1
Sets and Mappings

The notions of a 'set' and of a 'mapping' are fundamental in modern mathematics. In many mathematical contexts a perceptive choice of appropriate sets and mappings may lead to a better understanding of the underlying mathematical processes. We shall outline those aspects of sets and mappings which are relevant to present purposes and, for the delectation of the reader, conclude with a few logical paradoxes in regard to sets.

1.1 Union and Intersection

We are accustomed to speak of a 'collection' of books, or of an 'assembly' of people or of a 'list' of guests. In mathematics the word 'set' is used to denote the basic concept which is expressed by each of the collective nouns; in mathematics we say simply a 'set' of books, or a 'set' of people or a 'set' of guests.

Definition 1

A collection or assembly of objects is called a **set**. Each object is said to be an **element** of the set.

Thus in the phrase 'a set of books', each book involved in the set is an element of the set. Frequently the symbols constituting the elements of a (mathematical)

D. A. R. Wallace, *Groups, Rings and Fields*

set will be letters or numbers. If a set A consists of, say, the elements a, b, c then we write $A = \{a, b, c\}$, the use of curly brackets being customary. Notice that as we are concerned only with membership of the set we disregard any repetition of the symbols and have no preferred order for writing them down.

Example 1

Let A have 1, 2, 3, 4 as elements. Then $A = \{1,2,3,4\} = \{1,1,2,2,3,4\} = \{2,1,3,4\} = \{1,3,4,2\}$ etc.

Definition 2

Let A be a set. If A consists of a finite number of elements, say $a_1, a_2, \ldots, a_N$ (where the notation presumes the elements are distinct) then we write

$$A = \{a_1, a_2, \ldots, a_N\}$$

and A is said to be a **finite set** of **cardinality** N, written $N = |A|$. If A does not have a finite number of elements A is called an **infinite set** and is said to have **infinite cardinality**. The set consisting of no elements at all is called the **empty set** or the **null set** and is denoted by $\varnothing$ ($\varnothing$ is a letter of the Norwegian alphabet). Evidently $|\varnothing| = 0$.

Examples 2

1. $\varnothing$ = set of all unicorns.
2. $\varnothing$ = set of all persons living on the moon in 1996.
3. $|\{1,2,3,4\}| = 4$.
4. $|\{a, b, c, d, e\}| = 5$.

A set is often given by some property which characterizes the elements of the set. Before giving a definition we offer a colourful example.

Example 3

Let A be the set of the colours of the rainbow. Whether or not a given colour is in A is determined by a property, namely that of being one of the colours of the rainbow. Of course in this particular instance we may write down the elements explicitly. Indeed

$$A = \{\text{red, orange, yellow, green, blue, indigo, violet}\}.$$

Definition 3

Let P be some property. The set of elements, each of which has the property P, is written as

$$A = \{x|x \text{ has the property } P\},$$

which we read as 'A is the set of all x such that x has the property P'.

Examples 4

1. Let A consist of the squares of strictly positive integers. Then
$$A = \{x|x = n^2, n = 1, 2, \ldots\}.$$
The set A may also be written as
$$A = \{1, 4, 9, \ldots\},$$
but notice that this notation is ambiguous since it would only be an inference that A consists of squares of integers.
2. The set $\{x|x < 0 \text{ and } x > 1\}$ is the empty set since there is no number which is simultaneously less than 0 and greater than 1.
3. The set $\{x|x^2 = 3,\ x \text{ is an integer}\}$ is empty since there is no integer with square equal to 3.

Definition 4

Let A be a set. Let x be an element. If x is **an element of** A we write

$$x \in A,$$

and if x is **not an element of** A we write

$$x \notin A.$$

Example 5

$$a \in \{a, b, c\}, \quad b \notin \{1, 2, 3\},$$

$$36 \in \{x|x = n^2, n = 0, 1, 2, \ldots\}, \quad 37 \notin \{x|x = n^2, n = 0, 1, 2, \ldots\}.$$

Definition 5

A set A is said to be a **subset** of a set B if every element of A is also an element of B. We write

$$A \subseteq B$$

to indicate that A is a **subset** of B and read the notation as 'A is contained in or equal to B'. The empty set is deemed to be a subset of every set. If A is a subset of B but $A \neq B$ then A is said to be a **proper** subset of B.

If A is not a subset of B then there exists at least one element of A which is not an element of B and we write

$$A \not\subseteq B.$$

If $A \subseteq B$ and $B \subseteq A$ then the sets A and B are **equal** and we write

$$A = B.$$

If A and B are **not equal** we write

$$A \neq B.$$

If $A \subseteq B$ and $A \neq B$ we write $A \subset B$.

Given two sets A and B, to prove that $A \subseteq B$ we have to show that $x \in A$ implies $x \in B$. To prove that $A \not\subseteq B$, we have to exhibit an $x \in A$ such that $x \notin B$.

Two sets A and B are equal if and only if they are elementwise indistinguishable.

Examples 6

1. Let $A = \{a, c\}, B = \{a, b, c, d\}, C = \{a, b, c\}$. Then $A \subseteq B, C \subseteq B$.
2. Let $A = \{x | x^2 = 1\}, B = \{-1, 1\}$. Although A and B are described in different ways they have the same elements and so $A = B$.

Definition 6

Applications of the theory of sets usually take place within some fixed set (which naturally varies according to the circumstances). This fixed set for the particular application is called the **universal set** and is often denoted by U. The subset of U consisting of the elements of U having the **property** P is denoted by

$$\{x \in U | x \text{ has the property } P\},$$

or simply as

$$\{x | x \text{ has the property } P\}$$

if the universal set is obvious. Frequently explicit reference to a universal is omitted.

We now introduce the operations of union and intersection on sets.

Definition 7

Let $A, B, C, \ldots$ be sets. The set consisting of those elements each of which is in at least one of the sets $A, B, C, \ldots$ is called the **union** of $A, B, C, \ldots$ and is written

$$A \cup B \cup C \cup \ldots$$

The set consisting of those elements each of which is in all of the sets $A, B, C, \ldots$ is called the **intersection** of $A, B, C, \ldots$ and is written as

$$A \cap B \cap C \cap \ldots$$

The sets $A, B, C, \ldots$ are said to be **disjoint** if the intersection of any two distinct sets is empty, that is, $A \cap B = A \cap C = B \cap C = \ldots = \varnothing$.

The union $A \cup B \cup C \cup \ldots$ is said to be a **disjoint union** if the sets $A, B, C, \ldots$ are disjoint.

Example 7

Let $U = \{a, b, c, d, e, f, g, h, i\}$ be the universal set. Let $A = \{a, b, c\}$, $B = \{d, f, i\}$, $C = \{a, b, c, d, f, g\}$, $D = \{a, e, g, h, i\}$, $E = \{e, g, h\}$.

Then

$$A \cup B = \{a, b, c, d, f, i\}, \quad A \cap B = \varnothing,$$

$$C \cup D = \{a, b, c, d, e, f, g, h, i\} = U, \quad C \cap D = \{a, g\},$$

$$A \cup B \cup C = \{a, b, c, d, f, g, i\}, \quad A \cap B \cap C = \varnothing,$$

$$B \cup C \cup D = \{a, b, c, d, e, f, g, h, i\} = U, \quad B \cap C \cap D = \varnothing,$$

$$U = A \cup B \cup E,$$

where this union is disjoint as $A \cap B = A \cap E = B \cap E = \varnothing$.

It is immediate that for sets A and B we have $A \cap A = A$, $A \cup A = A$ and $A \cap B = B \cap A \subseteq A \subseteq A \cup B = B \cup A$.

We prove a useful lemma.

Lemma 1

Let A, B, X be sets such that $A \subseteq B$. Then the following hold.

1. $A \cap X \subseteq B \cap X$.
2. $A \cup X \subseteq B \cup X$.

Proof

1. We have to prove that every element of $A \cap X$ is also in $B \cap X$.
   Let $c \in A \cap X$. Then $c \in A$ and so, as $A \subseteq B$, $c \in B$. But $c \in X$ and so $c \in B \cap X$. Hence $A \cap X \subseteq A \cap X$.
2. Let $c \in A \cup X$. Then either $c \in A$ or $c \in X$. If $c \in A$ then $c \in B$ and so, in either case, $c \in B \cup X$. Thus $A \cup X \subseteq B \cup X$. □

Definition 8

Let A be a subset of the universal set U. The subset of U consisting of all elements of U not in A is called the **complement** (note spelling!) of A. The complement of A is denoted by $U \setminus A$ or by A' if the universal set is clear.

$$U \setminus A = A' = \{x \in U | x \notin A\}$$

(Another notation for the complement, but not used in this text, is $\complement A$.)

$$U = (U \setminus A) \cup A, \ (U \setminus A) \cap A = \varnothing,$$

and so

$$A = U \text{ if and only if } A' = \varnothing.$$

Example 8

Let $U = \{1, 2, 3, 4, 5\}, A = \{2, 3\}$. Then $U \setminus A = \{1, 4, 5\}$.

The notion of complement extends to that of relative complement.

Definition 9

Let A and B be sets. The **relative complement** of A in B, denoted by $B \setminus A$, is the set of elements of B which are not in A.

Example 9

Let $A = \{p, q, r\}, B = \{q, r, s, t\}$. Then $B \setminus A = \{s, t\}, A \setminus B = \{p\}$.

We conclude this section with a fairly obvious but useful result.

Theorem 1

Let A and B be sets. Then the following statements are equivalent.

1. $A \subseteq B$.
2. $A \cap B = A$.
3. $A \cup B = B$.

Proof

We prove the equivalence of 1 and 2, leaving the equivalence of 1 and 3 as an exercise.

Suppose $A \subseteq B$. Then, by Lemma 1,

$$A = A \cap A \subseteq A \cap B \subseteq A, \text{ and thus}$$

$$A = A \cap B.$$

Conversely if $A = A \cap B$ then certainly $A \subseteq B$. □

We conclude this section by introducing the 'Cartesian product' of sets. The adjective 'Cartesian' derives from the name of R. du P. Descartes (1596–1650), mathematician and philosopher whose philosophical outlook is enshrined in his famous aphorism "je pense, donc je suis", in English "I think, therefore I am". (Quotation from Discours de la Methode [Leyden, 1637, 4th part]).

Definition 10

Let A and B be two sets. The **Cartesian product** $A \times B$ of A and B is defined to be the set of all ordered pairs of the form $(a, b), a \in A, b \in B$;

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

The **Cartesian product** $A_1 \times A_2 \times \ldots \times A_n$ of the sets $A_1, A_2, \ldots, A_n$ (in this order) is defined to be the set of all ordered n-tuples of the form

$$(a_1, a_2, \ldots, a_n),\ a_1 \in A_1,\ a_2 \in A_2, \ldots, a_n \in A_n,$$

$$A_1 \times A_2 \times \ldots \times A_n = \{(a_1, a_2, \ldots, a_n\} | a_i \in A_i, i = 1, 2, \ldots, n\}.$$

Note that if the sets A and B are distinct, then $A \times B \neq B \times A$.

