \cup (B - A)$.

It is easily seen that $A \Delta B = (A \cup B) - (A \cap B)$.

Example 1.2 Let $A = \{x : x \text{ plays tennis}\}$ and $B = \{x : x \text{ plays golf}\}$, the set $A \Delta B = \{x : x \text{ plays tennis or golf but not both}\}$.

We define two special sets. The first is the **empty set**, which is denoted by \emptyset or $\{\}$. As the name implies, this set contains no elements. It is a subset of every set A since every element in the empty set is also in A . The second special set is the **universe** or **universe of discourse**, which we denote by \mathcal{U} . The universe is given, and limits or describes the type of sets under discussion, since they must all be subsets of the universe. For example if the sets we are describing are subsets of the integers then the universe could be the set of integers. If the universe is the the set of college students, then the set $\{x : x \text{ is a musician}\}$ would be the set of all musicians who are in college. Often the universe is understood and so is not explicitly mentioned. Later we shall see that the universe of particular interest to us is the set of all strings of symbols in a given alphabet.

Definition 1.8 Let A be a set. $A' = \mathcal{U} - A$ is the set of all elements not in A .

Example 1.3 Let A be the set of even integers and \mathcal{U} be the set of integers. Then A' is the set of odd integers.

Example 1.4 Let $A = \{x : x \text{ collects coins}\}$, then $A' = \{x : x \text{ does not collect coins}\}$.

The proof of the following theorem is left to the reader.

Theorem 1.1 Let A , B , and C be subsets of the universal set \mathcal{U}

(a) *Distributive properties*

$$\begin{aligned} A \cap (B \cup C) &= (A \cap B) \cup (A \cap C), \\ A \cup (B \cap C) &= (A \cup B) \cap (A \cup C). \end{aligned}$$

(b) Idempotent properties

$$\begin{aligned}A \cap A &= A, \\A \cup A &= A.\end{aligned}$$

(c) Double Complement property

$$(A')' = A.$$

(d) De Morgan's laws

$$\begin{aligned}(A \cup B)' &= A' \cap B', \\(A \cap B)' &= A' \cup B'.\end{aligned}$$

(e) Commutative properties

$$\begin{aligned}A \cap B &= B \cap A, \\A \cup B &= B \cup A.\end{aligned}$$

(f) Associative laws

$$\begin{aligned}A \cap (B \cap C) &= (A \cap B) \cap C, \\A \cup (B \cup C) &= (A \cup B) \cup C.\end{aligned}$$

(g) Identity properties

$$\begin{aligned}A \cup \emptyset &= A, \\A \cap \mathcal{U} &= A.\end{aligned}$$

(h) Complement properties

$$\begin{aligned}A \cup A' &= \mathcal{U}, \\A \cap A' &= \emptyset.\end{aligned}$$

Definition 1.9 The *size* or **cardinality** of a finite set A , denoted by $|A|$, is the number of elements in the set. An infinite set which can be listed so that there is a first element, second element, third element etc. is called **countably infinite**. If it cannot be listed, it is said to be **uncountable**. Two infinite sets have the same **cardinality** if there is a one-to-one correspondence between the two sets. We denote this by $|A| = |B|$. If there is a one-to-one correspondence between A and a subset of B , we denote this by $|A| \leq |B|$. If $|A| \leq |B|$ but there is no one-to-one correspondence between A and B , then we denote this by $|A| < |B|$.

Thus the cardinality of the set $\{a, b, c, \{d, e, f\}\}$ is 4. Intuitively, there is a one-to-one correspondence between two sets if elements of the two sets can be written in pairs so that each element in one set can be paired with one and only one element of the other set. The positive integers are obviously countable. Although it will not be proved here, the integers and rational numbers are

both countable sets. The real numbers however are not a countable set. We see that there are two infinite sets, the countable sets and the uncountable sets with different cardinality; however, we shall soon see that there are an infinite number of infinite sets of different cardinality.

Further discussion of cardinality will be continued in the appendices.