Example 10

Let A and B be finite sets of m and n elements respectively. Then $A \times B$ is a set of mn elements since in the ordered pair (a, b) there are m possibilities for a, and n possibilities for b.

Exercises 1.1

1. Let the universal set U be the set $\{u, v, w, x, y, z\}$. Let $A = \{u, v, w\}$, $B = \{w, x, y\}$, $C = \{x, y, z\}$. Write down the subsets: $A \cup B$, $A \cap B$, $A \cap C$, $A \cup C$, $A \setminus B$, $B \setminus A$, $A \setminus C$, $C \setminus A$, A', B', C', $A \setminus (B \cup C)$, $B \setminus (A \cap C)$, $(A \cap B) \cup (B \setminus A)$.

2. Let the universal set U be the set $\{a, b, c, 1, 2, 3\}$. Let $X = \{a, b, 1\}$, $Y = \{b, 2, 3\}$, $Z = \{c, 2, 3\}$. Write down the subsets: $X \cup Y$, $X \cap Y$, $X \cup Z$, $X \cap Z$, $X \setminus Y$, $Y \setminus X$, $X \setminus Z$, $Z \setminus X$, X', Y', Z', $(X \cap Y)'$, $X' \cup Y'$, $(X \cup Z)'$, $X' \cap Z'$.

3. Let the universal set U be the set $\{1, 2, 3, 4, 5, 6\}$. Let $A = \{1, 2, 4, 5\}$. Let X be a subset of U such that $A \cup X = \{1, 2, 4, 5, 6\}$ and $A \cap X = \{2, 4\}$. Prove that there is only one possibility for X, namely $\{2, 4, 6\}$.

4. Let A and B be sets. Prove that $A \subseteq B$ if and only if $B = A \cup B$ (Theorem 1).

5. Let A be the set $\{3, 5, 8, \ldots\}$. Is A the set $\{3, 5, 8, 13, \ldots\}$ or the set $\{3, 5, 8, 12, \ldots\}$ or neither?

6. Let A_i be a finite set of k_i elements, $i = 1, 2, \ldots, n$. Prove that

   $A_1 \times A_2 \times \ldots \times A_n$ is a finite set of $k_1 k_2 \ldots k_n$ elements.

1.2 Venn Diagrams

In this section we shall describe a technique which, in certain circumstances, enables us to visualize sets and their unions and intersections etc. by drawing pictures on paper. The resulting pictures are known as **Venn diagrams**, after J. Venn (1834–1923).

We proceed as follows. For the universal set U we draw a rectangle and for arbitrary subsets A, B of U we draw shapes as below:

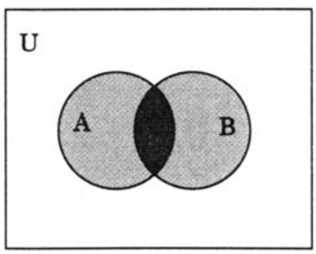

Figure 1.1.

The shaded area represents $A \cup B$ and the dark-shaded area $A \cap B$. Conveniently we may assign numbers to the regions:

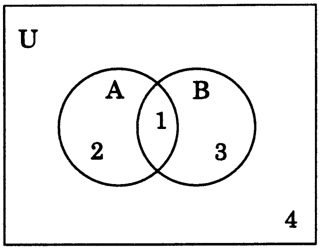

Figure 1.2.

Thus

region 1 represents $A \cap B$,
region 2 represents $A \setminus (A \cap B)$,
region 3 represents $B \setminus (A \cap B)$,
region 4 represents $U \setminus (A \cup B)$.

The Venn diagram makes clear that A is the disjoint union of the two subsets $A \setminus B$ and $A \cap B$, and $A \cup B$ is the disjoint union of the three subsets $A \setminus B$, $B \setminus A$ and $A \cap B$.

Wise use of Venn diagrams may lead to general results for which a rigorous proof may later be obtained. We give two examples of this procedure in the following examples.

Example 11

Using the above Venn diagram we may observe the following:

A	is represented by regions			1, 2
A'	...	...	...	3, 4
B	...	...	...	1, 3
B'	...	...	...	2, 4
$(A \cap B)'$	...	...	...	2, 3, 4
$A' \cup B'$	...	...	...	2, 3, 4

Thus, from our Venn diagram representation, we conclude that

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

Similarly we conclude that

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

A rigorous proof will be given in Theorem 3.

If now C is a third subset of U then the Venn diagram becomes:

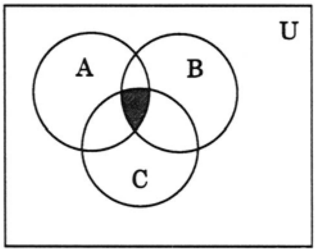

Figure 1.3.

The shaded region represents $A \cap B \cap C$.

For four or more subsets of U the method has fundamental limitations (as those attempting to draw satisfactory diagrams of four subsets will discover) and should be avoided.

Example 12

Let A, B, C be subsets of the universal set U and suppose $A \subseteq C$, $B \subseteq C$. The appropriate Venn diagram is:

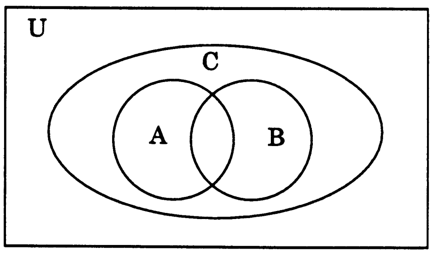

Figure 1.4.

Example 13

Let us draw a Venn diagram to illustrate the result that if $X \subseteq Y$ then $A \cap X \subseteq A \cap Y$.

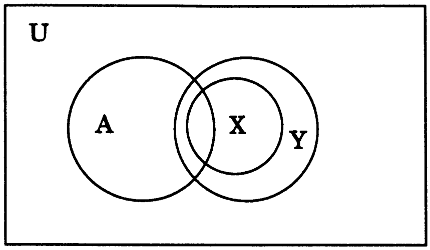

Figure 1.5.

Consider a Venn diagram with three subsets A, B, C of the universal set U and with regions assigned numbers as follows:

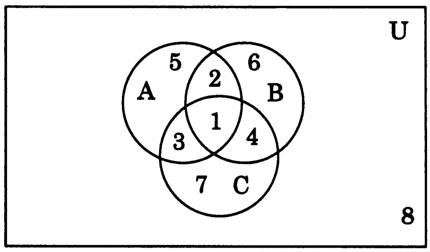

Figure 1.6.

region 1 represents $A \cap B \cap C$
region 2 represents $(A \cap B) \setminus (A \cap B \cap C)$
region 3 represents $(A \cap C) \setminus (A \cap B \cap C)$
region 4 represents $(B \cap C) \setminus (A \cap B \cap C)$
... ...

Example 14

In the above diagram, suppose we are asked to determine the regions corresponding to the following subsets:

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

Then

$B \cup C$	is represented by regions			1, 2, 3, 4, 6, 7
$A \cap (B \cup C)$	...	...	...	1, 2, 3
$A \cap B$	...	...	...	1, 2
$A \cap C$	...	...	...	1, 3
$(A \cap B) \cup (A \cap C)$	...	...	...	1, 2, 3

We notice that, from our Venn diagram representation,

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

Similarly we may conclude that

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

A rigorous proof is given in Theorem 2.

Theorem 2

Let A, B, C be sets. Then

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

(These results are called the **Distributive Laws** for sets.)

Proof

We prove 1, the proof of 2 is similar.

Since $B \subseteq B \cup C$ and $C \subseteq B \cup C$, we have $A \cap B \subseteq A \cap (B \cup C)$ and $A \cap C \subseteq A \cap (B \cup C)$ from which

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

We now have to prove that $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$. For this part of the proof we consider elements and not simply subsets. Therefore let $x \in A \cap (B \cup C)$. Then $x \in A$ and $x \in B \cup C$ and so x is in either B or C. If we suppose $x \in B$ then $x \in B$ and $x \in A$ from which we have $x \in A \cap B$ and so $x \in (A \cap B) \cup (A \cap C)$. The alternative supposition that $x \in C$ leads to the same conclusion. Consequently we have

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

This completes the proof. □

The next result (see Example 11) gives the so-called De Morgan Laws, after A. De Morgan (1806–71).

Theorem 3 De Morgan Laws

Let A, B be sets. Then the following statements hold.

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

Proof

We prove 1, the proof of 2 is similar.

Let $x \in (A \cap B)'$. Then $x \notin (A \cap B)$. This means that $x \notin A$ or $x \notin B$. If $x \notin A$ then $x \in A'$ and so $x \in A' \cup B'$. If $x \notin B$ then $x \in B'$ and so $x \in A' \cup B'$. Thus $(A \cap B)' \subseteq A' \cup B'$.

Let $x \in A' \cup B'$. Then $x \in A'$ or $x \in B'$. If $x \in A'$ then $x \notin A$ and so certainly $x \notin A \cap B$ and similarly if $x \in B'$ then $x \notin A \cap B$. Thus $x \notin A \cap B$ and so $x \in (A \cap B)'$. Thus $A' \cup B' \subseteq (A \cap B)'$. Hence we obtain the desired result. $\square$

Many of the sets with which we shall be concerned will be infinite, but for finite sets we now introduce some counting techniques.

If A and B are both finite sets then certainly $A \cup B$ is finite since there cannot be more elements than in A and B considered separately. We shall derive a formula for the number of distinct elements in $A \cup B$. We recall that $|A|$ is the number of elements in A (Definition 2).

Theorem 4

Let A and B be finite sets. Then $A \cup B$ is a finite set and

$$|A \cup B| = |A| + |B| - |A \cap B|.$$

Proof

Let us examine the Venn diagram for $A \cup B$. As we remarked

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

are disjoint unions of subsets of A or B. These subsets are necessarily finite and so, by obvious (and legitimate) counting, we have

$$\begin{aligned} |A| &= |A \setminus B| + |A \cap B|, \\ |B| &= |B \setminus A| + |A \cap B| \end{aligned}$$

and also

$$\begin{aligned} |A \cup B| &= |A \setminus B| + |B \setminus A| + |A \cap B| \\ &= [|A| - |A \cap B|] + [|B| - |A \cap B|] + |A \cap B| \\ &= |A| + |B| - |A \cap B|. \end{aligned}$$

$\square$

The following two examples illustrate the use of this formula.

Example 15

Let $A = \{a, b, c, d\}, B = \{a, c, e, f, g\}$.
Then $A \cup B = \{a, b, c, d, e, f, g\}, A \cap B = \{a, c\}$. As we expect

$$|A \cup B| = 7 = 4 + 5 - 2 = |A| + |B| - |A \cap B|.$$

Example 16

We are told that in a party of 95 English-speaking schoolchildren there are 20 who speak only English, 60 who can speak French and 24 who can speak German. We require to determine how many speak both French and German.