Definition 1.10 *Let A and B be sets. The **Cartesian product** of A and B , denoted by $A \times B$ is the set $\{(a, b) : a \in A \text{ and } b \in B\}$.*

For example, let $A = \{a, b\}$ and $B = \{1, 2, 3\}$, then

$$A \times B = \{(a, 1)(a, 2)(a, 3)(b, 1)(b, 2)(b, 3)\}.$$

The familiar Cartesian plane $R \times R$ is the set of all ordered pairs of real numbers. Note that for finite sets $|A \times B| = |A| \times |B|$.

Definition 1.11 *The **power set** of a set A , denoted by $\mathcal{P}(A)$, is the set of all subsets of A .*

For example the power set of $\{a, b, c\}$ is

$$\{\{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}, \emptyset\}.$$

In the finite case, it can be easily shown that $|\mathcal{P}(A)| = 2^{|A|}$.

Exercises

- (1) State which of the following are true and which are false:
 - (a) $\{\emptyset\} \subseteq A$ for an arbitrary set A .
 - (b) $\emptyset \subseteq A$ for an arbitrary set A .
 - (c) $\{a, b, c\} \subseteq \{a, b, \{a, b, c\}\}$.
 - (d) $\{a, b, c\} \in \{a, b, \{a, b, c\}\}$.
 - (e) $A \in \mathcal{P}(A)$.
- (2) Prove Theorem 1.1. Let A , B , and C be subsets of the universal set \mathcal{U} .
 - (a) **Idempotent property**

$$A \cap A = A,$$

$$A \cup A = A.$$

- (b) **Double Complement property**

$$(A')' = A.$$

- (c) **De Morgan's laws**

$$(A \cup B)' = A' \cap B',$$

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

(d) **Commutative properties**

$$A \cap B = B \cap A,$$

$$A \cup B = B \cup A.$$

(e) **Associative properties**

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

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

(f) **Distributive properties**

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

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

(g) **Identity properties**

$$A \cup \emptyset = A,$$

$$A \cap \mathcal{U} = A.$$

(h) **Complement properties**

$$A \cup A' = \mathcal{U},$$

$$A \cap A' = \emptyset.$$

- (3) Given a set $A \in \mathcal{P}(C)$, find a set B such that $A \Delta B = \emptyset$.
- (4) If $A \subseteq B$, what is $A \Delta B$?
- (5) Using the properties in Theorem 1.1 prove that $A \cap (B \Delta C) = (A \cap B) \Delta (A \cap C)$.
- (6) Use induction to prove that for any finite set A , $|A| < |\mathcal{P}(A)|$.
- (7) (Russell's Paradox) Let S be the set of all sets. Then $S \in S$. Obviously $\emptyset \notin \emptyset$. Let $W = \{A : A \notin A\}$. Discuss whether $W \in W$.
- (8) Prove using the properties in Theorem 1.1
- $A - (B \cup C) = (A - B) \cap (A - C)$,
 - $A - (B \cap C) = (A - B) \cup (A - C)$.
- (9) Use the fact that $A \cap (A \cup B) = A$ to prove that $A \cup (A \cap B) = A$.
- (10) Prove that if two disjoint sets are countable, then their union is countable.

1.2 Relations

Definition 1.12 Given sets A and B , any subset \mathcal{R} of $A \times B$ is a **relation** between A and B . If $(a, b) \in \mathcal{R}$, this is often denoted by $a\mathcal{R}b$. If $A = B$, \mathcal{R} is said to be a **relation** on A .

Note that relations need not have any particular property nor even be describable. Obviously we will be interested in those relations which are describable and have particular properties which will be shown later.

Example 1.5 If $A = \{a, b, c, d, e\}$ and $B = \{1, 2, 3, 4, 5\}$, then

$$\{(a, 3), (a, 2), (c, 2), (d, 4), (e, 4), (e, 5)\}$$

is a relation between A and B .

Example 1.6 $\{(x, y) : x \geq y\}$ and $\{(x, y) : x^2 + y^2 = 4\}$ are relations on R .

Example 1.7 If A is the set of people, then aRb if a and b are cousins is a relation on A .

Definition 1.13 The **domain** of a relation \mathcal{R} between A and B is the set $\{a : a \in A \text{ and there exists } b \in B \text{ so that } aRb\}$. The **range** of a relation \mathcal{R} between A and B is the set $\{b : b \in B \text{ and there exists } a \in A \text{ so that } aRb\}$.

Example 1.8 The domain and range of the relation $\{(x, y) : x^2 + y^2 = 4\}$ are $-2 \leq x \leq 2$ and $-2 \leq y \leq 2$ respectively.

Example 1.9 The relation \mathcal{R} is on the set of people. The domain and range of \mathcal{R} is the set of people who have cousins.

Definition 1.14 Let \mathcal{R} be a relation between A and B . The inverse of the relation \mathcal{R} denoted by \mathcal{R}^{-1} is a relation between B and A , defined by $\mathcal{R}^{-1} = \{(b, a) : (a, b) \in \mathcal{R}\}$.

Example 1.10 If $A = \{a, b, c, d, e\}$ and $B = \{1, 2, 3, 4, 5\}$, and

$$\mathcal{R} = \{(a, 3), (a, 2), (b, 3), (b, 5), (c, 3), (d, 2), (d, 3), (e, 4), (e, 5)\}$$

is a relation between A and B then

$$\mathcal{R}^{-1} = \{(3, a), (2, a), (3, b), (5, b), (3, c), (2, d), (3, d), (4, e), (5, e)\}$$

is a relation between B and A .

Example 1.11 If $\mathcal{R} = \{(x, y) : y = 4x^2\}$, then $\mathcal{R}^{-1} = \{(y, x) : y = 4x^2\}$.

Definition 1.15 Let \mathcal{R} be a relation between A and B , and let \mathcal{S} be a relation between B and C . The composition of \mathcal{R} and \mathcal{S} , denoted by $\mathcal{S} \circ \mathcal{R}$ is a relation between A and C defined by $(a, c) \in \mathcal{S} \circ \mathcal{R}$ if there exists $b \in B$ such that $(a, b) \in \mathcal{R}$ and $(b, c) \in \mathcal{S}$.

Example 1.12 Let $A = \{a, b, c, d, e\}$ and $B = \{1, 2, 3, 4, 5\}$ and

$$\mathcal{R} = \{(a, 3), (a, 2), (c, 2), (d, 4), (e, 4), (e, 5)\}$$

be a relation between A and B . Then, as shown above

$$\mathcal{R}^{-1} = \{(3, a), (2, a), (2, c), (4, d), (4, e), (5, e)\}$$

is a relation between B , and A ,

$$\mathcal{R} \circ \mathcal{R}^{-1} = \{(3, 3), (3, 2), (2, 2), (2, 3), (4, 4), (5, 5)\}$$

is a relation on B , and

$$\mathcal{R}^{-1} \circ \mathcal{R} = \{(a, a), (a, c), (c, a), (c, c), (d, d), (d, e), (e, e)\}$$

is a relation on A .

Example 1.13 If $\mathcal{R} = \{(x, y) : y = x + 5\}$ and $\mathcal{S} = \{(y, z) : z = y^2\}$ then $\mathcal{S} \circ \mathcal{R} = \{(x, z) : z = (x + 5)^2\}$.

Theorem 1.2 *Composition of relations is associative; that is, if A , B , and C are sets and if $R \subseteq A \times B$, $S \subseteq B \times C$, and $T \subseteq C \times D$, then $T \circ (S \circ R) = (T \circ S) \circ R$.*

Proof First show that $T \circ (S \circ R) \subseteq (T \circ S) \circ R$. Let $(a, d) \in T \circ (S \circ R)$, then there exists $c \in C$ such that $(a, c) \in S \circ R$ and $(c, d) \in T$. Since $(a, c) \in S \circ R$, there exists $b \in B$ so that $(a, b) \in R$ and $(b, c) \in S$. Since $(b, c) \in S$ and $(c, d) \in T$, $(b, d) \in T \circ S$. Since $(b, d) \in T \circ S$ and $(a, b) \in R$, $(a, d) \in (T \circ S) \circ R$. Thus, $T \circ (S \circ R) \subseteq (T \circ S) \circ R$. The second part of the proof showing that $(T \circ S) \circ R \subseteq T \circ (S \circ R)$ is similar and is left to the reader. \square

When \mathcal{R} is a relation on a set A , there are certain special properties that \mathcal{R} may have which we now consider.