The 'universal set' consists of 95 schoolchildren. We let F and G be the subsets consisting of those schoolchildren who can speak French and German respectively. Then $|F| = 60$, $|G| = 24$. $F \cup G$ is the subset of those schoolchildren who speak either French or German. Since 20 speak only English we have

$$|F \cup G| = 95 - 20 = 75.$$

$$\text{Then } |F \cup G| = |F| + |G| - |F \cap G|$$

$$\text{and so } 75 = 60 + 24 - |F \cap G|.$$

$$\text{Thus } |F \cap G| = 9.$$

This says that precisely 9 schoolchildren can speak both French and German.

We may extend Theorem 4 to consider three or more sets, but we confine our extension to the case of three sets.

Theorem 5

Let A, B and C be finite sets. Then $A \cup B \cup C$ is a finite set and

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|.$$

Proof

We apply Theorem 4. We note that

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

Then, on letting $P = B \cup C$, we have

$$\begin{aligned}
|A \cup B \cup C| &= |A \cup P| \\
&= |A| + |P| - |A \cap P| \\
&= |A| + |B \cup C| - |A \cap P| \\
&= |A| + |B| + |C| - |B \cap C| - |A \cap (B \cup C)| \\
&= |A| + |B| + |C| - |B \cap C| - |(A \cap B) \cup (A \cap C)| \text{ (by Theorem 2)} \\
&= |A| + |B| + |C| - |B \cap C| - [|A \cap B| + |A \cap C| \\
&\quad - |(A \cap B) \cap (A \cap C)|] \\
&= |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|.
\end{aligned}$$

□

Applications of this result are often made to problems of which the following is typical.

Example 17

In a gathering of 136 fairly athletic students, 92 engage in gymnastics, 68 are swimmers and 78 are tennis players. Of the 136 students, 41 do gymnastics and swim, 43 do gymnastics and play tennis and 24 swim and play tennis. If 4 students participate neither in gymnastics, swimming nor tennis, how many indulge in all three of these sporting activities? How many play tennis but do not have other sporting activities?

We have to reduce the situation of the problem to manageable mathematics.

Let U be the set of 136 students,
let G be the set of gymnasts,
let S be the set of swimmers, and
let T be the set of tennis players.

We are given the information that

$$|G| = 92, |S| = 68, |T| = 78, |G \cap S| = 41, |G \cap T| = 43, |S \cap T| = 24.$$

We are also given that $|U \setminus (G \cup S \cup T)| = 4$ from which we deduce that

$$\begin{aligned}
|G \cup S \cup T| &= |U| - |U \setminus (G \cup S \cup T)| \\
&= 136 - 4 = 132
\end{aligned}$$

Now applying Theorem 5 we have

$$
\begin{aligned}
132 = |G \cup S \cup T| &= |G| + |S| + |T| - |G \cap S| - |G \cap T| + |G \cap S \cap T| \\
&= 92 + 68 + 78 - 41 - 43 - 24 + |G \cap S \cap T|.
\end{aligned}
$$

Hence $|G \cap S \cap T| = 2$, and so 2 students engage in all three activities.

The number of students who play tennis but have no other sporting activities is given by $|T \setminus (G \cup S)|$. The easiest way to determine this number is by means of a Venn diagram in which $|G \cap S \cap T| = 2$, a is the number of students who are gymnasts and play tennis but do not swim, and b is the number of students who swim and play tennis but are not gymnasts.

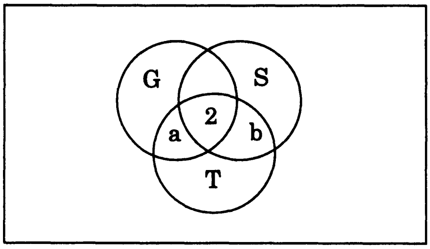

Figure 1.7.

We have

$$
\begin{aligned}
a = |(G \cap T) \setminus S| &= |(G \cap T) \setminus (G \cap S \cap T)| \\
&= |G \cap T| - |G \cap S \cap T| \\
&= 43 - 2 \\
&= 41.
\end{aligned}
$$

Similarly

$$
\begin{aligned}
b &= |(S \cap T) \setminus G| \\
&= 24 - 2 \\
&= 22.
\end{aligned}
$$

Then, from the diagram, the number of students who play tennis but have no other sports is

$$
\begin{aligned}
|T| - a - b - 2 &= 78 - 41 - 22 - 2 \\
&= 13.
\end{aligned}
$$

Exercises 1.2

1. Let A and B be sets. Establish the De Morgan Law
$$(A \cup B)' = A' \cap B'$$
   (i) by a Venn diagram,
   (ii) by a set-theoretic proof.

2. Let A, B and C be sets. Establish the Distributive Law
$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$
   (i) by a Venn diagram,
   (ii) by a set-theoretic proof.

3. Let A, B and C be sets. Prove, by constructing an appropriate example (often called a counter-example) that the result
$$A \cup (B \cap C) = (A \cup B) \cap C$$
does not necessarily hold. If $A \subseteq C$ does the result hold? Is the condition $A \subseteq C$ necessary and sufficient for the result to hold?

4. In a certain village of 1000 well-educated people, 250 read the *Economist*, 411 read the *Bangkok Post* and 315 read the *Straits Times*. Of these people, 72 read the *Economist* and the *Bangkok Post*, 51 read the *Economist* and the *Straits Times* and 31 read the *Bangkok Post* and the *Straits Times*. If only one person reads all three of the publications, how many do not read any of the publications?

5. A party of 200 schoolchildren is investigated with regard to likes and dislikes of three items, namely, ice cream, sweets and fizzy lemonade. It is found that of those children who like ice cream only 7 dislike sweets. 110 children like sweets and 149 like fizzy lemonade. 80 children like both sweets and fizzy lemonade and 36 like both ice cream and lemonade. If 31 children consume all three items avidly, how many children like none of these items?

1.3 Mappings

In our mathematics we have probably evaluated expressions such as x^2, $\sin x$, and $\sqrt{x^2 - 4}$ for given 'values of x'. We may have described these expressions loosely as being functions of x. While this description is somewhat vague it does encapsulate a concept which we would wish to make rather more precise. For a given value of x we expect unique evaluations of the expressions; thus

$(-2)^2 = 4$, $\sin \pi/4 = 1/\sqrt{2}$, but it is not permissible to put $x = 1$ in $\sqrt{x^2 - 4}$ if we wish to obtain a real square root. This suggests that we have to specify how the 'values of x' may be chosen. We begin to appreciate that, in each case, we need to specify a set of elements and to have the function defined exactly on this set. We make the following definition.

Definition 11

Let A and B be sets. Let there be a rule or prescription, denoted by f, by which to each element a of A there is assigned a unique element, denoted by $f(b)$, of B. Then the rule is said to be a **mapping** or **map** or **function** from A to B. We write

$$a \to f(a) \quad (a \in A)$$

and, to indicate that f is a mapping on sets, we use both of the following notations:

$$f : A \longrightarrow B \text{ and } A \xrightarrow{f} B.$$

A is called the **domain** of f and B is called the **codomain** of f.

[The designations 'map' and 'function' are perhaps more common in topology and analysis respectively. We shall use the term 'mapping'.]

For $a \in A$, $f(a)$ is called the **image** of a and, likewise, the subset of B given as

$$\{f(a) | a \in A\}$$

is called the **image** of A or, sometimes, the **range** of f. We also denote this subset by $f(A)$. Finally we note that $f(\varnothing) = \varnothing$.

Example 18

Let $A = \{a, b, c\}$ and $B = \{0, 1\}$. We define a mapping f where $f : A \to B$ by letting

$$f(a) = 0, f(b) = 1, f(c) = 1.$$

Then f has domain A, codomain B and range B. We define a second mapping g where $g : A \to B$ by letting

$$g(a) = 1, g(b) = 1, g(c) = 1.$$

Then g has domain A, codomain B and range $\{1\}$. We note that f and g are unequal since, for example,

$$f(a) = 0 \neq 1 = g(a).$$

The condition under which two mappings are equal should be fairly obvious but, for the sake of completeness, we state the condition formally.

Remark

Two mappings f and g are **equal** if and only if f and g have the same domain A and $f(a) = g(a)$ for all $a \in A$.

Example 19 (Continued from Example 3)

Let A be the set of the colours of the rainbow. Let $B = \{1, 2, 3, 4, 5, 6, 7\}$. We define a mapping f where $f : A \to B$ by the rule that the image of a given colour of the rainbow is the number of letters in that colour. We need not go further to specify the mapping although, in fact, we have

$$f(\text{red}) = 3, f(\text{orange}) = 6, f(\text{yellow}) = 6, f(\text{green}) = 5,$$
$$f(\text{blue}) = 4, f(\text{indigo}) = 6, f(\text{violet}) = 6.$$

We now introduce certain important sets of which we shall have more to say in the next chapter.

Notation

The set of **natural numbers**, which is also the set of **strictly positive integers**, is denoted by $\mathbb{N}$ ($\mathbb{N}$ for 'natural'),

$$\mathbb{N} = \{1, 2, 3, \ldots\}.$$

The set of **integers** is denoted by $\mathbb{Z}$ ($\mathbb{Z}$ for 'Zahl', the German word for 'number'),

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

The set of **rational numbers**, which is also the set of quotients of integers, is denoted by $\mathbb{Q}$ ($\mathbb{Q}$ for 'quotient'),

$$\mathbb{Q} = \{m/n | m, n \in \mathbb{Z}, n \neq 0\}.$$

Thus $\mathbb{Q}$ consists of all fractions such as $\frac{1}{2}, \frac{2}{3}, \frac{-15}{8}$.

The set of **real numbers** is denoted by $\mathbb{R}$ and the set of **complex numbers** is denoted by $\mathbb{C}$,

$$\mathbb{C} = \{a + ib : a, b \in \mathbb{R}\}.$$

Evidently

$$\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}.$$

A real number which is not rational is said to be **irrational**, $\mathbb{R} \setminus \mathbb{Q}$ is the set of irrational numbers.

We give three examples of mappings involving these sets before giving some useful terminology for describing mappings.

Examples 20

1. The mapping $f : \mathbb{N} \to \{-1, 1\}$ given by
$$f(n) = (-1)^n \quad (n \in \mathbb{N})$$
has domain $\mathbb{N}$, codomain $\{-1, 1\}$ and range $\{-1, 1\}$.
2. The mapping $f : R \to R$ given by
$$f(x) = x^2 + 1 \quad (x \in \mathbb{R})$$
has domain $\mathbb{R}$, codomain $\mathbb{R}$ and range $\{y \,|\, y \geq 1\}$.
3. The mapping $f : \mathbb{N} \to \mathbb{Q}$ given by
$$f(n) = \tfrac{1}{2}n \quad (n \in \mathbb{N})$$
has domain $\mathbb{N}$, codomain $\mathbb{Q}$ and range $\{\frac{1}{2}, 1, \frac{3}{2}, 2, \ldots\} = \mathbb{N} \cup \{\frac{n}{2} \,|\, n \in \mathbb{N}\}$.