Definition 1.16 *A relation \mathcal{R} on A is **reflexive** if $a\mathcal{R}a$ for all $a \in A$. A relation \mathcal{R} on A is **symmetric** if $a\mathcal{R}b \rightarrow b\mathcal{R}a$ for all $a, b \in A$. A relation \mathcal{R} on A is **antisymmetric** if $a\mathcal{R}b$ and $b\mathcal{R}a$ implies $a = b$. A relation is **transitive** if whenever $a\mathcal{R}b$ and $b\mathcal{R}c$, then $a\mathcal{R}c$.*

Example 1.14 Let A be the set of all people and $a\mathcal{R}b$ if a and b are siblings. The relation \mathcal{R} is not reflexive since a person cannot be their own brother or sister. It is symmetric however since if a and b are siblings, then b and a are siblings. It might appear that \mathcal{R} is transitive. Such is not the case however since if a and b are siblings, and b and a are siblings, we must conclude that a and a are siblings, which we know is not true.

Example 1.15 Let A be the set of all people and $a\mathcal{R}b$ if a and b have the same parents. The relation \mathcal{R} is reflexive since everyone has the same parents as themselves. It is symmetric since if a and b have the same parents, b and

a have the same parents. It is also transitive since if a and b have the same parents and b and c have the same parents, then a and c have the same parents.

Example 1.16 Let $A = \{a, b, c, d, e\}$ and

$$\mathcal{R} = \{(a, a), (a, b), (b, c), (b, b), (a, c), (c, c), (d, d), (a, d), (c, e), (d, a), (b, a)\}.$$

\mathcal{R} is not reflexive since $(e, e) \notin \mathcal{R}$. It is not symmetric because $(a, c) \in \mathcal{R}$, but $(c, a) \notin \mathcal{R}$. It is not antisymmetric since $(a, d), (d, a) \in \mathcal{R}$, but $d \neq a$. It is not transitive since $(a, c), (c, e) \in \mathcal{R}$, but $(a, e) \notin \mathcal{R}$.

Example 1.17 Let \mathcal{R} be the relation on Z defined by $a\mathcal{R}b$ if $a - b$ is a multiple of 5. Certainly $a - a = 0$ is a multiple of 5, so \mathcal{R} is reflexive. If $a - b$ is a multiple of 5, then $a - b = 5k$ for some integer k . Hence $b - a = 5(-k)$ is a multiple of 5, so \mathcal{R} is symmetric. If $a - b$ is a multiple of 5 and $b - c$ is a multiple of 5, then $a - b = 5k$ and $b - c = 5m$ for some integers k and m .

$$\begin{aligned} a - c &= a - b + b - c \\ &= 5k + 5m \\ &= 5(k + m) \end{aligned}$$

so that $a - c$ is a multiple of 5. Hence \mathcal{R} is transitive.

Definition 1.17 A relation \mathcal{R} on A is an **equivalence relation** if it is reflexive, symmetric, and transitive.

Example 1.18 Let Z be the set of integers and \mathcal{R}_1 be the relation on Z defined by $\mathcal{R}_1 = \{(m, n) : m - n\}$ is divisible by 5. \mathcal{R}_1 is shown above to be an equivalence relation on the integers.

Example 1.19 Let A be the set of all people. Define \mathcal{R}_2 by $a\mathcal{R}_2b$ if a and b are the same age. This is easily shown to be an equivalence relation.