Definition 12

Let A and B be sets. Let $f : A \to B$ be a mapping.

(i) The mapping f is said to be **injective,** or **one–one**, if whenever $f(a_1) = f(a_2)$ for $a_1, a_2 \in A$ then necessarily $a_1 = a_2$.

(ii) The mapping f is said to be **surjective** or **onto** if for each $b \in B$ there exists $a \in A$ such that $f(a) = b$.

(iii) The mapping f is said to be **bijective** or **one–one and onto** if f is both injective and surjective.

Examples 21

1. Let $A = \{a, b, c\}$ and $B = \{p, q\}$. We define $f : A \to B$ by
$$f(a) = p,\ f(b) = p,\ f(c) = p.$$
Then f is not injective since $f(a) = f(b)$ but $a \neq b$. We also have that f is not surjective since $f(A) = \{p\} \neq B$.
2. Let $A = \{a, b\}$ and $B = \{p, q, r\}$. We define $f : A \to B$ by
$$f(a) = p,\ f(b) = q.$$
Then f is injective since $f(a) \neq f(b)$ but is not surjective since $f(A) = \{p, q\} \neq B$.
3. Let $A = \{a, b, c\}$ and $B = \{p, q\}$. We define
$$f : A \to B \text{ by } f(a) = p,\ f(b) = p,\ f(c) = q.$$
Then f is not injective since $f(a) = f(b)$ but is surjective since $f(A) = \{p, q\} = B$.

[The reader may begin to suspect (correctly) that a bijective mapping exists between two finite sets if and only if they have the same number of elements. In particular the reader may rightly conclude that a bijective mapping cannot exist between a finite set and a proper subset; for infinite sets the situation is less restrictive, as the next example shows.]

4. Let $2\mathbb{N}$ denote the set of strictly positive even integers,

$$2\mathbb{N} = \{2n | n \in \mathbb{N}\}.$$

Now $2\mathbb{N}$ is a proper subset of $\mathbb{N}$ but, nevertheless, the mapping $f : \mathbb{N} \to 2\mathbb{N}$ given by

$$f(n) = 2n \quad (n \in \mathbb{N})$$

is bijective.

5. A mapping f is defined on $\mathbb{N}$ by

$$f(n) = \begin{cases} n & (n \text{ odd}) \\ \frac{1}{2}n & (n \text{ even}). \end{cases}$$

Suppose we are asked to describe f. We note first that f is defined so that $f : \mathbb{N} \to \mathbb{N}$. Then f is not injective since, for example, $f(3) = 3 = f(6)$. But f is surjective since if $k \in \mathbb{N}$ then $f(2k) = k$.

Frequently we have to consider the effect of applying mappings successively. More precisely we have the following definition.

Definition 13

Let A, B and C be sets and let $f : A \to B$ and $g : B \to C$ be given mappings. We have

$$A \xrightarrow{f} B \xrightarrow{g} C$$

where the range of f is a subset of the domain of g. Then for each $a \in A$ we have a mapping, denoted by $g \circ f$, called the **circle-composition** of the mappings g and f and given by

$$(g \circ f)(a) = g(f(a))$$

in which we first apply the mapping f to $a \in A$ and then apply the mapping g to $f(a) \in B$. If no ambiguity will arise we often write gf for $g \circ f$.

Theorem 6

Let A, B and C be sets and let $f : A \to B$ and $g : B \to C$ be mappings.

1. If f and g are surjective then $g \circ f$ is surjective.
2. If f and g are injective then $g \circ f$ is injective.
3. If f and g are bijective then $g \circ f$ is bijective.

Proof

We prove 1 and leave 2 to be proved in subsequent Exercises. 1 and 2 imply 3. Let $c \in C$. Then since g is surjective we have $b \in B$ such that $g(b) = c$. Since f is surjective we have $a \in A$ such that $f(a) = b$. Then

$$(g \circ f)(a) = g(f(a)) = g(b) = c$$

and so $g \circ f$ is surjective. □

Examples 22

1. Let $A = \{a, b, c, d\}$, $B = \{1, 2, 3\}$, $C = \{p, q, r, s\}$. Let mappings f, g be defined by $f(a) = 1$, $f(b) = 1$, $f(c) = 2$, $f(d) = 3$, $g(1) = p$, $g(2) = r$, $g(3) = r$. Then we have

$$A \xrightarrow{f} B \xrightarrow{g} C$$

   with, for example,

$$(g \circ f)(b) = g(f(b)) = g(1) = p,$$

$$(g \circ f)(d) = g(f(d)) = g(3) = r.$$

2. Let mappings f and g be defined by

$$f(x) = \sin x \quad (x \in \mathbb{R}), \qquad g(x) = x^2 \quad (x \in \mathbb{R}).$$

   Then we may form $g \circ f$ and also $f \circ g$:

$$\mathbb{R} \xrightarrow{f} \mathbb{R} \xrightarrow{g} \mathbb{R},$$

$$\mathbb{R} \xrightarrow{g} \mathbb{R} \xrightarrow{f} \mathbb{R},$$

   Now

$$(g \circ f)(x) = g(f(x)) = g(\sin x) = (\sin x)^2 = \sin^2 x$$

   but

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

$g \circ f$ and $f \circ g$ have the same domain but are different mappings since it is not true, contrary to an occasional misguided belief, that $\sin^2 x = \sin x^2$ for all $x \in \mathbb{R}$.

Consider the case of four sets A, B, C, D and three mappings f, g, h where $f : A \to B$, $g : B \to C$ and $h : C \to D$.

We may construct the mappings $g \circ f$ and $h \circ g$ and then the further compositions $h \circ (g \circ f)$ and $(h \circ g) \circ f$, giving the pictures below.

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[rr, bend left, "g \circ f"] \arrow[rrr, bend right, "h \circ (g \circ f)"'] & B \arrow[r, "g"] & C \arrow[r, "h"] & D \end{tikzcd} \qquad \begin{tikzcd} A \arrow[r, "f"] \arrow[rrr, bend right, "(h \circ g) \circ f"'] & B \arrow[r, "g"] \arrow[rr, bend left, "h \circ g"] & C \arrow[r, "h"] & D \end{tikzcd}$$

Figure 1.8.

Then $h \circ (g \circ f)$ and $(h \circ g) \circ f$ are both mappings from A to D but they have been constructed differently. Could they be equal?

We consider a specific example before proving the general result.

Example 23

Let f, g, h be the mappings given by

$$f(x) = x^2 + 1 \quad (x \in \mathbb{Z}),$$

$$g(n) = \frac{2}{3}n \quad (n \in \mathbb{N}),$$

$$h(t) = \sqrt{t^2 + 1} \quad (t \in \mathbb{Q}),$$

and so,

$$\mathbb{Z} \xrightarrow{f} \mathbb{N} \xrightarrow{g} \mathbb{Q} \xrightarrow{h} \mathbb{R}$$

But

$$(g \circ f)(x) = g(f(x)) = g(x^2+1) = \frac{2}{3}(x^2+1) \quad (x \in \mathbb{Z}),$$

$$[h \circ (g \circ f)](x) = h\left(\frac{2}{3}(x^2+1)\right) = \sqrt{\left(\frac{2}{3}(x^2+1)\right)^2 + 1},$$

$$(h \circ g)(n) = h(g(n)) = h\left(\frac{2}{3}n\right) = \sqrt{\left(\frac{2}{3}n\right)^2 + 1} \quad (n \in \mathbb{N}),$$

$$[(h \circ g) \circ f](x) = (h \circ g)(f(x)) = (h \circ g)(x^2+1) = \sqrt{\left(\frac{2}{3}(x^2+1)\right)^2 + 1} \quad (x \in \mathbb{Z}).$$

Thus

$$[h \circ (g \circ f)](x) = [(h \circ g) \circ f](x) \quad (x \in \mathbb{Z})$$

from which

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

Theorem 7 Associativity of Circle-Composition

Let A, B, C, D be sets and let f, g, and h be mappings such that

$$f : A \to B,\ g : B \to C,\ h : C \to D.$$

Then

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

Proof

The proof simply entails repeated and careful application of Definition 13. Let $a \in A$. Then

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

and

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

Thus

$$[h \circ (g \circ f)](a) = [(h \circ g) \circ f](a)$$

and since a is arbitrary

$$h \circ (g \circ f) = (h \circ g) \circ f. \qquad \square$$

We may now write, unambiguously, $h \circ g \circ f$ to mean either of the compositions $h \circ (g \circ f)$ or $(h \circ g) \circ f$.

Remark

Mappings may appear to be necessary but somewhat humdrum objects of study. However particular mappings may give rise to curious problems. Consider, for example, the mapping $f : \mathbb{N} \to \mathbb{N}$ given by

$$f(n) = \begin{cases} \frac{1}{2}n & (n \text{ even}) \\ \frac{1}{2}(3n+1) & (n \text{ odd}). \end{cases}$$

Thus $f(26) = 13$, $f(25) = \frac{1}{2}(75+1) = 38$. Suppose we iterate this mapping several times and, by way of illustration, we follow the effect of the iterations on the number 10. Then

$$\begin{aligned} f(10) &= 5, \\ (f \circ f)(10) &= f(5) = 8, \\ (f \circ f \circ f)(10) &= f(8) = 4, \\ (f \circ f \circ f \circ f)(10) &= f(4) = 2, \\ (f \circ f \circ f \circ f \circ f)(10) &= 1. \end{aligned}$$

After five iterations on 10 the number 1 appears. The reader may care to verify that commencing with 65 there are 19 iterations before 1 first appears. Other integers may be tried at random as test cases, but the reader is advised to cultivate patience as the number of iterations before 1 first appears may be quite large.

The conjecture, that for any $n \in \mathbb{N}$ and for sufficiently many iterations the number 1 always appears, remains to be proved or disproved.

Exercises 1.3

1. Let A, B, C be the sets $\{a, b, c\}$, $\{p, q, r\}$, $\{0, 1\}$ respectively. Let the mappings $f : A \to B$ and $g : B \to C$ be defined by

$$f(a) = p, f(b) = f(c) = q, g(p) = 0, g(q) = 1, g(r) = 0.$$

Evaluate $(g \circ f)(a), (g \circ f)(b), (g \circ f)(c)$.

2. Let A, B, C, D be sets and let p, q, r, s be mappings such that

$$p : A \to B, q : B \to C, r : A \to B, s : D \to C.$$

Which of the following are defined: $q \circ p$, $p \circ q$, $p \circ r$, $p \circ s$, $r \circ s$, $q \circ s$?

3. Let f, g, h be mappings of $\mathbb{Z}$ into $\mathbb{Z}$ given by

$$f(n) = 2n,\ g(n) = 3n + 5,\ h(n) = -6n \quad (n \in \mathbb{Z}).$$

Which of the following pairs of mappings are equal: $f \circ g$, $g \circ f$; $f \circ h$, $h \circ f$; $g \circ h$, $h \circ g$?

4. Let A, B and C be sets and let $f : A \to B$ and $g : B \to C$ be mappings.

   (i) If f and g are injective prove that $g \circ f$ is injective.

   (ii) If $g \circ f$ is injective, are g and f injective?

   (iii) If $g \circ f$ is surjective, are g and f surjective?

5. Let X, Y be sets and let $f : X \to Y$ be a mapping. Let A, B be subsets of X.

   (i) If $A \subseteq B$ prove that $f(A) \subseteq f(B)$.

   (ii) Prove that $f(A \cup B) = f(A) \cup f(B)$.

   (iii) Prove that $f(A \cap B) \subseteq f(A) \cap f(B)$.

6. Let A be the subset of $\mathbb{Z}$ consisting of the even integers and let B be the subset of $\mathbb{Z}$ consisting of the odd integers. Let a mapping $f : \mathbb{Z} \to \mathbb{Z}$ be defined by

$$f(n) = n^2 - 3n + 5 \quad (n \in \mathbb{Z}).$$

Prove that $3 \in f(A) \cap f(B)$ and so deduce that $f(A \cap B) \neq f(A) \cap f(B)$.

1.4 Equivalence Relations

In the context of humans, animals and plants, the notion of relationship is all pervasive; two individuals are regarded as 'related' if they share a common parent, grandparent or even a more distant ancestor. Thus cousins are said to be related but we would not normally regard a cat and a dog as being related. In these illustrations we encounter the idea of a universal set, whether composed of humans or of domestic animals, and of the relationship which members or elements of the set may bear to one another under some particular criterion. Since the underlying concept of relationship is very useful in mathematics we discuss a more mathematical example before proceeding to a precise definition.

Example 24

We consider a set A and a relationship which exists between some pairs of elements of A. Let X be a set and let $f : A \to X$ be a mapping. We shall say that elements a and b of A are 'related' if $f(a) = f(b)$. By this definition any two elements of A may or may not be related.

For convenience we write for $a, b \in A$, $a \sim b$ if and only if a, b are related; the presence of the symbol $\sim$ (pronounced 'twiddles') denoting that a and b are related.

We note three obvious facts:

1. For all $a \in A$, a is related to a since $f(a) = f(a)$ implies $a \sim a$ (for all $a \in A$).
2. If $a, b \in A$ are such that a is related to b, then b is related to a, since $a \sim b$ implies $f(a) = f(b)$ and so $f(b) = f(a)$ and $b \sim a$.
3. If a, b, $c \in A$ are such that a is related to b and b is related to c, then a is related to c since $a \sim b$ implies $f(a) = f(b)$ and $b \sim c$ implies $f(b) = f(c)$ from which $f(a) = f(b) = f(c)$ and so $a \sim c$.

The definition we seek basically repeats the conclusions of this example.

Definition 14

Let A be a set. A relation, denoted by $\sim$, is defined between some pairs of elements of A subject to the following (named) conditions.

1. For all $a \in A$, $a \sim a$ (reflexivity).
2. If $a, b \in A$ are such that $a \sim b$ then also $b \sim a$ (symmetry).
3. If a, b, $c \in A$ are such that $a \sim b$ and $b \sim c$ then also $a \sim c$ (transitivity).

A relation $\sim$ on A which is reflexive, symmetric and transitive as above, is called an **equivalence relation**.

Symbols R, ρ, σ are frequently used to denote equivalence relations.

We note in passing that the relation of the previous example is an equivalence relation.

Examples 25

1. On any set A the relation of equality is an equivalence relation since we have $a = a$ for all $a \in A$, we certainly have $a = b$ implies $b = a(a, b \in A)$ and if $a = b$ and $b = c(a, b, c \in A)$ then $a = c$.

   An equivalence relation between the elements of a set generalizes the notion of equality for elements of the set.

2. On $\mathbb{Z}$ a relation $\sim$ is defined by $a \sim b$ if and only if a, b are both even or a, b are both odd.

   Thus $4 \sim 4$ and $5 \sim 5$ but we do not have $4 \sim 5$.

   Now, in general, $a \sim a$ and certainly $a \sim b$ implies $b \sim a$ $(a, b \in \mathbb{Z})$. Suppose now $a \sim b$ and $b \sim c$ $(a, b, c \in \mathbb{Z})$. Then, if b is even, a and c must also be even and $a \sim c$, whereas if b is odd, a and c must also be odd and $a \sim c$. Thus $\sim$ is an equivalence relation on $\mathbb{Z}$.

   Notice that we could have defined this equivalence relation by means of a mapping $f : \mathbb{Z} \to \{0, 1\}$ for which

$$f(n) = \begin{cases} 0 & (n \text{ even}) \\ 1 & (n \text{ odd}) \end{cases} \quad (n \in \mathbb{Z}).$$

3. Let S be the set of all words in a given English dictionary. Define two words to be related by ρ if they begin with the same letter and end with the same letter. Thus we have 'atom ρ alum', 'pleasure ρ perseverance' and 'a ρ aroma'. Then ρ is easily seen to be an equivalence relation on S.

4. Let S be the set of points composing the circumference of a given circle. For P, $Q \in S$ define a relation σ by $P \sigma Q$ if and only if there is a diameter on which P, Q are points. Thus if $P \sigma Q$ then either P, Q coincide or P, Q are at opposite ends of a diameter. Simple geometrical considerations show that σ is an equivalence relation.

5. Let X be the set $\mathbb{Q} \times \mathbb{Q}$ of ordered pairs of rational numbers.

   For $a = (a_1, a_2) \in \mathbb{Q} \times \mathbb{Q}$ and $b = (b_1, b_2) \in \mathbb{Q} \times \mathbb{Q}$ we define a relation $\sim$ by

$$a \sim b \text{ if and only if } a_1 + a_2 = b_1 + b_2.$$

   We claim that $\sim$ is an equivalence relation on X. Certainly $\sim$ is reflexive.

If for some $a, b \in X$ we have $a \sim b$ then $a = (a_1, a_2)$, $b = (b_1, b_2)$, where $a_i, b_i \in \mathbb{Q}$ $(i = 1, 2)$ and $a_1 + a_2 = b_1 + b_2$. But then $b_1 + b_2 = a_1 + a_2$ and so $b \sim a$ and $\sim$ is symmetric.

Suppose now for some $a, b, c \in X$ we have $a \sim b$ and $b \sim c$. Then writing $a = (a_1, a_2)$, $b = (b_1, b_2)$, $c = (c_1, c_2)$ we have $a_1 + a_2 = b_1 + b_2 = c_1 + c_2$ and so $a \sim c$ and $\sim$ is transitive. Hence $\sim$ is an equivalence relation.

6. A relation, ρ, is defined on $\mathbb{Q}$ by letting, for $a, b \in \mathbb{Q}$, $a\rho b$ if and only if we have $a - b \in \mathbb{Z}$. By this relation we have

$$\frac{43}{19}\rho\frac{5}{19} \text{ as } \frac{43}{19} - \frac{5}{19} = \frac{38}{19} = 2 \in \mathbb{Z}$$

but

$$\frac{1}{2}\rho\frac{1}{3} \text{ is false as } \frac{1}{2} - \frac{1}{3} = \frac{5}{6} \notin \mathbb{Z}.$$

We may prove that ρ is an equivalence relation as follows:

(i) For all $a \in \mathbb{Q}$, $a - a = 0 \in \mathbb{Z}$ and so $a \sim a$ (reflexivity).

(ii) If for some $a,\ b \in \mathbb{Q}$, $a \sim b$ then $a - b \in \mathbb{Z}$ which immediately implies that $b - a = -(a - b) \in \mathbb{Z}$ and so $b \sim a$ (symmetry).

(iii) If for some $a,\ b,\ c \in \mathbb{Q}$, $a \sim b$ and $b \sim c$ then evidently $a - b \in \mathbb{Z}$ and $b - c \in \mathbb{Z}$ from which $a - c = (a - b) + (b - c) \in \mathbb{Z}$ and so $a \sim c$ (transitivity).

It is sometimes important, in regard to a set of conditions specifying a mathematical entity such as an equivalence relation, to know whether the stipulated conditions are themselves independent or not. We show that the three conditions of reflexivity, symmetry and transitivity for an equivalence relation are independent by exhibiting three examples in each of which two of the conditions are satisfied but not the remaining condition.

Examples 26

1. Let a relation $\sim$ be defined on $\mathbb{Z}$ by $a \sim b$ if and only if $ab \neq 0$ $(a, b \in \mathbb{Z})$. Then the relation is symmetric since $a \sim b$ implies $ab \neq 0$ and so $ba \neq 0$. Thus $b \sim a$ $(a, b \in \mathbb{Z})$.

   The relation is also transitive since $a \sim b$, $b \sim c$ implies $ab \neq 0$, $bc \neq 0$. Hence $a \neq 0$, $b \neq 0$, $c \neq 0$ and thus $ac \neq 0$ giving $a \sim c$.

   On the other hand the relation is not reflexive since we do not have $a \sim a$ for all $a \in \mathbb{Z}$, in particular we do not have $0 \sim 0$.

2. The relation of inequality, $\leq$, on $\mathbb{R}$ is reflexive and transitive since we have, for all $a \in \mathbb{R}$, $a \leq a$ and if $a \leq b$, $b \leq c$ then $a \leq c$ $(a, b, c \in \mathbb{R})$. We cannot infer from $a \leq b$ $(a, b \in \mathbb{R})$ that $b \leq a$ and so this relation is not symmetric.
3. Let a relation $\sim$ be defined on $\mathbb{Z}$ by $a \sim b$ if and only if 2 divides $a - b$ or 3 divides $a - b$. Such a relation is not transitive since, for example,

   $7 \sim 5$ since $7 - 5 = 2$

   and $5 \sim 2$ since $5 - 2 = 3$

   but $7 \sim 2$ is false since $7 - 2 = 5$ which is divisible by neither 2 nor 3.

   But the relation is reflexive since for all $a \in Z$, $a - a = 0$ and so $a \sim a$ and the relation is symmetric since $a \sim b$ $(a, b \in \mathbb{Z})$ implies that $a - b$, and thus $b - a$, is divisible by 2 or by 3 and so $b \sim a$.

We may consider the totality of the inhabitants of a given town as being distributed into the families which dwell in the town. Any two members of the same family are somehow related but no two members of different families are related. An inhabitant of the town belongs to only one family and so identifies uniquely the family to which he or she belongs. In a similar way a set with an equivalence relation will be seen to be the union of disjoint subsets called equivalence classes, each equivalence class consisting (like a family) of all elements which are related to one another and each equivalence class will be uniquely identifiable by any element belonging to it.

We make these ideas more precise.