An equivalence relation on a set A divides A into nonempty subsets that are **mutually exclusive** or **disjoint**, meaning that no two of them have an element in common. In the first example above, the sets

$$\begin{aligned} &\{\dots - 20, -15, -10, -5, 0, 5, 10, 15, 20, \dots\} \\ &\{\dots - 19, -14, -9, -4, 1, 6, 11, 16, 21, \dots\} \\ &\{\dots - 18, -13, -8, -3, 2, 7, 12, 17, 22, \dots\} \\ &\{\dots - 17, -12, -7, -2, 3, 8, 13, 18, 23, \dots\} \\ &\{\dots - 16, -11, -6, -1, 4, 9, 14, 19, 24, \dots\} \end{aligned}$$

contain elements that are related to each other and no element in one set is related to an element in another set. In the second example the sets $\{s_n = x : x$ is n years old $\}$ for $n = 0, 1, 2, \dots$ also divide the set of people into sets that are

related to each other. Also no person can belong to two sets. (See the definition of partition below.)

Notation 1.1 Let R be an equivalence relation on a set A and $a \in A$. Then $[a]_{\mathcal{R}} = \{x : x\mathcal{R}a\}$. If the relation is understood, then $[a]_{\mathcal{R}}$ is simply denoted by $[a]$. Let $[A]_{\mathcal{R}} = \{[a]_{\mathcal{R}} : a \in A\}$.

Definition 1.18 Let A and I be nonempty sets and $\langle A \rangle = \{A_i : i \in I\}$ be a set of nonempty subsets of A . The set $\langle A \rangle$ is called a **partition** of A if both of the following are satisfied:

- (a) $A_i \cap A_j = \emptyset$ for all $i \neq j$.
- (b) $A = \bigcup_{i \in I} A_i$; that is, $a \in A$ if and only if $a \in A_i$ for some $i \in I$.

Theorem 1.3 A nonempty set of subsets $\langle A \rangle$ of a set A is a partition of A if and only if $\langle A \rangle = [A]_{\mathcal{R}}$ for some equivalence relation \mathcal{R} .

Proof Let $\langle A \rangle = \{A_i : i \in I\}$ be a partition of A . Define a relation \mathcal{R} on A by $a\mathcal{R}b$ if and only if a and b are in the same subset A_i for some i . Certainly for all a in A , $a\mathcal{R}a$ and \mathcal{R} is reflexive. If a and b are in the same subset A_i , then b and a are in the subset A_i and \mathcal{R} is symmetric. Since the sets $A_i \cap A_j = \emptyset$ for $i \neq j$, if a and b are in the same subset and b and c are in the same subset, then a and c are in the same subset. Hence \mathcal{R} is transitive and \mathcal{R} is an equivalence relation.

Conversely, assume that \mathcal{R} is an equivalence relation. We need to show that $[A]_{\mathcal{R}} = \{[a] : a \in A\}$ is a partition of A . Certainly, for all a , $[a]$ is nonempty since $a \in [a]$. Obviously, A is the union of the $[a]$, such that $a \in A$. Assume that $[a] \cap [b]$ is nonempty and let $x \in [a] \cap [b]$. Then $x\mathcal{R}a$ and $x\mathcal{R}b$, and by symmetry, $a\mathcal{R}x$. But since $a\mathcal{R}x$ and $x\mathcal{R}b$, by transitivity, $a\mathcal{R}b$. Therefore, $a \in [b]$. If $y \in [a]$, then $y\mathcal{R}a$ and since $a\mathcal{R}b$, by transitivity, $y\mathcal{R}b$. Therefore, $[a] \subseteq [b]$. Similarly, $[b] \subseteq [a]$ so that $[a] = [b]$, and we have a partition of A . \square

Definition 1.19 $[A]_{\mathcal{R}}$ is called the set of **equivalence classes** of A given by the relation \mathcal{R} .

If the symmetric property is changed to antisymmetric property, we have the following:

Definition 1.20 A relation \mathcal{R} on A is a **partial ordering** if it is reflexive, antisymmetric, and transitive. If \mathcal{R} is a partial ordering on A , then (A, \mathcal{R}) is called a **partially ordered set** or a **poset**.