Definition 15

Let S be a non-empty set with an equivalence relation $\sim$. Let $a \in S$. The subset S_a of S given by

$$S_a = \{x \in S : x \sim a\}$$

is said to be the **equivalence class** determined by, or containing, a (note that as $a \sim a$, $a \in S_a$).

We now prove a result which we shall have frequent occasion to use.

Theorem 8

In the notation of Definition 15 the following hold:

1. $S = \bigcup_{a \in S} S_a$.
2. $S_a = S_b$ if and only if $a \sim b$ $(a, b \in S)$.
3. Either $S_a = S_b$ or $S_a \cap S_b = \varnothing$ $(a, b \in S)$.

Proof

1. Since $a \in S_a$ it follows that $S \subseteq \bigcup_{a \in S} S_a$ and so $S = \bigcup_{a \in S} S_a$.
2. If $S_a = S_b$ then $a \in S_b$ and so $a \sim b$. Conversely suppose $a \sim b$. We prove that $S_a \subseteq S_b$. Let $x \in S_a$. Then $x \sim a$ and $a \sim b$ implies that $x \sim b$ and so $x \in S_b$. Thus $S_a \subseteq S_b$. Since, by symmetry, $b \sim a$ we also have $S_b \subseteq S_a$ and so $S_a = S_b$.
3. Suppose $S_a \cap S_b \neq \varnothing$. We show that $S_a = S_b$. Let $c \in S_a \cap S_b$ and so $c \sim a$ and $c \sim b$. But then $a \sim c$ and $c \sim b$ which implies, by transitivity, that $a \sim b$. By (ii) we conclude that $S_a = S_b$. □

It is a consequence of Theorem 8 that from the union $\bigcup_{a \in S} S_a$, on eliminating equivalence classes that formally coincide, we may write

$$S = \bigcup_{a \in T} S_a$$

where T is a subset of S such that S_a $(a \in T)$ are distinct, and $S_a \cap S_b = \varnothing$ $(a, b \in T, a \neq b)$. The non-empty set S is thereby expressed as a disjoint union of distinct equivalence classes.

Examples 27 (Continued from Examples 25)

We examine the examples immediately following Definition 14 to determine the appropriate equivalence classes.

1. With equality as the equivalence relation on a set each equivalence class consists of a single element.
2. There are two equivalence classes, namely the subset of $\mathbb{Z}$ consisting of the even integers and the subset of $\mathbb{Z}$ consisting of the odd integers.
3. The English alphabet has 26 letters: $a, b, c, \ldots, x, y, z$. Each word begins with, and ends with, one of these letters. We now define $26^2 = 676$ subsets each defined for any pair of letters of the alphabet as follows:

Let S_{aa} be the subset of all words beginning with a and ending with a.

Let S_{ab} be the subset of all words beginning with a and ending with b.

... ...

Let S_{zz} be the subset of all words beginning with z and ending with z.

The reader will immediately observe that some of the subsets $S_{aa}, S_{ab}, \ldots, S_{zz}$ are empty ($S_{zz} = \varnothing$ but, perhaps surprisingly, $S_{az} \neq \varnothing$). Any one of these subsets, if non-empty, is an equivalence class. S is the union of these subsets and, on omitting empty subsets, becomes a disjoint union of equivalence classes. (We leave it to the aspiring lexicographer to determine which subsets are non-empty.)

4. Every diameter determines an equivalence class consisting of the two end-points of the diameter.
5. For every $q \in \mathbb{Q}$ there is an equivalence class given by

$$X_q = \{(a_1, a_2) \in Q \times Q | a_1 + a_2 = q\}.$$

Each equivalence class is of this form.

We have seen that if a set admits an equivalence relation then that set is a disjoint union of particular subsets called equivalence classes. Conversely if a set is a disjoint union of subsets then we shall show that, correspondingly, an equivalence relation may be defined on the set. We are led to make the following definition.

Definition 16

Let S be a non-empty set. Let $\{S_\lambda : \lambda \in \Lambda\}$ be a collection, indexed by an index-set Λ, of non-empty subsets of S such that

1. $S_\lambda \cap S_\mu = \varnothing\ (\lambda, \mu \in \Lambda, \lambda \neq \mu)$ and
2. $\bigcup_{\lambda \in \Lambda} S_\lambda = S$.

The collection of subsets is said to form a **partition** of S.

Suppose we have a non-empty set S with a partition as above. For $a, b \in S$ define a relation $\sim$ by letting $a \sim b$ if and only if a, b belong to the same subset S_λ (say) of the partition. Thus any two elements in an S_λ are related but no element in S_λ is related to an element in S_μ $(\lambda \neq \mu)$. Then it may readily be verified that $\sim$ is an equivalence relation on S and that the equivalence classes are the subsets S_λ $(\lambda \in \Lambda)$. A partition therefore induces an equivalence relation and an equivalence relation induces a partition, subsets of the partition forming the equivalence classes of the equivalence relation.

Example 28

Let $S = \{a, b, c, d, e, f, g\}$. Let $S_1 = \{a, b, d\}$, $S_2 = \{c, g\}$, $S_3 = \{e, f\}$. Then the subsets S_1, S_2, S_3 form a partition $\{S_1, S_2, S_3\}$ of S. We define the corresponding equivalence relation $\sim$ on S as follows:

$$\begin{array}{lll} a \sim a, a \sim b, a \sim d, & c \sim c, & e \sim e, \\ b \sim a, b \sim b, b \sim d, & c \sim g, & e \sim f, \\ d \sim a, d \sim b, d \sim d, & g \sim c, & f \sim e, \\ & g \sim g, & f \sim f. \end{array}$$

Exercises 1.4

1. A relation ρ is defined on $\mathbb{R}$ by $a\rho b$ if and only if $a^2 = b^2$ $(a, b \in \mathbb{R})$. Prove that ρ is an equivalence relation on $\mathbb{R}$. Identify the equivalence classes.

2. A relation R is defined on $\mathbb{Z}$ by aRb if and only if $a - b$ is even $(a, b \in \mathbb{Z})$. Prove that R is an equivalence relation on $\mathbb{Z}$. Identify the equivalence classes.

3. A relation τ is defined on $\mathbb{Z}$ by $a\tau b$ if and only if $a - b$ is divisible by 6 $(a, b \in \mathbb{Z})$. Prove that τ is an equivalence relation and determine the equivalence classes.

4. What are the equivalence classes in Examples 25, no. 6 immediately following Definition 14?

5. Let Oxy be the two-dimensional coordinate plane. Let P, Q be points of Oxy.

   (i) P, Q are said to be related by σ if the points O, P, Q are collinear. Is σ an equivalence relation?

   (ii) P, Q are said to be related by τ if there exists a rotation about O which sends P into Q. Is τ an equivalence relation?

   Sketch, if possible, the equivalence classes.

6. How many distinct equivalence relations may be defined on a set of one, two, three or four elements?

7. A relation ρ is defined on $\mathbb{Z}$ by $a\rho b$ if and only if $a - b$ is divisible either by 5 or by 7 $(a, b \in \mathbb{Z})$. Is ρ an equivalence relation?

8. Let $S = \{a, b, c, x, y, z\}$. Two relations ρ, σ are defined on S as follows:

   $a\rho a$, $b\rho b$, $c\rho c$, $x\rho x$, $y\rho y$, $z\rho z$, $a\rho b$, $b\rho a$, $a\rho c$, $c\rho a$, $b\rho c$, $c\rho b$; $a\sigma a$, $b\sigma b$, $c\sigma c$, $x\sigma x$, $y\sigma y$, $z\sigma z$, $a\sigma x$, $x\sigma a$, $b\sigma y$, $y\sigma b$, $c\sigma z$, $z\sigma c$, $a\sigma y$, $y\sigma a$.

   Do either ρ or σ define an equivalence relation on S?

9. Let S be a set on which a relation $\sim$ is defined. The relation $\sim$ is symmetric and transitive. Loose thinking would suggest that $a \sim b$ $(a, b \in S)$ implies $b \sim a$ (by symmetry) and so $a \sim a$ (by transitivity) thus giving reflexivity, and consequently $\sim$ would be an equivalence relation. What is wrong with this loose thinking?

1.5 Well-ordering and Induction

The elements of the set $\mathbb{N}$, that is the set of strictly positive integers, may be written down in ascending order with a repeated inequality sign, thus:

$$1 < 2 < 3 < 4 < \dots$$

Let S be a non-empty subset of $\mathbb{N}$. Let $N \in \mathbb{N}$. From the integers $1, 2, \dots, N$ we may select that one which is least amongst these integers and which also belongs to S. Intuitively therefore we have the following principle which we shall accept as axiomatic.

Principle of Well-ordering in $\mathbb{N}$

Every non-empty subset S of $\mathbb{N}$ has a least integer in S.

It frequently happens that we have some assertion, proposition or statement $P(n)$ which depends on the particular integer n. The proposition may itself be true or false. We give three examples.

Examples 29

1. $1 + 2 + \dots + n = \frac{n}{2}(n+1) \quad (n \in \mathbb{N})$.
2. $2n + 1 \le 2^n \quad (n \in \mathbb{N})$.
3. $n^2 \le 2^n \quad (n \in \mathbb{N})$.

In each of these examples we have a statement that depends on n. We are not asserting the truth or falsity of the statement. Naturally, however, we wish to know whether the particular statement is true for all $n \in \mathbb{N}$ or, possibly, for all

$n \in \mathbb{N}$ greater than some fixed integer. We are led to the so-called Principle of Induction and to an obvious and convenient variant of this principle. We may derive the Principle of Induction from the Principle of Well-ordering but both, for present purposes, may be regarded as simply axiomatic or, indeed, as 'obvious'.

Principle of Induction

Let $P(n)$ be a proposition depending on the integer n. Suppose that

1. $P(1)$ is true and
2. if $P(k)$ is true then $P(k+1)$ is true (induction assumption).

Then $P(n)$ is true for all $n \in \mathbf{N}$.

Proof (may be omitted)

Let S be the subset of $\mathbb{N}$ of those integers n for which $P(n)$ is true. Then certainly $1 \in S$ and so $S \neq \emptyset$. Let $X = \mathbb{N} \setminus S$. We wish to show that $X = \emptyset$ and then $S = \mathbb{N}$. For the sake of argument suppose $X \neq \emptyset$. We apply the Principle of Well-ordering to X. Let N be the least integer in X. Now $N \neq 1$ since $1 \in S$ and so $N > 1$. Since N is the least integer in X, $N-1$ is an integer not in X and so $N-1 \in S$. But then $P(N-1)$ is true and so, by hypothesis 2, $P(N)$ is also true and $N \in S$. But this is a contradiction as $X \cap S = \emptyset$. Hence $X = \emptyset$ and $S = \mathbb{N}$. □

The Principle of Induction is often used in a modified version which we may also deem to be axiomatic.

Principle of Induction (Modified Version)

Let $P(n)$ be a proposition depending on the integer n. Suppose that

1. $P(1)$ is true and
2. if for each $m \leq k$, $P(m)$ is true, then $P(k+1)$ is true (induction assumption).

Then $P(n)$ is true for all $n \in \mathbb{N}$.

It sometimes happens that in either version of the Principle of Induction statement 1 that '$P(1)$ is true' is replaced by 'For some $N \in \mathbb{N}$, $P(N)$ is true' with corresponding changes to statement 2. In this circumstance the conclusion is that $P(n)$ is true for all $n \in \mathbb{N}$, $n \geq N$.

Let us consider further examples:

Examples 30

1. $P(n)$ is the statement

$$1+2+\ldots+n=\frac{n}{2}(n+1) \quad (n \in \mathbb{N}).$$

Certainly $P(1)$ is true since

$$1=\frac{1}{2}(1+1).$$

If we now make the induction assumption that $P(k)$ is true, then we suppose that

$$1+2+\ldots+k=\frac{k}{2}(k+1).$$

But this implies that

$$\begin{aligned} 1+2+\ldots+k+(k+1) &= \frac{k}{2}(k+1)+(k+1) \\ &= \frac{(k+1)}{2}(k+2) \\ &= \frac{(k+1)}{2}[(k+1)+1] \end{aligned}$$

and so we may assert that $P(k)$ implies $P(k+1)$. Hence we have for all $n \in \mathbb{N}$

$$1+2+\ldots+n=\frac{n}{2}(n+1).$$

2. $P(n)$ is the statement that

$$2n+1 \leq 2^n \quad (n \in \mathbb{N}).$$

Now $P(1)$ and $P(2)$ are, in fact, false since

$$2(1)+1>2^1 \text{ and } 2(2)+1>2^2.$$

However, $P(3)$ is true since

$$2(3)+1=7 \leq 2^3.$$

Let us suppose that $P(k)$ is true for all $k \geq 3$. Then we suppose

$$2k+1 \leq 2^k \quad (\text{if } k \geq 3).$$

But this implies that

$$2(k+1)+1=2k+3=2k+1+2 \leq 2^k+2 \leq 2^k+2^k=2^{k+1} \quad (k \geq 3)$$

and so $P(k+1)$ is true. Hence we conclude that for all $n \in \mathbb{N}$, $n \geq 3$

$$2n+1 \leq 2^n.$$

3. $P(n)$ is the statement that

$$n^2 \leq 2^n \quad (n \in \mathbb{N}).$$

$P(1)$ and $P(2)$ are true since

$$1^2 = 1 \leq 2^1, 2^2 = 4 \leq 2^2$$

but $P(3)$ is false since

$$3^2 = 9 > 2^3.$$

However, $P(4)$ is true since

$$4^2 \leq 2^4.$$

We make the induction assumption that $P(k)$ is true for all $k \geq 4$. But then

$$k^2 \leq 2^k \quad (\text{if } k \geq 4)$$

implies that

$$(k+1)^2 = k^2 + 2k + 1 \leq 2^k + 2k + 1 \leq 2^k + 2^k = 2^{k+1} \quad (\text{by 2 above})$$

and so $P(k+1)$ is true. Hence we conclude that for all $n \in \mathbb{N}$, $n \geq 4$,

$$n^2 \leq 2^n.$$

When we attempt to apply induction as above we must be on guard in regard to two aspects. We must ensure that we do not go blindly on from the truth of $P(1)$ (say) and try to prove $P(k+1)$ from $P(k)$ when in fact $P(2)$ or $P(3)$ or whatever may be false (as in the Example above). The second aspect which may cause trouble is an invalid use of a particular induction assumption. We illustrate this aspect in the next example.

Example 31

By induction we shall 'prove' that, given any set of billiard balls on a billiard table, the balls are necessarily of the same colour.

Our statement $P(n)$ is that if n balls or fewer are on a billiard table they are of the same colour. Certainly if there is only one ball there is only one colour and $P(1)$ is true. We now try to prove, from the assumption that if we have k balls or fewer then they are of the same colour, that we may deduce that if we have $k+1$ balls or fewer then they are of the same colour.

Given a set S of $k+1$ balls we may select two distinct subsets A, B of S of k balls each. Then $S = A \cup B$ and $A \cap B \neq \varnothing$. Now by the induction hypothesis the balls in A are of one colour and the balls in B are of one colour. But A and B have at least one ball in common and so the balls in A and B must be of a single colour. Hence, as $A \cup B = S$, the balls in S are all of the same colour and we have completed the induction step of the argument, namely $P(k)$ implies

$P(k+1)$. Hence $P(n)$ is true for all $n \in \mathbb{N}$ and the balls on a billiard table are all of the same colour.

The purported conclusion is clearly false – so what is wrong in our arguments? We were careless in supposing that $P(2)$ is a consequence of $P(1)$. A moment's reflection should reveal that $P(2)$ is false.

This example should serve as a warning that, in applying induction, care must be taken to ensure that the conditions are properly met.

We give some further examples in the use of induction. In these examples we shall omit specific reference to a $P(n)$ but we use the convention that

$$\sum_{r=1}^{n} a_r = a_1 + a_2 + \dots + a_n.$$

Examples 32

1. Prove that

$$\sum_{r=1}^{n} r^2 = \frac{n(n+1)(2n+1)}{6} \quad (n \in \mathbb{N}).$$

Certainly for $n = 1$ we have

$$1^2 = 1 = \frac{1(1+1)(2+1)}{6}$$

and so the statement holds for $n = 1$. We now suppose that

$$\sum_{r=1}^{k} r^2 = 1^2 + 2^2 + \dots + k^2 = \frac{k(k+1)(2k+1)}{6}.$$

Then

$$\begin{aligned}
\sum_{r=1}^{k+1} r^2 &= 1^2 + 2^2 + \dots + (k+1)^2 = (1^2 + 2^2 + \dots + k^2) + (k+1)^2 \\
&= \frac{k(k+1)(2k+1)}{6} + (k+1)^2 \\
&= \frac{(k+1)}{6}[k(2k+1) + 6(k+1)] \\
&= \frac{(k+1)}{6}[2k^2 + 7k + 6] \\
&= \frac{(k+1)}{6}(k+2)(2k+3) \\
&= \frac{(k+1)}{6}[(k+1)+1][2(k+1)+1].
\end{aligned}$$

This completes the induction argument and so the statement is true for all $n \in \mathbb{N}$.

2. Prove that

$$\sum_{r=1}^{n} \frac{1}{r^2} = \frac{1}{1^2} + \frac{1}{2^2} + \ldots + \frac{1}{n^2} \leq 2 - \frac{1}{n} \quad (n \in \mathbb{N}).$$

Certainly for $n = 1$ we have

$$\frac{1}{1} = 1 = 2 - \frac{1}{1}.$$

Suppose

$$\sum_{r=1}^{k} \frac{1}{r^2} = \frac{1}{1^2} + \frac{1}{2^2} + \ldots + \frac{1}{k^2} \leq 2 - \frac{1}{k}.$$

Then

$$\sum_{r=1}^{k+1} \frac{1}{r^2} = \frac{1}{1^2} + \frac{1}{2^2} + \ldots + \frac{1}{k^2} + \frac{1}{(k+1)^2} \leq 2 - \frac{1}{k} + \frac{1}{(k+1)^2}.$$

If we now focus our attention on the desired outcome of the induction argument we realize that we would like to show that

$$2 - \frac{1}{k} + \frac{1}{(k+1)^2} \leq 2 - \frac{1}{(k+1)}.$$

But this inequality is true since

$$\begin{aligned}\left(2 - \frac{1}{k+1}\right) - \left(2 - \frac{1}{k} + \frac{1}{(k+1)^2}\right) &= \frac{1}{k} - \frac{1}{k+1} - \frac{1}{(k+1)^2} \\ &= \frac{1}{k(k+1)} - \frac{1}{(k+1)^2} \geq 0.\end{aligned}$$

Hence

$$\frac{1}{1^2} + \frac{1}{2^2} + \ldots + \frac{1}{(k+1)^2} \leq 2 - \frac{1}{k+1}$$

and the statement is true for all $n \in \mathbb{N}$.

Exercises 1.5

Establish the following eleven statements by induction:

1. $\sum_{r=1}^{n} r(r+1) = \frac{1}{3}n(n+1)(n+2) \quad (n \in \mathbb{N})$.
2. $\sum_{r=1}^{n} r^3 = \frac{1}{4}n^2(n+1)^2 \quad (n \in \mathbb{N})$.
3. $\sum_{r=1}^{n} a^{r-1} = 1 + a + \ldots + a^{n-1} = \begin{cases} \dfrac{1-a^n}{1-a} & (a \in R, a \neq 1) \\ n \quad (a=1) & (n \in \mathbb{N}). \end{cases}$
4. $\sum_{r=1}^{n} \frac{1}{r(r+1)} = \frac{n}{n+1} \quad (n \in \mathbb{N})$.
5. $\sum_{r=1}^{n} (5r-2) = \frac{n}{2}(5n+1) \quad (n \in \mathbb{N})$.
6. $\sum_{r=1}^{n} r2^r = 2 + (n-1)2^{n+1} \quad (n \in \mathbb{N})$.
7. $(1+x)^n \geq 1 + nx \quad (x \in \mathbb{R}, x \geq 0)$.
8. $3(2n+1) \leq 2^n \quad (n \in \mathbb{N}, n \geq 6)$.
9. $3n^2 \leq 2^n \quad (n \in \mathbb{N}, n \geq 8)$.
10. $2(\sqrt{n+1} - 1) \leq \sum_{r=1}^{n} \frac{1}{\sqrt{r}} \quad (n \in \mathbb{N})$.
11. The Fibonacci sequence $u_1, u_2, \ldots$ is defined inductively by

$$u_1 = 1, u_2 = 2, u_{n+1} = u_n + u_{n-1} \quad (n \geq 2).$$

Write down the first nine terms of the sequence and prove independently the two following results:

(i) $u_n \leq \left(\frac{7}{4}\right)^n \quad (n \in \mathbb{N})$.

(ii) $u_n = \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^{n+1} - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^{n+1} \quad (n \in \mathbb{N})$.

The sequence was originally devised by Leonardo of Pisa, also called Fibonacci (c. 1170–1240), to model the procreative habits of amorous rabbits. Leonardo, through his text *Liber abbaci*, was influential in spreading the use of Hindu-Arabic numerals in Europe. We do well to remember the inestimable benefits these numerals have conferred and to acknowledge our intellectual debt to the civilizations from which they came. In the next chapter we shall exploit some of the advantages of the numerals.

1.6 Countable Sets

The sets $\{a, b, c, d\}$, $\{\alpha, \beta, \gamma, \delta\}$, $\{1, 2, 3, 4\}$ have no elements in common yet they share the property of being finite sets with the same number of elements. As we have seen, we may write the elements of a set X which has a finite number N of elements as

$$X = \{x_1, x_2, \ldots, x_N\},$$

in other words there is a bijection from $\{1, 2, \ldots, N\}$ to the set X. If a set X does not have a finite number of elements then X is infinite and there may or may not be a bijection from $\mathbb{N}$ to X. It is convenient to distinguish between 'levels' of infinity – as a porcine Napoleon might have decreed "All infinite sets are non-finite but some infinite sets are more infinite than others." (after *Animal Farm* by George Orwell, 1945). More precisely, we make the following definition to distinguish between those sets that admit a bijection from $\mathbb{N}$, or from a subset of $\mathbb{N}$, and those that do not.

Definition 17

A non-empty set X is said to be **countable** if the elements of X may be enumerated as a finite or infinite sequence of the form $x_1, x_2, x_3, \ldots$ If X is finite and has N elements then $X = \{x_n | n = 1, 2, \ldots, N\} = \{x_1, x_2, \ldots, x_N\}$ and if X is infinite then $X = \{x_n | n \in \mathbb{N}\} = \{x_1, x_2, \ldots\}$. Otherwise X is said to be **uncountable**.

Examples 33

1. The set $-\mathbb{N}$ of strictly negative integers given by $-\mathbb{N} = \{-n | n \in \mathbb{N}\}$ is countable since we have the sequence $-1, -2, -3, \ldots$ The bijection f from $\mathbb{N}$ to $-\mathbb{N}$ is given by $f(n) = -n$ $(n \in \mathbb{N})$.
2. The set $\mathbb{Z}$ of all integers is countable since we have the sequence $0, 1, -1, 2, -2, 3, -3, \ldots$ The bijection f from $\mathbb{N}$ to $\mathbb{Z}$ is given by

$$f(n) = \begin{cases} \dfrac{n}{2} & (n \text{ even}) \\ -\left(\dfrac{n-1}{2}\right) & (n \text{ odd}). \end{cases}$$

Since the elements of a countable set may be enumerated as a finite or infinite sequence it follows that the elements of any non-empty subset may also be enumerated as a sequence, namely as the subsequence of the given sequence obtained by omitting those elements not in the subset. Consequently we have the following result which we state for completeness.

Theorem 9

Any subset of a countable set is countable.

We shall prove that the set $\mathbb{Q}$ of rational numbers is countable but first we must investigate the countability of an array.

Remark

Let X be a set of elements x_{ij} having double suffices such that

$$X = \{x_{pq} \mid p, q \in \mathbb{N}\}.$$

We may write the elements down in the form of an infinite array similar to a matrix array:

$$\begin{array}{ccccc} x_{11} & x_{12} & x_{13} & x_{14} & \cdots \\ x_{21} & x_{22} & x_{23} & x_{24} & \cdots \\ x_{31} & x_{32} & x_{33} & x_{34} & \cdots \\ x_{41} & x_{42} & x_{43} & x_{44} & \cdots \\ \cdots & \cdots & \cdots & \cdots & \cdots \end{array}$$

We begin the first stage of the enumeration of these elements by choosing x_{11}. For the second stage we choose those elements of which the sums of their suffices are 3 and we take them in the order of first suffix. At the third stage we choose those elements of which the sums of their suffices are 4 and we again take them in order of the first suffix. Continuing we obtain a sequence as follows:

$$x_{11}; x_{12}, x_{21}; x_{13}, x_{22}, x_{31}; x_{14}, x_{23}, x_{32}, x_{41}; \ldots$$

Each element of the array appears precisely once in this sequence and so X is countable.

Before drawing general conclusions let us determine explicitly the bijection f from $\mathbb{N}$ to X. Certainly we have $f(x_{11}) = 1, f(x_{12}) = 2, f(x_{21}) = 3, \ldots$ We require to determine the integer to which x_{pq} corresponds. Now x_{pq} is the pth element in the stage of choosing in which we commence with $a_{1,p+q-1}$.

The stages prior to this stage have involved successively $1, 2, 3, \ldots, p + q - 2$ elements. Thus x_{pq} is the element in the $[[1 + 2 + \ldots + (p + q - 2)] + p]$th place in the sequence of enumeration. But, from an earlier example, we have

$$\begin{aligned} f(x_{pq}) &= [1+2+\ldots+(p+q-2)]+p \\ &= \frac{1}{2}(p+q-2)(p+q-1)+p \\ &= \frac{1}{2}[(p+q)^2-p-3q+2]. \end{aligned}$$

This gives, for example,

$$f(x_{34}) = \frac{1}{2}[(3+4)^2-3-12+2] = 18$$

and we may verify directly that x_{34} is in the 18th place. We may now derive several useful conclusions.

Theorem 10

The union of a countable number of sets, each of which is itself countable, is countable.

Proof

Let $X_1, X_2, \ldots$ be the countable sets of the union.

$$\begin{array}{llll} \text{Let } X_1 & \text{have elements} & x_{11}, x_{12}, & \ldots \\ \text{Let } X_2 & \text{have elements} & x_{21}, x_{22}, & \ldots \\ \ldots & \ldots & \ldots & \ldots \\ \text{Let } X_n & \text{have elements} & x_{n1}, x_{n2}, & \ldots \\ \ldots & \ldots & \ldots & \ldots \end{array}$$

Thus the elements of $\bigcup_n X_n$ may be written in an array identical to that in the Remark above. We know that the array above is countable and so $\bigcup_n X_n$ is countable. $\square$

Example 34

Since N, $-$N and $\{0\}$ are countable, so also is

$$\mathbb{Z} = -\mathrm{N} \cup \{0\} \cup \mathrm{N}.$$

Theorem 11

The Cartesian product of a finite number of countable sets is countable.

Proof

We prove the result first for the Cartesian product of two countable sets A, B.

Let A have elements $a_1, a_2, \ldots$ and let B have elements $b_1, b_2, \ldots$ Then the elements of $A \times B$ may be written in the array

$$\begin{array}{c} (a_1, b_1), (a_1, b_2), (a_1, b_3), \ldots \\ (a_2, b_1), (a_2, b_2), (a_2, b_3), \ldots \\ \ldots \quad \ldots \quad \ldots \end{array}$$

The array is countable and so is $A \times B$.

If now we have countable sets $X_1, X_2, \ldots, X_N$, then we have

$$X_1 \times X_2 \times \ldots \times X_N = (X_1 \times X_2 \times \ldots \times X_{N-1}) \times X_N$$

and a simple application of the Principle of Induction gives the final result. $\square$

Theorem 12

The set of rational numbers $\mathbb{Q}$ is countable.

Proof

Every strictly positive rational number is of the form $\frac{m}{n}$ for some $m, n \in \mathbb{N}$ and so may be identified with the ordered pair $(m, n) \in \mathbb{N} \times \mathbb{N}$. Thus $\frac{2}{3}$ may be identified with $(2, 3)$ and $\frac{4}{6}$ may be identified with $(4, 6)$; of course, purely as numbers, $\frac{2}{3} = \frac{4}{6}$ but formally $\frac{2}{3}$ and $\frac{4}{6}$ are distinct as the ordered pairs $(2, 3)$ and $(4, 6)$ are certainly distinct. Thus the set of strictly positive rational numbers $\mathbb{Q}^+$ is identified with $\mathbb{N} \times \mathbb{N}$ and so, by Theorem 11, $\mathbb{Q}^+$ is countable.

But letting $-\mathbb{Q}^+ = \{-q | q \in \mathbb{Q}^+\}$ we see that $-\mathbb{Q}^+$ is countable and so finally

$$\mathbb{Q} = -\mathbb{Q}^+ \cup \{0\} \cup \mathbb{Q}^+ \text{ is countable.}$$ $\square$

Not all commonly occurring sets are countable. We state, but do not prove, the following result.

Theorem 13

The set of real numbers $\mathbb{R}$ is uncountable.

Nevertheless it would be useful to exhibit at least one example of uncountability as follows.

Example 35

Let A be the set of all mappings with domain $\mathbb{N}$ and range $\{0, 1\}$. We claim that A is uncountable. We shall argue by contradiction in supposing that we have included all such mappings in a sequence of enumeration and then, like a conjuror producing a rabbit out of a hat, we shall produce a mapping not previously in the sequence. This then will be our contradiction.

Suppose, therefore, we have enumerated all of the given mappings from $\mathbb{N}$ to $\{0, 1\}$ in the sequence $f_1, f_2, \ldots$ Then every mapping from $\mathbb{N}$ to $\{0, 1\}$ occurs as an f_r for some $r \in \mathbb{N}$. We define $f : \mathbb{N} \to \{0, 1\}$ as follows:

$$f(n) = \begin{cases} 0 & \text{if } f_n(n) = 1 \\ 1 & \text{if } f_n(n) = 0 \end{cases} \quad (n \in \mathbb{N}).$$

Then for all $n \in \mathbb{N}$, $f(n) \neq f_n(n)$ and so $f \neq f_n$ $(n \in \mathbb{N})$. But then f cannot have occurred in the sequence $f_1, f_2, \ldots$ Hence the supposition of countability is invalid and so A is uncountable.

It is not the purpose of this text to give a logically impeccable account of the theory of sets, fundamental as this may be for mathematics. The reader should be aware, however, that matters in the affairs of sets, as in the affairs of hearts, may not be as straightforward as they appear. As illustration we offer some examples upon which the reader may exercise his or her analytical skills.

Examples of paradoxes

1. Epimenides of Crete is supposed to have said "Cretans are always liars" with the meaning that Cretans tell only lies. Was Epimenides lying or not when he made his statement? (Epimenides, 6th century BC, is believed to be the 'prophet' of St Paul's Epistle to Timothy, Chapter I, verse 12).
2. In a certain village there is a barber who shaves all and only those persons in the village who do not shave themselves. Does the barber shave himself? (attributed to B. Russell, 1872–1970).
3. In a certain country every prefecture must have a prefect and no two may have the same prefect. A prefect may be non-resident in the prefecture. The government passes a law creating a special area for non-resident prefects and obliging all non-resident prefects to live there. Eventually there are so many non-resident prefects in this area that the government declares it to be a prefecture. Where does the prefect of this new prefecture reside?

Exercises 1.6

1. Prove that $\mathbb{N} \times \mathbb{N}, \mathbb{N} \times \mathbb{N} \times \mathbb{N}, \mathbb{Z} \times \mathbb{Z}, \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$ are countable sets.
2. Prove that $\{a + b\sqrt{2} \,|\, a, b \in \mathbb{Z}\}$ is countable.
3. Let A, B be sets. Prove that A is countable if and only if $A \cap B$, $A \setminus B$ are countable sets.
4. Let $\mathbb{N}^{\mathbb{N}}$ denote the set of all mappings of $\mathbb{N}$ into $\mathbb{N}$. Prove that $\mathbb{N}^{\mathbb{N}}$ is uncountable.
5. Let the elements of the set X be denoted by x_{pq} where p is an element of $\mathbb{N}$ and q is an element of $\{1, 2, \ldots, N\}$ for some given N. Prove that X is countable.